Archives and Records

Privacy, Personality Rights, and Access

Mikuláš Čtvrtník

OPEN ACCESS

palgrave
macmillan

Archives and Records

Mikuláš Čtvrtník

Archives and Records

Privacy, Personality Rights, and Access

palgrave
macmillan

Mikuláš Čtvrtník
State Regional Archives in Prague
Prague, Czech Republic

ISBN 978-3-031-18666-0 ISBN 978-3-031-18667-7 (eBook)
https://doi.org/10.1007/978-3-031-18667-7

This Palgrave Macmillan imprint is published by the registered company Springer Nature Switzerland AG.
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

To Martina.

Acknowledgements

This book is the output of the "Analysis of Personal Data Processing in the Archives" research project (Code: VI20192022125) carried out within the Security Research Programme of the Czech Republic in the years 2015–2022 (BV III/1 VS) provided by the Ministry of Interior.

Keywords

Access to archives • Archival science • Data minimisation • Personality rights • Post-mortem privacy • Privacy protection • Records management • Right to be forgotten • Right to know

About the Book

The aim of this open access book is both to provide the reader with an overview of the complex issue of the protection of personality rights and privacy in archives, archiving, and in the context of records management in close connection with the analysis of policies of access to archives in its current setting and in historical perspective covering its development from 1945 to the present day in a broad international comparative perspective, and to provide inspiration for the adaptation of policies concerning the protection of personality rights and privacy in public administration with an emphasis on archiving in the public interest and records management.

The book explores the policies, specific inspirational models, and some distinct procedural and regulatory settings of the protection of personal rights and privacy in public administration, particularly in archives and records management. The book deals in detail with post-mortem privacy protection in archives and data archiving, which is given by the fact that the vast majority of materials preserved in archives concerns deceased persons.

The monograph presents several significant cases of misuse of personal data contained in records and archives, such as misuse of census data, medical records, and other groups of materials. It analyses in detail the topic of minimisation and reduction of data in public records and archives, including the current phenomenon of data anonymisation and pseudonymisation, and the risks of de-anonymisation and reidentification of persons.

Contents

About the Author

Mikuláš Čtvrtník, Ph.D., is an assistant professor in the Department of Archival Science and Auxiliary Sciences of History at the Faculty of Arts, Jan Evangelista Purkyně University in Ústí nad Labem, Czech Republic, and a visiting assistant professor at the Charles University in Prague and head of the Department of Public Administration Archives in the State Regional Archives, Prague, Czech Republic. He holds a Ph.D. from Charles University, Prague, specialising in theory and methodology of history. In his research he focuses on archival science, theory, and methodology of history and historiography, and governance issues with particular emphasis on the analysis of public administration records and on records management. He is the author of several monographs; in Germany, he wrote the book *Geschichte der Geschichtswissenschaft: Der tschechische Historiker Zdeněk Kalista und die Tradition der deutschen Geistesgeschichte* (Diplomica Verlag. Hamburg 2010). His latest book deals with the topic of intellectual history in the context of European historiography of the nineteenth and twentieth centuries (Argo. Prague 2019).

Abbreviations

ECHR	European Court of Human Rights
GDPR	General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC)
FOIA	1. Freedom of Information Act of 4 July 1966, 5 United States Code § 552; 2. Freedom of Information Act of 30 November 2000. Ch. 36
NARA	National Archives and Records Administration
CADA	Commission d'accès aux documents administratifs [Committee on Access to Administrative Documents]
ICO	Information Commissioner's Office
NCTR	National Centre for Truth and Reconciliation
NS-Archiv	Archive of National Socialism

List of Tables

CHAPTER 1

Introduction

"Do the interests of the living outweigh those of the dead? … Does the privacy of living persons override the importance of historical research and does the right of access give way to the right to forget?"[1]

(Eric Ketelaar, Archivalization and Archiving)

"Commit nothing to paper, and certainly not to a computer or a cell phone. Keep it in your head. It's the only private place we have left."[2]

(Frederick Forsyth, The Cobra)

"To begin, then, at the beginning, I was serving at that time on the staff of a division commander whose name I shall not disclose, for I am relating facts, and the person upon whom they bear hardest may have surviving relatives who would not care to have him traced."[3]

(Ambrose Bierce, The Major's Tale)

[1] Ketelaar, E. (1998, 23 October). Archivalization and archiving. Unpublished inaugural address as Chair of Archivistics, University of Amsterdam, p. 6. As cited In V. Harris, Knowing right from wrong: the archivist and the protection of people's rights. *Janus*, 1999.1, 32–38, here p. 33.

[2] Forsyth, F. (2010). *The Cobra*. G. P. Putnam's Sons.

[3] Bierce, A. (1890, 5 January). *The Major's Tale*. First published in the San Francisco Examiner as: A Practical Joke: Major Broadwood Recalls the Heroic Past.

M. Čtvrtník, *Archives and Records*,
https://doi.org/10.1007/978-3-031-18667-7_1

The mission of archives and records management is not just to collect and store materials and information. Their purpose is also to make them accessible. Archives are one of the most important places where the right of a free society to access to information, the right to know and, with it, the freedom of expression are exercised. However, both the collection and preservation of information, including archiving, and the opening of access to it, enter the area of the protection of personality rights, privacy, and personal data, that is, one of the most complex areas of archiving and records management, in a significant way. This is also due to the fact that at the very heart of the issue is the fundamental tension: On the one hand, the collected and preserved public records and archives, including a wide range of personal and sensitive data, serve a plethora of public interests and the exercise of citizens' rights; on the other hand, they carry an ever-present latent risk of potential misuse, including very serious forms with serious implications for people's lives and rights. This can be generally expressed in the form of a paradox: By sharing data about themselves, whether to the state, its authorities, private entities, and other people, individuals exercise and protect their rights, including the protection of their personality rights and privacy. The same act, however, puts them at risk of misuse. Yet, if an individual did not share their data, they would not be able to exercise their rights at all.

The protection of privacy, personality, and personal data in archives represents one of the most complicated domains of the archival sector. This is due to its initial situation. On the one hand, archives containing a vast range of personal data represent important tools for exercising citizens' rights, from economic rights (archives are important proofs of ownership, etc.) to fundamental human rights, as characteristically shown—providing one example for all—by the archives of security forces during the period of totalitarian regimes, which serve to administer justice to victims and perpetrators in the period after the end of the dictatorial regimes of the respective societies. On the other hand, personal data such as the content of the same archives may be grossly misused and have a very serious impact on the lives of people concerned in the archives. In a similar context, Eric Ketelaar made an excellent point that it is therefore "so difficult to keep the right balance between, on the one hand, the requirement to destroy personal data when they have served their primary purpose, including that of serving the legal rights of the data subjects, and, on the

other hand, the possibility that the files might get a new meaning and purpose in the future".[4]

Concisely, the same document may in one situation be used to assert legal and democratic rights, often after a very long time and often in quite different contexts and for quite different purposes than those for which the document was originally created, for example, during restitution, for inheritance claims, but also for the purposes of judicial rehabilitation, punishment of perpetrators of, for example, political crimes, crimes against humanity, and so on. On the other hand, the same document in a different situation can lead to considerable harm to a person and their fundamental rights and freedoms. There is much historical evidence to support Christian Keitel's statement: "Every totalitarianism loves personal data".[5] However, personal data may be misused even in societies perceived as democratic. I shall examine some examples in this book.

Access to public records and archives as one of the concrete manifestations of the general and usually constitutionally guaranteed freedom of expression and information and the right to know and, on the other hand, the protection of personality rights and privacy in archiving and records management form an inseparable pair of 'communicating vessels' and have become the subject of this book. Their connection is determined first by the fact that archiving and records management cannot be separated. Archival management takes over from records management and records keeping at the stage when records are still managed and preserved by their creators, be they public institutions, private entities, natural persons, families, associations, and so on. However, a small part of the records will one day become archives and will continue to be preserved and maintained in the respective archives.

The inseparability is also determined on the level of the relationship between data protection on the one hand and access to data on the other, in the specific aspect of working with archival sources. No functioning democracy and rule of law could exist without the freedom of expression, the right of access to information, the right to know. After all, open access

[4] Ketelaar, E. (2005). Recordkeeping and Societal Power. In S. McKemmish, M. Piggott, B. Reed, F. Upward (Eds.), *Archives: Recordkeeping in Society* (pp. 277–298). Charles Sturt University, p. 285.

[5] Keitel, Ch. (2019). Archivcamp "Volkszählung 2021 und Rolle der digitalen Archive". In *23. Tagung des Arbeitskreises Archivierung von Unterlagen aus digitalen Systemen*, National Archives (Prague). https://www.nacr.cz/wp-content/uploads/2019/KnihaAUDS_e-kniha_DEF.pdf, p. 167.

to archives is one of the pillars of the *Universal Declaration on Archives* developed by the International Council on Archives and adopted by UNESCO in 2011.[6] In addition to knowledge, its aim should also be to promote democracy. The role of archives in this regard becomes all the more important the closer to the truth is the recent warning by a group of liberal intellectuals, authors, and public figures who, in their "A Letter on Justice and Open Debate", expressed their belief that "The free exchange of information and ideas, the lifeblood of a liberal society, is daily becoming more and more constricted".[7] The signatories of the Letter observe a growing trend throughout our culture today to restrict freedom of speech, open debate, and tolerance of differing opinions.

The accessibility of information embodied in public archives and records and physically stored in public archives, as well as in other institutions managing records of various kinds, constitutes one of the fundamental pillars of the exercise of the freedom of expression and information. Alas, this right is not a universally applicable principle. As Eric Ketelaar succinctly pointed out in one of his interviews: "There is no natural law stating that archives should be accessible to anyone. That is something that is only 200 years old. What most archivists do not realise is that availability, accountability, findability, etc., are not universal and natural laws or principles. It is the law, yes, but the law is only an expression of what society at a particular point in time believes to be right or wrong."[8]

Archival materials and public records preserved in archives—unlike books and other forms of multiplied and recycled data in today's world—have one extremely important aspect: their uniqueness and irreplaceability. The absolute majority of the content of archives consists of primary sources. Unlike secondary sources—typically published in some form—these sources are characterised by uniqueness, that is, they only exist in a single or several copies; although especially after 1945, the multiplication of records production increased enormously, manifesting, for example, in the creation of multiples of multiple copies of official records, which until

[6] The Universal Declaration on Archives (2010). Endorsed by 36th Session of the General Conference of UNESCO Paris, 10 November 2011. Adopted at the General Assembly of ICA Oslo, September 2010. https://www.ica.org/en/universal-declaration-archives

[7] A Letter on Justice and Open Debate. (2020, 7 July). *Harper's Magazine*. https://harpers.org/a-letter-on-justice-and-open-debate/

[8] Glaudemans, A., Jonker, R., Smit, F. (2014). Beyond the traditional boundaries of archival theory. An interview with Eric Ketelaar. In F. Smit, A. Glaudemans, R. Jonker (Eds.), *Archives in Liquid Times* (pp. 294–305). Stichting Archiefpublicaties, p. 304.

a few decades ago were often produced in only one or at most two copies. To close the gate on such a unique source of information, often stored in a single archive, is to close access to it altogether.

Primary sources represent both the primary and the least mediated trace of the past. These are the materials that stood closest to a particular event or phenomenon and are only minimally reinterpreted by their future reporters. Very often, the creator did not even expect that his information output would one day be used as a source, for example, by researchers. This adds to the quality and value of such a primary source, which is in this sense figuratively speaking a "raw", original, and "unprocessed" source of data. Adding this "rawness" and "unprocessed" form of information to the rarity and very often the uniqueness of primary sources, restricting access to such sources of information often means a catastrophic intervention leading to the elimination of the possibility of knowledge and the right to know.

This, however, also reveals the reverse side of the matter. Allegorically speaking, the high value of the primary source thus formed increases the price to be paid. This price is the high protection of the data that the source carries. The more the primary source represents material not originally intended for publication, material not intended for various future uses and in this respect unintended, the greater the urgency of the need to adequately protect the data contained therein, including personal data. This is significantly amplified by the fact that the persons concerned in archival records usually have no knowledge that data about them is being handled in the context of archiving and have no possibility to influence its future use and disclosure.

Let us look at the whole situation from the perspective of archival practice. Access to archives and information, together with archival processing and archival appraisal resulting in the selection of a very small number of records for, what archives believe will be, permanent preservation, are the three most important and robust domains of archival work. Access to archives is inextricably linked to the protection of the data they contain and, in particular, to the protection of data relating to the individual people concerned in the records in question. The issue of providing access to archives and the protection of their actors is implied by several formative constants framing the entire context; these constants need to be kept in mind when policies, strategies, as well as specific procedures for access to archives containing personal data are established. What are they?

1. Archives collect and provide access to material containing personal data or entering the protected area of privacy and personality rights in the absolute largest number of cases without the knowledge of those concerned. It is a phenomenon that can be succinctly described by the phrase "without consent", which was chosen as the title of her book by the distinguished author in the field of archival science, Heather MacNeil.[9] This is interconnected with another constant:
2. Archives collect and provide access to records and the data they contain, including personal data, for fundamentally different purposes and motivations than those for which the records were created. In other words, the reasons that led to the creation of a record and the appearance of certain personal data in it were quite different from the reasons behind, first, its transfer to an archive, and second, the requests for access to this material by various groups of requestors—historians, genealogists, students, relatives, and many other private entities; apart from those, access to such material may also be requested for a variety of official purposes. Once again, their motivations are usually different from those that led to the creation of the data in question. I will give just one illustrative example: Minutes of the meetings of a municipal council are taken for the purpose of running the local government and the municipality. However, after a certain period of time, they can serve, for example, as evidence in an investigation of alleged corruption.

   The crucial point from the perspective of personality and privacy protection is that the consultation and use of personal data in archives happens for fundamentally different purposes than those to which the data subject gave their implicit or explicit consent, if a consent had been given at all. The importance of this fact grows in those societies and their legal systems in which there is a strong awareness of the need to maintain the duty of confidentiality. A prime example of this is the United Kingdom and British common law, as well as societies and legal systems that follow the tradition of British common law, as is the case of Canada. It was a Canadian author Heather MacNeil who aptly described the core of this issue: "The invasion of privacy that results from the failure to obtain consent for a clearly different use of the information than the one origi-

[9] MacNeil, H. (1992). *Without Consent. The Ethics of Disclosing Personal Information in Public Archives.* Society of American Archivists, Scarecrow Press.

nally agreed to may be exacerbated by the breaking of a promise of confidentiality that was made, either explicitly or implicitly at the time the information was originally collected. The moral rule against breaking a promise of confidentiality is rooted in respect for individuals' autonomy over information about themselves, as well as respect for the integrity and importance of the confidential relationship in which such information is shared."[10] Hence another constant:

3. A certain level of control over what information I share about myself, with whom, and for what purposes lies at the very heart of privacy and personality protection. This fact is inherent in most democratic societies, whether it manifests, among other things, in the principle of confidentiality, as it does in the British society and its common law, in Canada, Australia, and other countries, usually those where British law has made its mark, or in slightly different tools. Indeed, the recently approved EU General Data Protection Regulation (GDPR)[11] embodies this very intention to allow citizens a much greater control over the flow of information about themselves. Such control also extends to the field archiving and the management of information archives maintain.
4. It is, however, still true that an individual's control over their information will forever remain limited. Individual citizens cannot be given an exclusive and unlimited right to manage information about themselves. This cannot be done in the exercise of public administration and the implementation of the entire set of obligations imposed on citizens by the state, as well as on the state and government itself, on public administration and public authorities in the performance of the necessary legal duties. This also applies to the field of archiving and records management, including the personal data contained in such records. Using the GDPR terminology, the "right to be forgotten" is not indefinite. But how are its boundaries constructed? What defines them against the right to know? There is no simple answer. The text of this book intends to, among other things, present certain means and actual options to find these bor-

[10] MacNeil, H. (1992). *Without Consent*, p. 169.

[11] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). https://eur-lex.europa.eu/eli/reg/2016/679/oj

ders and to move along them, especially in the field of archiving in the public interest and records management.

Yet, this is far from being solely a legal problem. The legal system only mirrors reality in a formalised and limited manner. A person necessarily leaves traces of living their life. The hypothetical possibility of a complete "covering of the tracks" would have disastrous consequences for any society, as it would threaten to open the gates for violations of the law and basic rules of the functioning of the whole society; and just as disastrous would be the consequences of any Orwellian big-brother totalitarian surveillance of all life and every step of an individual and the whole society. A man's freedom and an open democratic society are only possible when they fall in a reasonable Aristotelian middle ground between these extremes. And the same applies to the field of archiving and archives, specifically to the area of access to archives and the protection of the personality and privacy of those who have become actors of public records and archives.

However, the search for the imaginary "right middle ground", for the right measure between restricting and providing access to information stored in archives, is at its deepest core shaped by the fact that the proverbial "explicit consent" to the collection and access to the data of those concerned has not been given. An alternative perspective can express the same in a different way: Unlike books, which were written and usually published with the clear intention of being read by the masses (the author wrote the text knowing it would reach many readers), in the case of public records and archival material the opposite is overwhelmingly true. Public records, some of which are subsequently preserved in public archives, were in the vast majority not created with the primary intention of being published. On the contrary, their creators and, even more significantly, their actors usually did not foresee that these records would one day be read, or rather read for the purposes and intentions of research. This does not mean that access to such materials should be restricted. Although originally spoken in a different context, we can take into account the words of distinguished French historian Arlette Farge: "The witness, the neighbor, the thief, the traitor, and the rebel never wanted to leave any written record, much less the one they ended up leaving".[12] But that is no reason why society should not have the right to know about the actions of

[12] Farge, A. (2013). *The allure of the archives*. Yale University Press, p. 16.

at least some of them. From the perspective of a historian, Farge views this premise of the unmediated, unintended, and therefore all the more spontaneous and authentic testimony of archival historical sources as encountering not something dead, as it might at first seem, but rather life itself.

Access to archives and the related protection of the data they contain, in particular the protection of the individuals concerned, their personal data, personality and privacy rights, encompasses several levels, each of which represents a different overall perspective on the issue. Those levels are in particular:

1. Legal: Every country with a developed archival system stipulates a basic body of rules for access to archival material at the legislative level, usually by law and other implementing regulations, or in case law, especially in countries implementing the common law system. Apart from archive-specific legislation, the legislation regulating data protection and management in general, and the protection of personal data and privacy in particular, plays an increasingly important role.
2. Reality and practice of archiving in the public interest and of records management form another level: Although it is the legal system that lays down the basic rules and boundaries, the actual practice of archives and archiving in providing access to records and in data protection, its specifics, real limitations, issues and risks cannot be entirely covered by any one legal regulation and a purely legal analysis is not sufficient in such cases.
3. Ethical: Access to public records and archives and the protection of privacy, personality rights, and personal data in archival materials are substantially linked to the ethical aspects of the issue. Although both this book and archival practice itself are primarily concerned with the first two levels, the ethical and moral layer of meaning is always latently present and contributes to the formation of both the legal and archival practice. All three levels should also be considered and incorporated in the codes of ethics of archivists and of other professions working with records and archives. In 1996, International Council on Archives compiled a Code of Ethics that is still valid

> today and is currently available in 24 languages.[13] Section 7 states: "Archivists should respect both access and privacy, and act within the boundaries of relevant legislation. Archivists should take care that corporate and personal privacy as well as national security are protected without destroying information, especially in the case of electronic records where updating and erasure are common practice. They must respect the privacy of individuals who created or are the subjects of records, especially those who had no voice in the use or disposition of the materials." This code of ethics fundamental for the whole field of international archiving thus mirrors the above phenomenon: When implementing privacy protection, managing and providing access to personal information, archivists shall bear in mind the "non-existent consent" of those concerned in the records. And the "without consent" phenomenon also reflects in other ethical codes that archivists follow.[14]

The codes of ethics of other allied professions and disciplines also very often include the topic of privacy or the whole sphere of personality rights. For example, already in its Code of Professional Responsibility of 1992, the International Association of Records Managers and Administrators (ARMA International), sets this as one of the social principles for records and information managers: "Affirm that the collection, maintenance,

[13] International Council on Archives. (1996). *ICA Code of Ethics*. Adopted by the General Assembly in its XIIIth session in Beijing (China) on 6 September 1996. All language versions available at https://www.ica.org/en/ica-code-ethics. Codes of ethics, or more generally the relationship between ethics and the profession of archivists or records managers, are also the subject of several professional texts. Cf., for example, Benedict, K. M. (2003). *Ethics and the Archival Profession: Introduction and Case Studies*. Society of American Archivists; also, for example, Cook, M. (2006). Professional ethics and practice in archives and records management in a human rights context. *Journal of the Society of Archivists*, 27(1), 1–15; Neazor, M. (2008). Recordkeeping Professional Ethics and their Application. *Archivaria*, 64 (April), 47–87. https://archivaria.ca/index.php/archivaria/article/view/13146; Ketelaar, E. (1998, 3 October). Professional Ethics: The Moral Defence of the Archivist. Paper presented at the conference "Cyber, Hyper or Resolutely Jurassic? Archivists and the Millennium". University College Dublin.

[14] Cf., for example, Society of American Archivists. *Code of Ethics for Archivists*. Approved by the SAA Council, February 2005; revised, January 2012 and August 2020 (https://www2.archivists.org/statements/saa-core-values-statement-and-code-of-ethics: "As appropriate and mandated by law, archivists place access restrictions on collections to ensure that privacy and confidentiality are maintained, particularly for individuals and groups who have had no voice or role in collections' creation, retention, or public use".

distribution, and use of information about individuals is a privilege in trust: the right to privacy of all individuals must be both promoted and upheld".[15] In its Code of Ethics, they outline the requirement to "protect the privacy of individuals".[16]

Antoon de Baets, a distinguished historian focusing, among other things, on censorship and restricting access to historical sources, as well as on the ethics of work as a historian, has drafted a proposal for a "code of ethics for historians".[17] In it he also devotes significant space to freedom of expression and information (Article 4 in the draft Code). One of the proposed articles, however, also includes selection of information. According to him, historians "are entitled to demand that archival selection criteria (that is, criteria to preserve or destroy records) are not politically inspired and take due account of the historical interest".[18] This book will discuss archival appraisal in Chap. 8. In the draft Code, Antoon de Baets also stresses that access to sources and archives should be as open and equal as possible for researchers, and that restrictions and exemptions should only be very rare and legal. On the other hand, de Baets, in his draft code of ethics for historians, referring to the International Covenant on Civil and Political Rights (1966), emphasises the protection of the dignity of and respect for those appearing in the sources: "historians shall respect the dignity of the living and the dead they study". Historians, according to de Baets' draft, have the right "not to disclose historical facts harming the privacy and reputation of persons, either living or dead".[19] In balancing the requirement for maximum openness of access to information and the right to know, on the one hand, and the legitimate demands for confidentiality on the other, Antoon de Baets states in his draft code that historians "should balance any nondisclosure against disclosure with a presumption in favour of disclosure".[20]

[15] Association of Records Managers and Administrators. (1992). *The Code of Professional Responsibility.* https://www.usna.edu/Users/cs/adina/teaching/it360/spring2013/ethics/ARMACodeOfProfessionalResponsibility.pdf

[16] Association of Records Managers and Administrators. *Code of Ethics.* https://www.arma.org/page/IGP_Ethics#

[17] De Baets, A. (2009). *Responsible history.* Berghahn Books, pp. 173–196, the Draft Code can be found on pp. 188–196.

[18] De Baets, A. (2009). *Responsible history*, p. 191.

[19] De Baets, A. (2009). *Responsible history*, pp. 192 and 193.

[20] De Baets, A. (2009). *Responsible history*, p. 193.

This book will cover all the three levels of the issue, legal, practical, and ethical and will also mention the perspectives of access to public records and archives and the protection of privacy and personality rights of those concerned.

The very term "personality rights", whose protection is embedded in a number of legal systems, is not straightforward. The concept of personality rights is based on the existence of persons in the sense of physical as well as spiritual and moral entities.[21] These rights include, among others, the right to physical liberty, privacy, identity, likeness and image, reputation, dignity, physical-psychological integrity, and also the right to life itself, sentience, and some other rights. While in the common law system "personality rights" include rather particular acts and torts protecting certain aspects of personality, such as misappropriation of name, breach of confidentiality, and so on, they have a stronger position in continental law. Moreover, some legal systems have introduced or are gradually introducing post-mortem personality protection, that is, the protection of at least some of the personality rights of a person at the time of and after their death. However, in cases when legal systems do establish post-mortem personality protection, they do not equate the protection of the personality rights of the living and the deceased. They usually gradually reduce the post-mortem protection of personality in proportion to the time that passed since the death of the person concerned. The book will touch on the topic of post-mortem personality protection in various contexts continuously in almost all chapters.

The concept of "privacy" is even more multi-layered. It is often shaped quite differently in different contexts, from legal, philosophical, ethical and moral, political, sociological, to anthropological, technological, security, and other contexts.[22] At the level of legislation and case law, lawmakers and courts most often avoid any explicit definition of privacy. This book will analyse privacy in the context of archives, records management, archival practice, and data protection within archival practice. The concept of privacy is derived from the Latin term "privatus" meaning personal,

[21] A detail analyses of personality rights in comparative legal perspective is provided in Neethling, J. (2006). Personality Rights (entry). In J. M. Smits (Ed.), *Elgar Encyclopedia of Comparative Law*. Edward Elgar, 530–547.

[22] Cf. the definition of privacy in, for example, DeCew, J. (2018). Privacy. In *The Stanford Encyclopedia of Philosophy*. Spring 2018 Edition. https://plato.stanford.edu/archives/spr2018/entries/privacy/; Staples, W. G. (Ed.). (2007). *Encyclopedia of privacy*. Greenwood Press.

separate, belonging to oneself. The significant feature is its distinction from the public sphere, or rather its concealment from the public gaze.[23] An important moment in the protection of privacy is the inviolability of the person and the possibility of control over information about oneself, which is given to citizens. This control then includes, among other things, what data is communicated, how, to whom and for what purpose it is communicated, made available, but also directly published. For this very reason, this area directly affects the field of archiving and archives, whose mission is not only to preserve data and records, including often very sensitive data about persons, but also to make them accessible and often publish them. Ultimately, privacy protection includes the protection of human dignity, integrity, autonomy, and independence. Privacy also includes the protection of a person's intimate sphere; it embraces the physical part of life (home, etc.) as well as the virtual part, including the online space. In legal systems, privacy is usually protected as a constitutional right and constitutes one of the personality rights of the individual.

The book will address protection of personality rights in archives in the broader context of the issue of access to archival records, and in some respects also on the general level of protection of information not only of a personal nature. It will pay special attention to post-mortem protection of personality and privacy, which represents a very young domain within archival law and practice, and this also applies to research in this field. Yet, it is post-mortem protection of personality and privacy that should lie at the centre of the field of archiving as the vast majority of those concerned in the archives are now deceased. This is also the reason why the protection of privacy and personality rights in the field of archiving takes on specific contours, in contrast to the general protection of personal data, where the relevant legislation usually targets solely or almost exclusively living persons. After all, the very definition of personal data is most often limited to the category of living persons and as such usually omits post-mortem protection.

Chapters 2 and 3, will focus on several selected specific situations, models, or special procedural settings that can be encountered in the archival systems of some countries, namely Germany, the United Kingdom, and France, and it will also touch on the situation in the USA and some other countries. The aim is not to provide a comprehensive and summary

[23] Cf. Mates, P. (Ed.) et al. (2019). *Ochrana osobnosti, soukromí a osobních údajů*. Leges, p. 15ff.

synthesis of the overall setup of access to archives and personal data protection in these countries, but to highlight and analyse in more detail some specifics, peculiarities, and inspirational moments that could be potentially used in other archival systems.

Although recent developments in the area of data protection and increasingly serious cases of data leaks and misuse point to data retention as a potential threat to their future misuse, Chap. 4, will aim to prove that the opposite can also be true. It will argue and use several specific cases to demonstrate that and in what sense archiving represents not only a risk to the protection of personality and privacy, but also a form of protection. In this respect, it will identify one of the paradoxes of archival work.

Chapter 5, will concentrate on the specific "right to be forgotten", increasingly referred to in the European Union and beyond, as a form of protection of privacy and personality rights. It will define it against the right to know, the right to information, and freedom of expression, and analyse its place in the field of public archives and archiving in the public interest. It will look at its implications for archives and records management and conclude by presenting a proposal for a model of four categories of the right to be forgotten, including the possibilities of its use in practice, especially in records management and archiving.

Chapter 6, will provide a bridge that will take the book to its second part and the primary perspective on the risks associated with the preservation and archiving of personal data. In Chap. 6, the book will first follow the phenomenon of the enormous increase in the volume of records and data created, especially after 1945. The chapter will present the results of an international empirical survey providing specific figures showing the extreme increase in the volume of records created and maintained in public archives. Chapter 7, will then conduct a detailed case study analysis of several examples of leaks and misuse of personal data in the twentieth century, some of which have had tragic impacts on broad groups of the population. The records that come into play include, for example, census records, medical records, Jewish files during the Nazi dictatorship, and archives of the former East German State Security Service.

The final chapter, Chap. 8, will examine protection of personality rights, privacy, and personal data in the space of archiving and records management from the perspective of one of the most important tools used to implement this protection, that is, the minimisation of preserved data and restrictions on their storage. This covers data reduction in two related respects: first, data destruction and reduction of their content, and second,

limiting the period for which data are retained. Data minimisation and storage limitation will be analysed both in the records management phase as well as in the subsequent archiving phase, when a very small part of the created information and records is transferred to archives for long-term or permanent archiving. Archives and archiving play a specific and perhaps surprisingly crucial function in this case. They are the places where the vast majority of legal destruction of public records takes place within the specific process of archival appraisal, with approximately 95% of the created records being destroyed so that the remaining approximately 5% can be archived. The chapter will ask how the nature of archival appraisal has been formed and changed in recent times and will point out the trends that can be expected in the near future.

As part of the analysis of data minimisation tools, the process of data anonymisation and pseudonymisation in the pre-archiving phase and during archiving is examined, and finally the increasingly current phenomenon of the dramatically increasing possibilities and related risks of de-anonymisation and reidentification are touched upon. As early as the early 1990s, Heather MacNeil saw a trend of increasing societal concern about the loss of privacy that had been going on for at least two decades. Already then, she noticed the considerable risk represented by the massive technological developments in IT and the possibilities of extremely large-scale mass data collection. In particular, she highlighted the dangers of combining data on citizens from different sources: "Civil libertarians maintain that, even if nothing intrinsically private or improperly derogatory is stored in a data bank, the possibility exists that the vast quantities of ostensibly innocuous information on citizens, combined with the technological capacity to link information from a variety of sources, will result in a less spontaneous and, ultimately, less free society".[24] These tendencies have, since then, intensified considerably. While at that time MacNeil detected a greater risk in the use of these new tools by government institutions, we now see that more significant risks come from private companies, of which the Facebook-related cases are the most visible.

Since the text combines a purely scientific treatise with the aim to bring practical inspiration and guidance, especially in the field of archiving and records management, the book will conclude with a final section containing a summary of some, as far as possible, specific recommendations for archival practice, suitable for application in various archival systems. There

[24] MacNeil, H. (1992). *Without Consent*, p. 3

is therefore a significant limitation given by the fact that the book is not framed by the archiving and legal system of a single country, but rather its intention was to provide a broad international comparison.

The book does not aim to be a compendium of all the legislation and practice of archives and records management across all countries and continents, but to present an analysis of the issues of personal data and privacy protection in relation to opening access to archives and records, and to highlight, by means of a comparative approach, some of the main problems and solutions offered in the management of records and archives in particular. It therefore focuses only on several selected countries for which it makes sense to conduct a comparative research. The geographic focus was chosen so that it took into account first, the continental and common law and second, countries with a long democratic tradition (USA, Canada, Australia, United Kingdom, France) and include them in analyses and comparisons together with either young democracies or countries that underwent periods of dictatorship, totalitarianism, or oppression in the twentieth century (some countries in Central Europe, including Germany, and also France, during the time of Nazi occupation and Vichy France). Overall, the perspective focuses mainly on Europe, and looks towards North America and Australia on several occasions.

The enduring mission of archives and archiving has always been, and should continue to be, to preserve in the very long term, with the ambition of permanently preserving information that is valuable to society and its memory, to make this information as accessible to the public as possible, but also to protect a certain segment of data. They should in particular, protect such data that could harm the individuals concerned in the archival records. This book intends to be one perspective on how to seek a balanced approach in this field based on international comparisons, both in the field of archiving and records management. It also aims to present some of the already implemented and some yet-to-be-implemented or under-developed solutions and last but not least to summarise recommendations on how to address some of the fundamental issues in the field of personality protection in relation to access to archives and records.

CHAPTER 2

Personality Rights, Privacy, and Post-mortem Privacy Protection in Archives: International Comparison, Germany and "Protection of Legitimate Interests"

The protection of personal data, personality, and privacy is implemented in the rule of law at various levels. One of them is the protection of data relating to an individual, a natural person, and giving evidence about them in one way or another. A specific case is the protection of personality in archives and records. This is closely linked to the broad area of archival methodology and practice, commonly referred to as *access to archives*. At the same time, it enters a distinct field of legislation, legal practice, and research that has increasingly come into question in recent years and for which the term "post-mortem privacy" and its protection begin to apply.

There is also another perspective that is of great importance to the study of protection of a person, their personality, and privacy in the archives. It has been almost 30 years since a prominent Canadian author in the field of archival science, Heather MacNeil, published an excellent book with a fitting title, "Without Consent".[1] The title is better than good. It aptly concentrates some of the essential features of the situation of virtually all public archives (but in certain situations also other public institutions as administrators of public information): The mission of archives is not just to collect and store materials and information. Their purpose is also to make them accessible. Archives are one of the most important places where society's right of access

[1] MacNeil, H. (1992). *Without Consent. The Ethics of Disclosing Personal Information in Public Archives*. Society of American Archivists, Scarecrow Press.

M. Čtvrtník, *Archives and Records*,
https://doi.org/10.1007/978-3-031-18667-7_2

to information is exercised. It is impossible to imagine a functioning democracy without this right. However, it is also true that in the vast majority of cases, archives make information available when they do not have the consent of the persons whose data, privacy, and personality are concerned. This is a given that archives cannot change in real practice. In the vast majority of cases, it is not possible or realistic to identify the specific person concerned in the archives without a complex investigation (the name alone is not sufficient for identification). In other situations, while it is possible to identify the particular person, it is impossible to contact them, either because their address is unknown, because the archive does not have access to public administration records, in which they would trace the address, or because it is not within the archive's capacity to address the vast number of people who appear in the archives and so on. Ultimately, the reason consent cannot be obtained in by far the greatest number of cases, is the simple fact that the person concerned is deceased. Which thus opens a specific area of the so-called post-mortem protection of personality and privacy, which has only recently become a more debated topic in both legal and archival science.

Archives are therefore put in a position in which they represent one of the key places of public interest in access to information, that is, they are supposed to strive for maximum openness, and at the same time they are forced to face the need to make available material concerning persons who in most cases cannot be given the opportunity to comment on such disclosure. This represents a fundamental difference from the initial situation where the data administrator has the possibility to obtain consent from the persons concerned without major difficulty, which is most often the case when the data subject voluntarily provides their data usually to private entities and they also give explicit consent to the disclosure of such data. However, in the vast majority of cases, public archives do not have such consents.

The absence of consent, however, comes second to the actual acquisition of personal data: A citizen does not usually consent to the collection and processing of their personal data when the data are collected and processed by government authorities, public administration, and public authorities within their legal authority. The citizen must, of course, tolerate such processing to the extent necessary. The problem, however, is that, as Heather MacNeil also pointed out,[2] by providing their data to a certain

[2] MacNeil, H. (1992). *Without Consent*, p. 169. On the phenomenon of the consent of those concerned in the archives, cf. also a more theoretical perspective of Todd, M. (2006). Power, Identity, Integrity, Authenticity, and the Archives: A Comparative Study of the Application of Archival Methodologies to Contemporary Privacy. *Archivaria*, 61 (Spring), 181–214.

public authority, the citizen has not automatically consented to their use in absolute terms and in other contexts. And this is particularly true to the use of personal data maintained in archives for various research purposes. It is obvious that if the person concerned knew that their personal data would be further processed and disclosed to third parties in different contexts, they would very likely not have given their general consent to such use.

Thus formed specific need to open access and, at the same time, the not initially granted explicit consent to the collection of personal data and their use for other purposes (usually by researchers in the archives), together with the very frequent impossibility of obtaining and granting additional consent of the persons concerned to the disclosure of their personal data open an allegorical gateway to the wide field in which the whole multi-layered process of personality and privacy protection in the archives takes place.

2.1 European Court of Human Rights: Archives, Privacy, and the Right to Be Forgotten

The European Court of Human Rights (ECHR), as the European court responsible for interpreting the European Convention on Human Rights and examining violations thereof, is of particular relevance to the subject of this book especially with regard to Article 8, "Right to respect for private and family life", and Article 10, "Freedom of expression". In this respect, the ECHR plays an important role in interpreting the relationship between archives and data protection, including the protection of personal data of living persons, the right to be forgotten, and with it the freedom of expression and the right of access to information.[3] In its judgements in recent years and quite recently, the Court has emphasised that data administrators in particular must carefully implement a multi-faceted balancing of the right to be forgotten against the right to freedom of expression. Let us take a brief look at some of the cases the ECHR has dealt with in this area.

To begin with, it should be noted that already in 2009, the ECHR expressed its support for wide and unrestricted access to information, and

[3] A continuously updated summary and interpretation of the most important case law of the European Court of Human Rights on the subject of data protection is published by the Court as the European Court of Human Rights. (2021). *Guide to the Case-Law of the European Court of Human Rights: Data protection*. Updated on 31 December 2021. https://www.echr.coe.int/Documents/Guide_Data_protection_ENG.pdf

freedom of expression in the sense of the European Convention on Human Rights.[4] When it comes to archiving, the ECHR comments greatly on cases regarding internet archives, especially media archives, and to a lesser extent on traditional, printed, and analogue materials. This fact is not surprising and the reason is distinctly provided in the ECHR case law: "Internet sites are an information and communication tool particularly distinct from the printed media, especially as regards the capacity to store and transmit information, and that the risk of harm posed by content and communications on the Internet to the exercise and enjoyment of human rights and freedoms, particularly the right to respect for private life, is certainly higher than that posed by printed publication".[5]

On the issue of online storage of personal data for journalistic purposes, the ECHR has in several cases stressed the "substantial contribution made by Internet archives to preserving and making available news and information. Such archives constitute an important source for education and historical research, particularly as they are readily accessible to the public and are generally free."[6] In one such case two people convicted of murder on their release after 14 years in prison unsuccessfully asked newspaper web archives to remove all their information, including the photographs and their identification. They invoked the right to start a new life in the public space. The Court mentioned in particular the right to erasure ("right to be forgotten"). In the cited judgement M.L. and W.W. v. Germany (2018), in the context of media web archives the court did admit that the data subject may claim the right to erasure, at the same time it stressed that this right is not absolute and that "it must be balanced against the general

[4] Kenedi v. Hungary (Application no. 31475/05). Judgment. Strasbourg. 26 May 2009; European Convention on Human Rights of 4 November 1950 as amended by Protocols Nos. 11 and 14 supplemented by Protocols Nos. 1, 4, 6, 7, 12, 13 and 16. https://www.echr.coe.int/documents/convention_eng.pdf

[5] Hurbain v. Belgium (Application no. 57292/16). Judgment. Strasbourg. 22 June 2021. https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-210884%22]}

[6] Times Newspapers Ltd. v. the United Kingdom (nos. 1 and 2) (Applications nos. 3002/03 and 23,676/03). Judgment. Strasbourg. 10 March 2009, §§ 27 and 45. https://hudoc.echr.coe.int/eng#{%22languageisocode%22:[%22ENG%22],%22appno%22:[%223002/03%22,%2223676/03%22],%22documentcollectionid2%22:[%22CHAMBER%22],%22itemid%22:[%22001-91706%22]}; Węgrzynowski and Smolczewski v. Poland (Application no. 33846/07), Judgment. Strasbourg. 16 July 2013, § 59. https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-122365%22]}; M.L. and W.W. v. Germany (Applications nos. 60,798/10 and 65,599/10). Judgment. Strasbourg. 28 June 2018 § 90. https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-184438%22]}.

public's right to be informed of past events and about contemporary history, particularly by means of press digital archives".[7] The judgement is particularly linked to the press and its role in preserving archival materials of a journalistic nature, especially in the online space. On the one hand, the ECHR refers in principle to the public right to information, on the other hand, it underlines the need of a balancing act. In this context, the court mentioned that it is really necessary to distinguish whether the call for data erasure "concerned the original publisher of the information, whose activity was generally at the heart of what freedom of expression was intended to protect, or a search engine whose main interest was not in publishing the initial information about the person concerned, but in particular in facilitating identification of any available information on that person and establishing a profile of him or her".[8]

The ECHR has also granted citizens the right to be forgotten in other contexts, including in relation to the preservation of data in archives. One of these cases was the case of Segerstedt-Wiberg and Others v. Sweden in 2006. In this case, the issue was whether the state authorities were entitled to keep data on an individual's participation in a political rally, including sensitive personal data such as membership in a particular political party, for a long period of time, or to permanently archive it. In its judgement, the ECHR pointed out that the reasons that led to the initial collection and retention of data on the individual in this case by the security forces do not automatically justify permanent retention or archiving of such data. The original reasons for protecting national security that justified the original acquisition and retention of the personal data may or may not have the same relevance 30 years later. The Court acknowledged that a continued storage of the information in relation to certain persons "entailed a disproportionate interference with their right to respect for private life".[9]

In other judgements, the ECHR has, in different contexts, established the right of citizens to know what personal data are collected about them by different authorities. Specifically in relation to archiving, the ECHR

[7] European Court of Human Rights, *Guide to the Case-Law of the European Court of Human Rights*, p. 63.

[8] European Court of Human Rights, *Guide to the Case-Law of the European Court of Human Rights*, p. 87.

[9] Segerstedt-Wiberg and Others v. Sweden (Application no. 62332/00). Judgment. Strasbourg. 6 June 2006, § 90. https://hudoc.echr.coe.int/eng#{%22languageisocode%22:[%22ENG%22],%22appno%22:[%2262332/00%22],%22documentcollectionid2%22:[%22CHAMBER%22],%22itemid%22:[%22001-75591%22]}

ruled that citizens have the right to know what information about them was collected by the former security forces and secret services during the period of totalitarian regimes and what information is stored in state archives.[10] In other cases, the ECHR has recognised this right of citizens in relation to health information in order to understand their childhood and early development or, for example, to research their origin, in particular the identity of their parents.[11]

A very important ECHR judgement was delivered in Axel Springer AG v. Germany (2012). In this case, the ECHR outlined and summarised six criteria to be considered when conducting a balancing exercise between the right to freedom of expression and the right to respect for private life.[12] They are the following: contribution to a debate of general interest; how well known is the person concerned and what is the subject of the report; prior conduct of the person concerned; method of obtaining the information and its veracity; content, form, and consequences of the publication; severity of the sanction imposed.

The ECHR referred to this set of criteria and the cited judgement in its very recent judgement in the case of Hurbain v. Belgium (2021). Belgian courts have ordered the Belgian daily newspaper *Le Soir* to anonymise the name of the driver who caused an accident resulting in the death of two people. The person responsible for the accident invoked the right to be forgotten, his efforts to re-enter society and civic life after the sentence, and the damage to his medical practice by allowing his patients to look up his name in connection with the accident. *Le Soir*, on the other hand, argued for the right to freedom of expression. The ECHR conducted a balancing exercise which resulted in the confirmation of the verdict of the Belgian courts. At the same time, however, the ECHR stressed that this

[10] Haralambie v. Romania (Application no. 21737/03). Judgment. Strasbourg. 27 October 2009, § 79. https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-95302%22]}; Jarnea v. Romania (Application no. 41838/05). Judgment. Strasbourg. 19 July 2011, § 50. https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-105705%22]}; Joanna Szulc v. Poland (Application no. 43932/08). Judgment. Strasbourg. 13 November 2012, § 87. https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-114520%22]}.

[11] See European Court of Human Rights, *Guide to the Case-Law of the European Court of Human Rights*, pp. 58–59.

[12] Axel Springer AG v. Germany (Application no. 39954/08), 7 February 2012, §§ 88–95. https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-109034%22]}.

verdict does not mean that media should systematically and constantly search their archives and carry out balancing exercises. "Without prejudice to their duty to respect private life at the time of the initial publication of an article, when it comes to archiving the article they are required to carry out a check, and thus weigh the rights at stake, only if they receive an express request to that effect."[13]

This ECHR verdict has raised serious concern among a number of human rights organisations, journalists, media outlets, universities, and other entities. Some of them, in a summary response to the cited judgement, point out that in situations when it is necessary to balance between the right to freedom of expression and the right to protection of private life "the permanent removal of information from the media archive in the digital form is not a proportionate restriction on freedom of expression and will have a deleterious impact on the integrity of that archive. … The weight of the right to freedom of expression under Article 10 is not diminished by the passing of time."[14]

The cited ECHR case law, however, is for the most part primarily related to persons who are still alive. However, the absolute majority of the material preserved in the archives relates to people already deceased. For this reason we must pay special attention to post-mortem protection of personality and privacy. In recent years, the first research and studies on post-mortem protection of personality and privacy have begun to emerge, but their scope is limited to the perspective of the common law, or law in the field of general protection of personality, privacy, and other personality rights, and does not include the specific level of archival legislation and practice of processing and protection of personal data maintained in

[13] Hurbain v. Belgium.

[14] In the European Court of Human Rights. Application No. 57292/16 between Hurbain and Belgium. Written Comments of Article 19: Global Campaign for Free Expression, Centre for Democracy and Rule of Law, Prof. David Kaye, Digital Security Lab Ukraine, Electronic Frontier Foundation, The European Centre for Press & Media Freedom, Guardian News Media Limited, The Helsinki Foundation for Human Rights, The Human Rights Centre of Ghent University, The Hungarian Civil Liberties Union, International Press Institute, Times Newspapers Ltd., Mass Media Defence Centre, Media Defence, Nyugat, Open Net Association. 21 January 2022. http://www.concernedhistorians.org/content_files/file/le/731.pdf

archives. This handicap has implications in some cases on the not entirely correct interpretation of the overall setup of post-mortem protection of personal data, personality, and privacy in individual legal systems. Indeed, in many cases, it is archival legislation that implements post-mortem protection where the legislation regulating the protection of personal data explicitly limits its reach solely to living persons. In this respect, the aim of this text is to show, based on several illustrative examples from some countries, how archival legislation can complement the scope of law regulating the field of post-mortem protection.

2.2 Post-mortem Personality Protection from a Common Law Perspective and in International Comparison

László Majtényi, former Hungarian ombudsman and unsuccessful opposition candidate for president in Hungary in the 2017 presidential elections, introduced the following metaphor[15]: The essence of human existence does not cease with the biological end of man. We can imagine man as a comet in space. The solid core of the comet is the human essence of a living being, while the tail of the comet represents the personality that a man leaves behind even after their death. As time passes, the remnants of the personality become less and less attached to the human being of the deceased, just as the tail of the comet disappears into the darkness of the universe. "Individual uniqueness, or if you prefer, unique personality, does not disappear with death", writes Székely.

Post-mortem rights, and in particular post-mortem privacy and personality protection (not only) in relation to materials maintained in archives, represent a relatively young area of rights that is undergoing continuous development and transformation in a number of countries and is gaining increasing research interest. For archives, this is a level of rights that affects them deeply. The reason is obvious: The vast majority of records in the archives contain data—including very sensitive data—relating to deceased persons. In addition, the percentage of materials related to deceased persons in relation to records containing data on living people will gradually

[15] As cited in Székely, I. (2017). Does It Matter Where You Die? Chances of Post-Mortem Privacy in Europe and in the United States. In D. J. B. Svantesson, D. Kloza (Eds.), *Trans-Atlantic Data Privacy Relations as a Challenge for Democracy* (pp. 313–320). Intersentia, p. 313.

increase proportionally to the ever-increasing archival acquisitions and "ageing" of records, including those concerned in them. This trend would only change if archives resorted to massive reductions of once archived records. This is not yet on the horizon in developed democracies. One of the pillars of archival thinking and archiving has long been based on the assumption that records maintained in the archives are kept permanently and "for good". And usually archival legislation does not provide for that either. Although it is not inconceivable that one day this too will be placed on the scales in the context of thinking about the indefinite, permanent preservation of archival wealth.

A definition of post-mortem privacy was given, for example, by Lilian Edwards together with Edina Harbinja, a researcher working extensively in the field of post-mortem privacy protection, especially with regard to the digital world: "the right of a person to preserve and control what becomes of his or her reputation, dignity, integrity, secrets or memory after death".[16] Asta Tūbaitė-Stalauskienė, a lawyer and linguist at the Court of Justice of the European Union, also relies on this definition. Another possible definition was provided by Antoon de Baets, a prominent Belgian historian specialising in the ethics of historical research, censorship, and access to records and historical sources, in his "Declaration of the Responsibilities of Present Generations towards Past Generations": "Given that the dead are former human beings, posthumous dignity is not the same as the human dignity of the living, but it is still closely related. Human dignity is an appeal to respect the actual humanity of the living and the very foundation of their human rights; posthumous dignity is an appeal to respect the past humanity of the dead and the very foundation for the responsibilities of the living."[17]

Of course the rights of the living and the deceased in common or continental law are not equal. The essential question is what rights are transferable and enforceable even after the death of the person concerned. Usually, in legal systems, the distinction between two categories of rights plays a fundamental role in the exercise of the rights of the deceased: (1) economic rights and property rights; (2) personality rights, including the set of rights related to personality (dignity, good name, reputation,

[16] Edwards, L., Harbinja, E. (2013). Protecting Post-Mortem Privacy: Reconsidering the Privacy Interests of the Deceased in a Digital World. *Cardozo Arts & Entertainment Law Journal*, 32(1), 83–130, p. 85; Tūbaitė-Stalauskienė, A. (2018). Data Protection Post-Mortem. *International Comparative Jurisprudence*, 4(2), 97–104, p. 97.

[17] De Baets, A. (2004). A Declaration of the Responsibilities of Present Generations toward Past Generations. *History & Theory*, 43(4), 130–164, p. 136.

informational self-determination, etc.). While the transferability of economic rights of the deceased is generally accepted, as manifested in particular in the law of succession and freedom of testation, copyright, and so on, there are considerable differences in personality rights.

As Edwards and Harbinja accurately summarise, the system of common law follows the basic principle of *actio personalis moritur cum persona*, that is, that personal claims die with the person.[18] To date, the prevailing notion in the common law is that, unlike economic claims passed on to the descendants of the deceased, the damaged dignity and reputation are of no significance for the deceased. The very concept of "personality rights", as the authors summarise, is not recognised as a terminus technicus in common law. Rather, the common law includes certain acts and offences protecting certain aspects of personality, such as misappropriation of a name, breach of confidentiality and the like, which will be addressed in more detail later in Chap. 3. Overall, however—Edwards and Harbinja conclude—there is little support for post-mortem privacy, either in the United Kingdom, in the USA, or in other countries observing the common law.[19] In a nutshell: protect the property, not the privacy of the deceased.

In the USA, privacy protection today only applies to living persons. FOIA exemptions,[20] in the form of unwarranted invasion of personal privacy (exemptions 6 and 7) apply to living persons.[21] When it comes to privacy and sensitive personal data of deceased persons, they are only taken into account in principle if their violation would unduly infringe the privacy of the surviving family, that is, living persons. The term "survivor privacy" is sometimes used in the USA.

A prime example was the case of the New York Times Co. v. NASA and the court's decision to refuse to release a recording of the last words of the Challenger astronauts just before their deaths caused by the 1986 space shuttle explosion on the grounds that releasing their last words would

[18] Edwards, L., Harbinja, E. (2013). Protecting Post-Mortem Privacy, pp. 102, 119. For further reference to case law and literature the authors build on, ibid. The principle has its roots in the judgement Baker v. Bolton and others: KBD 8 Dec 1808. EWCC J38, [1808] EWHC KB J92, (1808) 1 Camp 493, 170 ER 1033.

[19] Edwards, L., Harbinja, E. (2013). Protecting Post-Mortem Privacy, p. 121.

[20] Freedom of Information Act, 5 United States Code (U.S.C.) § 552 (b) (6) and (7). https://www.govinfo.gov/app/details/USCODE-2011-title5/USCODE-2011-title5-partI-chap5-subchapII-sec552

[21] Including references to case law, see FOIA Update. (1982). FOIA Counselor: Questions & Answers, Vol. III, No. 4. https://www.justice.gov/oip/blog/foia-update-foia-counselor-questions-answers-24

cause pain to the surviving family.[22] Another analogous case, already involving the National Archives and Records Administration (NARA), concerned a request for disclosure of photographs of the dead body of Vincent Foster Jr., Deputy White House Counsel in the Bill Clinton administration.[23] The US Supreme Court refused to disclose the photographs to attorney Allan Favish, stating that "FOIA recognizes surviving family members' rights to personal privacy with respect to their close relative's death-scene images".

At the same time, the Supreme Court emphasised that if there is a right to privacy, there must be a public interest in disclosing the data, and "the requester must establish more than a bare suspicion in order to obtain disclosure. Rather, the requester must produce evidence that would warrant a belief by a reasonable person in the alleged Government impropriety." The Supreme Court also commented on the term "unwarranted invasion of personal privacy" as it is used in FOIA. "The term 'unwarranted' requires us to balance the family's privacy interest against the public interest in disclosure." We are thus faced with an approach very similar to British law at the level of the public interest test, which will receive detailed attention in Chap. 3.

Directly in relation to the deceased, personality is protected only in the case of appropriation of a name or likeness.[24] In Nelson v. Times (1977),[25] the Court summarised the essential reasoning for this approach, which, in principle, with certain exceptions discussed above, does not accept post-mortem protection of the personality rights of the deceased: First, allowing relatives to sue in cases of invasion of privacy of the deceased open room for unfounded actions or actions based on a purely emotional basis. Second, "if actions for violating the right of privacy were allowed by other than the person directly involved, fixing their boundaries and parameters would become an almost impossible task".

The situation is different in, at least some, countries observing continental law. As of 2014, Damien McCallig counted a total of 12 EU countries where some independent rights are granted to the deceased, namely Bulgaria,

[22] New York Times Co. v. NASA. 782 F. Supp. 628 (D.D.C. 1991). 12 December 1991. https://law.justia.com/cases/federal/district-courts/FSupp/782/628/2186506/

[23] National Archives and Records Administration v. Favish. 541 U.S. 157 (2004). https://supreme.justia.com/cases/federal/us/541/157/

[24] Restatement of the Law, Second, Torts, § 652.

[25] Lorraine Nelson et al. v. Maine Times. 373 A.2d 1221 (1977). Supreme Judicial Court of Maine. 3 June 1977. https://law.justia.com/cases/maine/supreme-court/1977/373-a-2d-1221-0.html. For US case law confirming this concept cf. also, for example, Hendrickson v. California Newspapers. 16 April 1975. Inc. 48 Cal.App.3d 59 (Cal. Ct. App. 1975). https://casetext.com/case/hendrickson-v-california-newspapers-inc.

Czech Republic, Denmark, Estonia, France, Italy, Latvia, Lithuania, Portugal, Slovakia, Slovenia, and Spain, of which ten countries (Czech Republic, Denmark, France, Italy, Latvia, Lithuania, Portugal, Slovakia, Slovenia, Spain) required that there be a link to the living person when exercising the rights of the deceased. Estonia imposed a period of 30 years.[26] McCallig's calculations, however, are inaccurate; for example, he forgot to mention Germany as one of the countries where the protection of the personality of the deceased is applied and plays a very important role compared to other countries as will be shown below in the analysis of several specific cases of post-mortal protection of personality rights in relation to archival records and the processing of personal data in the German archival system.

However, at the level of the European Union as such, post-mortem personality protection is not well developed. The European General Data Protection Regulation (GDPR) explicitly declares that its scope does not extend to the personal data of deceased persons.[27] Also, the case law of the European Court of Human Rights relating to violations of the European Convention on Human Rights apart from some very limited exemptions, does not accept post-mortem protection of personality rights and the transferability of personality rights of the deceased. An illustrative example can be seen in the recent dismissal of a complaint filed by Stalin's grandson, Yevgeny Yakovlevich Dzhugashvili, against the article "Beria found guilty", published in the opposition newspaper *Novaya Gazeta*, in which Stalin and Beria are held responsible for, among other things, the Katyn massacre. The alleged defamation of his grandfather was rejected by the court on the grounds that Article 8 of the European Convention on Human Rights, the right to respect for family and private life, is not transferable.[28] The court also declares the

[26] McCallig, D. (2014). Data protection and the deceased in the EU. Paper presented at the Computers Privacy Data Protection. Brussels 2014. As cited in: Buitelaar, J. C. (2017). Post-mortem privacy and informational self-determination. *Ethics and Information Technology*, 19, 129–142, p. 135.

[27] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Rec. 27. https://eur-lex.europa.eu/eli/reg/2016/679/oj

[28] Yevgeniy Yakovlevich Dzhugashvili against Russia (Application no. 41123/10). The European Court of Human Rights (First Section). Decision. 9 December 2014, §§ 22–24. Conclusion in Article 24: "The Court does not find sufficient reasons to depart from its established case law in the instant case. It follows that the applicant does not have the legal standing to rely on his grandfather's rights under Article 8 of the Convention because of their non-transferable nature." https://hudoc.echr.coe.int/eng?i=001-150568#{%22itemid%22:[%22001-150568%22]}.

applicability of this right to living persons in its official methodology interpreting Article 8, although to a certain and very limited extent it considers the applicability of this right to deceased persons, namely, for example, expressing respect for a deceased relative at their grave or the right to attend a funeral.[29] Thus, although interpretations pointing out that the European Convention on Human Rights cannot be limited to living persons, as, for example, J. C. Buitelaar does,[30] are not incorrect, it should be borne in mind that the European Convention on Human Rights provides only the very scope of recognition of personality rights of deceased persons and their transferability.

Likewise, another international convention important for Europe, drawn up by the Council of Europe in 1981, gradually signed and ratified by all member states of the Council of Europe and currently amended, the Convention on the Protection of Individuals with regard to the Automatic Processing of Personal Data, in its amended form, the so-called Convention 108+, limits its scope to living persons, as explicitly stated in its explanatory memorandum.[31] Buitelaar,[32] with reference to McCallig, therefore wrongly evokes the impression that the Convention may also apply to deceased persons.

If we look at international conventions with a global reach, the Universal Declaration of Human Rights (1948) prohibits arbitrary interference with one's private life, family, home or correspondence, and attacks upon their honour and reputation.[33] None of its provisions mention the right of

[29] European Court of Human Rights, Guide on Article 8 of the European Convention on Human Rights. Right to respect for private and family life, home and correspondence. Updated on 31 August 2021. https://www.echr.coe.int/documents/guide_art_8_eng.pdf, Sec. 150–157. On the development of the European Court of Human Rights case law in recent years in relation to the application of Article 8 to deceased persons, see also, Valeska D. (2016, 8 February). Insulting a politician right after her death: Does the ECHR protect the reputation of the deceased? *Strasbourg Observers*. https://strasbourgobservers.com/2016/02/08/insulting-a-politician-right-after-her-death-does-the-echr-protect-the-reputation-of-the-deceased/#_ftn1

[30] Buitelaar, J. C. (2017). Post-mortem privacy and informational self-determination. *Ethics and Information Technology*, 19, 129–142, p. 131.

[31] Convention 108+. Convention for the protection of individuals with regard to the processing of personal data from 28 January 1981. See Explanatory Report Art. 3, § 30: "The Convention applies to living individuals: it is not meant to apply to personal data relating to deceased persons". https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1

[32] Buitelaar, J. C. (2017). Post-mortem privacy and informational self-determination, p. 135.

[33] Universal Declaration of Human Rights (UDHR) of 10 December 1948, Art. 12. https://www.un.org/en/about-us/universal-declaration-of-human-rights

post-mortem protection or the rights of deceased persons. The original intention to aim the Declaration towards living persons is clear from the entire text. The same provisions and orientation towards living persons apply to the International Covenant on Civil and Political Rights (1966).[34]

The question is what the future development of post-mortem personality protection will look like in countries applying both continental and Anglo-American law. Edina Harbinja made an interesting observation. In recent developments in European legislation, particularly with regard to some features of the European GDPR, she observes a significant change in the understanding of data protection, which is no longer just a rights-based term, but personal data are understood much more as property with economic significance. She is undeniably right, as evidenced by the growing number of cases of misuse of personal data for economic as well as political purposes, the most prominent example in recent years being the Cambridge Analytica and Facebook case, which ended with the then maximum possible fine of £500,000 imposed on Facebook by the UK Information Commissioner's Office (ICO) in 2018 and the highest ever fine of $5 billion for misuse of personal data imposed on Facebook by the Federal Trade Commission in the USA in 2019. Harbinja sees this trend to view personal data increasingly as a commercial commodity and economically exploitable material rather than as part of a personality and protected human rights as the main reason that personality rights of the deceased will be marginalised in the future.[35]

There are also some other clear signals that seem to suggest that personality rights in continental law in European countries will not spread further towards the deceased. The explanatory memorandum to the amended text of Convention 108+ explicitly states that it applies only to living persons. Similarly, the 2016 GDPR clearly limits its reach solely to living persons and, finally, the European Court of Human Rights has interpreted the European Convention on Human Rights to concern only living persons, with some qualified exemptions, and very significantly limits the transferability of personality rights of the deceased.

However, if we remain in Europe, the scope for the application of the protection of the personality and privacy of the deceased still remains with

[34] International Covenant on Civil and Political Rights (ICCPR) of 19 December 1966, Art. 17. https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

[35] Edwards, L., Harbinja, E. (2013). Protecting Post-Mortem Privacy, p. 121.

the individual national legislations of the Member States of the European Union. Germany is one of the countries that respects such protection in some form, but the conclusions on the strength and scope of German personality protection made by Edwards and Harbinja (2013), which are taken over by Székely (2017) and Tūbaitė-Stalauskienė (2018), are not accurate. To illustrate, let us use the following section to take a closer look at the situation in Germany and at some cases of what post-mortem and pre-mortem personality protection may look like in relation to data and materials maintained in archives.

2.3 Germany and Protection of "Legitimate Interests of Data Subjects" ("Schutzwürdige Belange")

At a general level, the protection of personality is addressed by the German constitution, which explicitly mentions certain general personality rights. These include, for example, the right to preserve one's dignity and honour, but also, for example, the free development of personality.[36] In fact, the German Federal Constitutional Court (Bundesverfassungsgericht), in its 1983 judgement known as the "Census Act Judgement" ("Volkszählungsurteil"), derived the newly formulated fundamental right to the so-called information self-determination from the right to free development of personality.[37] Although this right applies only to living persons, the Federal Constitutional Court had already in the early 1970s derived the existence of post-mortem personality protection from the same constitutionally guaranteed right to free development of personality, together with inviolability of human dignity.[38] The German Federal Court of Justice (Bundesgerichtshof) presupposes it in its case law as early as the late 1960s. At the same time, however, this judgement of the Federal Court of Justice had already stipulated that post-mortem personality

[36] Grundgesetz für die Bundesrepublik Deutschland (Grundgesetz für die Bundesrepublik Deutschland in der im Bundesgesetzblatt Teil III, Gliederungsnummer 100-1, veröffentlichten bereinigten Fassung, das zuletzt durch Artikel 1 des Gesetzes vom 15. November 2019 (BGBl. I S. 1546) geändert worden ist), Art. 1, 2.

[37] Urteil des Ersten Senats vom 15. Dezember 1983 auf die mündliche Verhandlung vom 18. und 19. Oktober 1983. BVerfGE 65, 1. https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/1983/12/rs19831215_1bvr020983.html

[38] Bundesverfassungsgericht, Beschluss vom 24. February 1971, Az. 1 BvR 435/68 ("Mephisto").

protection is not "limitless".[39] The Court argued that only living persons potentially affected in relation to the deceased can assert the rights of the deceased. Yet, the need to protect the rights of the deceased "disappears as the memory of the deceased fades" ("schwindet gerade in Fällen der vorliegenden Art in dem Maße, in dem die Erinnerung an den Verstorbenen verblaßt"). Already at that time, the Court mentioned preserving the dignity of the deceased and "respect in the social sphere" ("die eigene Ehre des Verstorbenen in Gestalt eines fortbestehenden Achtungsanspruchs im sozialen Raum geschützt wird"), which was also reiterated by the Federal Constitutional Court in the cited 1971 "Mephisto" case resolution. In a similar vein, the Federal Constitutional Court also upheld post-mortem protection in its 2006 resolution (known as "Der blaue Engel"), in which, although it did not grant the deceased the same personality rights as living persons, it did grant them protection of memory of the dead, their dignity, and reiterated the right to respect in social space.[40] As regards the protection of the personality rights of the survivors, the case law of the Federal Constitutional Court emphasises that the interests of the survivors must be separately and individually harmed.[41]

In German law in general, in the field of personality protection, a model of personality spheres has crystallised over time based on the German Federal Court of Justice case law.[42] In principle, it is possible to distinguish two or three such spheres—social, private, and intimate. The data in the social sphere of a person include their public life and as such are generally accessible. The private sphere, which is sometimes

[39] "Auch ohne eine derartige gesetzgeberische Einzelregelung ist kein uferloser postmortalter Schutz des Lebensbildes zu befürchten." Bundesgerichtshof, Urteil vom 20. März 1968, I ZR 44/66. Cf. also, including references to case law, the discussion in Lübben, V. (2019). Stolperfallen im Netz. Postmortaler Persönlichkeitsschutz und die Belange von Hinterbliebenen. In I. Christa Becker, C. Rehm, U. Schäfer (Eds.), *Nicht nur Archivgesetze … Archivarinnen und Archivare auf schwankendem rechtlichem Boden? Best Practice – Kollisionen – Perspektiven. Beiträge zum 22. Archivwissenschaftlichen Kolloquium der Archivschule Marburg* (pp. 151–169). Archivschule Marburg, pp. 158–163.

[40] "Das allgemeine Persönlichkeitsrecht wirke nicht über den Tod hinaus. Geschützt seien nur das Andenken an den und die Menschenwürde des Verstorbenen. Das postmortale Persönlichkeitsrecht erfasse nur den Achtungsanspruch des Verstorbenen im sozialen Raum." Bundesverfassungsgericht, Beschluss der 1. Kammer des Ersten Senats vom 22. August 2006, 1 BvR 1168/04 ("Der blaue Engel").

[41] Bundesverfassungsgericht, Beschluss der 1. Kammer des Ersten Senats vom 19. Oktober 2006, 1 BvR 402/06.

[42] Cf. in particular Bundesverfassungsgericht. Beschluss des Zweiten Senats vom 14. September 1989, 2 BvR 1062/87.

distinguished from the intimate sphere, can be briefly summarised as the circle of family, close friends, or private life in one's own home.[43] It is possible to enter the private sphere in certain circumstances, but the principle of balance between the rights concerned must be respected. In addition to the private sphere, it is also possible to define an intimate sphere. This sphere is in essence inviolable and the principle of balance does not apply to it. Although this sphere has not yet been precisely defined by the German Federal Constitutional Court, it has recognised the existence of "an ultimate inviolable sphere of private life, which is absolutely separate from public power. Even serious interests of the general public cannot justify interventions in this sphere."[44] Referring to the German Constitution, the Federal Court found it crucial that "the core of personality is protected by the inviolable dignity of the human being".[45]

However, this text is primarily concerned with the application of personality rights, especially in the field of archiving and with the processing of data maintained in archives. The following text shall therefore detail several cases that have significantly affected the protection of personality rights in the German archival sector, both pre-mortem and post-mortem. I will illustrate the practice of personality protection in German archiving, controversial issues, and solutions that were eventually found. I will briefly introduce the so-called closure periods that serve as one of the instruments used to protect personality primarily in the field of archiving. The common denominator of all the analysed German cases is the specific category of the so-called legitimate interests of data subjects ("schutzwürdige Belange, schutzwürdige Interessen") concerned in the records and archives. Although the term is considerably vaguely defined, it plays an important role in German (not only archival) law and is decisive not only for pre-mortem but also for post-mortem personality protection.

[43] Cf., for example, Epping, V. (2010). *Grundrechte*. Springer, p. 273, Sec. 620.

[44] "Das Bundesverfassungsgericht erkennt jedoch einen letzten unantastbaren Bereich privater Lebensgestaltung an, der der öffentlichen Gewalt schlechthin entzogen … Selbst schwerwiegende Interessen der Allgemeinheit können Eingriffe in diesen Bereich nicht rechtfertigen; eine Abwägung nach Maßgabe des Verhältnismäßigkeitsgrundsatzes findet nicht statt." Bundesverfassungsgericht. Beschluss des Zweiten Senats vom 14. September 1989, 2 BvR 1062/87.

[45] "der Kern der Persönlichkeit durch die unantastbare Würde des Menschen geschützt wird." Bundesverfassungsgericht. Beschluss des Zweiten Senats vom 14. September 1989, 2 BvR 1062/87.

2.3.1 Klaus Kinski's Psychiatric History and Closure Periods for Access to Post-mortem Data

In 2008, the Landesarchiv Berlin (Berlin State Archive) released Klaus Kinski's medical records from 1950, when the actor was hospitalised for three days at the Karl-Bonhoeffer-Nervenklinik in Berlin.[46] The case soon became an infamous precedent throughout the entire German archival sector demonstrating how poor management of personal data in archives can look, and showing violation of basic principles of personality protection by archives as custodians of vast amounts of personal, including extremely sensitive, data of their citizens. What was this case about?

The Klaus Kinsky file was part of a larger set of medical records from the Karl-Bonhoeffer-Nervenklinik from the second half of the nineteenth century, Nazi Germany and the post-war period, which was transferred to the Landesarchiv in Berlin for archiving in 2008. The Landesarchiv Berlin, under the direction of Uwe Schaper, decided to disclose the file relying on the consent of the then Berlin Commissioner for Data Security and Freedom of Information, Alexander Dix. The argument was that patient files can be accessed 10 years after the death of the person concerned, which was fulfilled in this case (Klaus Kinski died in 1991). In German law, this period is based on general personality protection, in this case at the level of the general closure periods. Both the Federal Archives Act and the Berlin Archives Act (including the previous Berlin Archives Act in force at the time, and similarly in the federal acts of other German states[47]) stipulate that archives containing personal

[46] On the early days of this case cf., for example, Kotlorz, T. (2008, 22 July). Krankenakten werden möglicherweise wieder geschlossen. *Die Welt*. https://www.welt.de/regionales/berlin/article2240109/Krankenakten-werden-moeglicherweise-wieder-geschlossen.html. Further developments in the case are summarised, for example, in a report from the Institut für Urheber- und Medienrecht: Rechtsstreit um Krankenakte von Klaus Kinski endet mit Vergleich. (2009, 29 April). http://www.urheberrecht.org/news/3625/; Anker, J. (2009, 3 March). Klaus Kinskis Akten bleiben verschlossen. *Berliner Morgenpost*. https://www.morgenpost.de/berlin/article103914505/Klaus-Kinskis-Akten-bleiben-verschlossen.html; Heymann, N. (2009, 28 April). Kinskis Krankenakte soll für immer zu bleiben. *Der Tagesspiegel*. https://www.tagesspiegel.de/berlin/stadtleben/datenschutz-kinskis-krankenakte-soll-fuer-immer-zu-bleiben/1800012.html

[47] The claims of Vinzenz Lübben published in 2019 regarding the absence of such periods at the federal level are not correct. Cf. Lübben, V. (2019). Stolperfallen im Netz., p. 158. On closure periods in Germany, cf. Becker, I. Ch., Rehm C. (Eds.). (2017). *Archivrecht für die Praxis. Ein Handbuch*. MUR-Verlag, pp. 142–165.

data are to be disclosed to third parties—unless the person whose personal data are to be disclosed (or his or her next of kin) has consented to disclosure—at the earliest 10 years after their death. If the date of death cannot be established, both acts determine a period of 100 years after the birth of the persons concerned, and if this date cannot be established either, the Federal Archives Act stipulates a period of 60 years after the creation of the particular document, while the Berlin Archives Act determines an even longer period of 70 years after the creation of the document.[48] The length of closure periods, including the post-mortem ones, varies slightly in the individual German states, and special periods may apply to specific records, such as the archives of the former East German State Security Service, in which case the period applied to data on persons or third parties affected by the totalitarian regime of that time is 30 years after death, as will be shown below.

However, Klaus Kinski's widow and his son Nikolai filed a lawsuit due to the disclosure of Kinski's medical history on the grounds that private information had been violated under the German penal code.[49] The

[48] "Once the term of protection stipulated in (1) has expired, federal archive material whose purpose or essential content concerns one or more natural persons may only be used at least ten years after the death of the respective person. If their year of death cannot be established—or only with an unreasonable amount of time and effort—the term of protection shall expire 100 years after the birth of the persons concerned. If their birthday cannot be established either—or only with an unreasonable amount of time and effort—the term of protection shall expire 60 years after the creation of the documents." Bundesgesetz über die Sicherung, Aufbewahrung und Nutzung von Archivgut des Bundes (Bundesarchivgesetz) of 10 March 2017. BGBl. I s. 410. https://www.bundesarchiv.de/DE/Content/Artikel/Ueber-uns/Rechtsgrundlagen/rechtsgrundlagen_bundesarchivgesetz.html, § 11, Sec. 2. The Archives Act for the state of Berlin sets out the conditions as follows: "Archivgut, das sich seinem wesentlichen Inhalt nach auf eine natürliche Person bezieht (personenbezogenes Archivgut), darf unbeschadet des Absatzes 2 Dritten nur mit der Einwilligung der Betroffenen zugänglich gemacht werden. Nach dem Tode der Betroffenen bedarf die Benutzung des Archivgutes bis zum Ablauf von zehn Jahren der Einwilligung der Angehörigen […] Ist das Todesjahr der Betroffenen dem Landesarchiv Berlin nicht bekannt, so endet die Schutzfrist hundert Jahre nach der Geburt. Ist auch das Geburtsjahr dem Landesarchiv Berlin nicht bekannt, so endet die Schutzfrist siebzig Jahre nach der Entstehung der Unterlage. Die Schutzfrist gilt nicht für die Benutzung durch die Betroffenen oder ihre Angehörigen." Gesetz über die Sicherung und Benutzung von Archivgut des Landes Berlin (Archivgesetz des Landes Berlin), § 9, Sec. 3. Former Berlin Archives Act Gesetz über die Sicherung und Nutzung von Archivgut des Landes Berlin (Archivgesetz des Landes Berlin) of 29 November 1993. A comprehensive comparison of the wording of both acts is available online: http://landesarchiv-berlin.de/archivgesetz-des-landes-berlin-gegenueberstellung-der-gesetzestexte

[49] Strafgesetzbuch, § 203 (Verletzung von Privatgeheimnissen).

prosecutor's office then initiated proceedings against Uwe Schaper, but dropped them saying that although disclosure of the file had been unlawful, Schaper had not acted intentionally but out of ignorance of the law, relying on the opinion of the Commissioner for Data Security and Freedom of Information. However, the file was closed pending a further decision on the matter by the court. Legal proceedings initiated before the Berlin Administrative Court concluded in a conciliation agreement between Kinski's son Nikolai and the Landesarchiv Berlin. It reads that the Archive shall grant access to Kinski's file only when Nikolai Kinsky gives consent. Should the Archive want to disclose the material despite Kinsky's protest, the decision on the matter shall lie with the court (using the diction of the German Stasi Records Act[50]).

Of course, the archive should not have disclosed the (psychiatric) medical history of patients, whether it was Klaus Kinski or anyone else. This is primarily commanded by general tact, a sense of discretion, confidentiality, and the protection of the personality of those concerned in the archives. Archives should naturally apply this protection in a comprehensive assessment of whether or not to grant access to the requested records. The Landesarchiv Berlin had clearly not only violated this tact and discretion by disclosing Klaus Kinski's file, it had also violated the law. German legislation—federal as well as individual state archives acts and other related legislation—establishes a specific institute of the so-called legitimate interests of data subjects ("schutzwürdige Belange") whose personal data appear in records and archives. This institute obliges not only the Berlin Archive, but also other German archives together with the institutions that transfer their records to the archives, to respect and ensure the protection and care of the "legitimate interests" of the persons concerned in the—not only archival—records. These were already referred to in the previous Berlin Archives Act and are taken up in the current Act. While the Berlin Archives Act, as well as the Federal Archives Act, do indicate the above-mentioned general periods for the disclosure of archival records containing personal data (10 years after the death of the person concerned, etc.), they almost identically add further protective restrictions, especially

[50] Gesetz über die Unterlagen des Staatssicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik of 20 December 1991 (Stasi-Unterlagen-Gesetz). https://www.gesetze-im-internet.de/stug/

in situations when "there is reason to believe that disclosure is contrary to the legitimate interests of data subjects".[51]

Unlike closure periods, the duration of protection using the institute of "legitimate interests of data subjects" spans indefinitely after the death of the person concerned, as the law does not stipulate any specific time limits. That is the theory. In practice, however, the case law of the German courts, as we have seen above, has since the 1960s continuously referred to the factor of the "fading memory of the deceased" and, in view of this, it assumes the time-limited nature of post-mortem personality protection. However, no precise time limits are given, so it remains the responsibility of data controllers, including archives, to assess the sensitivity of the data and determine whether disclosure would harm the "legitimate interests" of individuals to such an extent that the data should remain withheld.

2.3.2 Victims of Nazi "Euthanasia" in Germany

Let the names of all the victims of the Nazi "euthanasia" programme be published on the web—to use a contemporary euphemism for the mass murder of people with physical or mental disabilities! This was one of the appeals made (most recently to archivists in Suhl in 2019) by Götz Aly, a well-known German historian, political scientist, and journalist.[52] The issue of access to archives, or rather the personal data of persons who were murdered by Nazi Germany in the "euthanasia" programme, is another prime example in the field of protecting the personality of those concerned in archival records. The development of this case, which has a long genealogy in Germany, is also remarkable. Let us now take a closer look at it.

A society-wide debate on the disclosure of data from the files of the Nazi "euthanasia" programme has been going on in Germany for several years. Some survivors of "euthanasia" victims, in particular, have opposed

[51] "Die Benutzung ist zu versagen oder einzuschränken, soweit Grund zu der Annahme besteht, dass schutzwürdige Belange Dritter entgegenstehen." Gesetz über die Sicherung und Benutzung von Archivgut des Landes Berlin (Archivgesetz des Landes Berlin), § 9, Sec. 9 (2). The same applies to the federal level: "The Federal Archives may restrict or deny use in accordance with the provisions set forth in §§ 10 to 12 if there is reason to believe that such usage is prevented by the legitimate interests of data subjects or their relatives". Bundesarchivgesetz, § 13, Sec. 1 (2).

[52] Aly, G. (2019). Seit 40 Jahren der Geschichte auf der Spur. Warum mich ein Archivbesuch glücklich macht. Conference contribution at: RECHTsicher—Archive und ihr rechtlicher Rahmen. 89. Deutscher Archivtag in Suhl.

and continue to oppose this step. Archives have traditionally applied the strict practice of withholding such materials (as I can attest from my own research experience on the example of archival fonds relating to the "euthanasia" programme maintained in the Landesarchiv Berlin), as has been confirmed by several court judgements. Gradually, however, voices from the other side have been raised, criticising the fact that the names of those murdered by the German Nazi regime under the "euthanasia" programme have not yet been published. Open access to these data was even required by means of a petition submitted to the German Bundestag. At the same time, a debate erupted over the publication of the book "Gedenkbuch für die Münchner Opfer der nationalsozialistischen 'Euthanasie'–Morde" (2018), in which the authors summarised and published the names of approximately 2000 Munich victims of Nazi "euthanasia".[53] In justifying the publication of their names, the authors state, among other things, that "the book pays homage to the victims by giving their names and details of their lives. The memory of those murdered will become part of the collective memory of the city of Munich after a long period of silence."[54] After all, the same publishing house, Wallstein Verlag, came up with another book on the subject, when it published a collection of stories of 23 victims of the "euthanasia" programme a decade earlier.[55] But debates also took place at the level of seminars and conferences. In 2016 a conference took place under the auspices of the Federal Government Commissioner for Culture and the Media, Monika Grütters; it was aptly titled "Giving the Victims a Name. Commemoration and data protection in connection with the public naming of Nazi victims in exhibitions, memorial books and databases."[56]

[53] Von Cranach, M., Eberle, A., Hohendorf, G., von Tiedemann, S. (2018). *Gedenkbuch für die Münchner Opfer der nationalsozialistischen „Euthanasie"-Morde*. Wallstein-Verlag.

[54] Cf. book annotation: https://www.wallstein-verlag.de/9783835332126-gedenkbuch-fuer-die-muenchner-opfer-der-nationalsozialistischen-euthanasie-morde.html

[55] Fuchs, P., Rotzoll, M., Müller, U., Richter, P., Hohendorf, G. (Eds.) (2007). *"Das Vergessen der Vernichtung ist Teil der Vernichtung selbst". Lebensgeschichten von Opfern der nationalsozialistischen "Euthanasie"*. Wallstein-Verlag.

[56] "Den Opfern einen Namen geben. Gedenken und Datenschutz im Zusammenhang mit der öffentlichen Nennung der Namen von NS-Opfern in Ausstellungen, Gedenkbüchern und Datenbanken." Eine Veranstaltung der Stiftung Denkmal für die ermordeten Juden Europas und der Stiftung Topographie des Terrors in Zusammenarbeit mit dem Bundesarchiv. Conference report by Roth, M. (2016, 29 June). Bericht zur Tagung "Den Opfern einen Namen geben." https://www.holocaustliteratur.de/deutsch/Den-Opfern-einen-Namen-geben-Gedenken-und-Datenschutz-im-Zusammenhang-mit-der-F6ffentlichen-Nennung-der-Namen-von-NS-Opfern-in-Ausstellungen2C-Gedenkbuechern-und-Datenbanken-2039/

When Götz Aly listed potential arguments against publishing the names of the "euthanasia" programme victims, he mentioned to German archivists what I would call a rather marginal reason that it might be embarrassing for some survivors to learn that their ancestor had been euthanised because of syphilis and the like. On the other hand, a much more relevant argument was presented by Axel Metz, archivist and head of the Würzburg City Archive. If the names of the victims are disclosed, a problem may arise if one of the persons murdered under the "euthanasia" programme had a hereditary disease. In such cases, disclosing the information about the health of the ancestors also has implications for the survivors. These effects are not only reflected at the level of protection of personality and reputation, but also on a quite practical level. Metz very rightly pointed out the possible risk of survivors intending to take out life insurance being subject to insurance companies screening and checking the databases of "euthanasia" victims for the health status of the ancestors of their potential clients. And this is not necessarily limited only to victims of "euthanasia". Metz reminds archives to be very careful as there might come a day when an insurance company makes a request to an archive for all the information concerning the health status of a person's ancestors (who are deceased, and therefore not subject to the standard personal data protection as a living person is), for the same purpose of checking the health status of their potential life insurance client. The same issue, that is, the risk of medical records containing information on hereditary diseases falling into the hands of health or other insurance companies, was also raised at the congress of German archivists in Suhl by Clemens Rehm, a well-known German expert on archival law from the Stuttgart archives. And indeed, American health insurance companies, for example, implement the well-known practice of examining and scrutinising the health status of their clients as thoroughly as possible for which they do not hesitate to use what could without any exaggeration be called detective methods. The institute of legitimate interests of data subjects that are covered in archival legislation and that make it possible to extend the usual length of closure periods, thus plays a very important role in civil society at this level as well.

But let us return to the case of the disclosure of the names of "euthanasia" victims in Germany; over the years the case progressed towards at least a certain disclosure of files relating to the "euthanasia"

programme. In 2014, Ehrhart Körting, a legal expert and former vice-president of the Constitutional Court of the State of Berlin, issued an expert opinion (not a court judgement) concluding that the disclosure of the names of victims of Nazi "euthanasia" programme, including their birth and death dates, did not violate the above-mentioned legitimate interests ("schutzwürdige Belange" Dritter/Betroffener) of the survivors in this case.[57] Körting's report was subsequently invoked by the German Federal Archives when it finally disclosed the names of the victims of the Nazi "euthanasia" programme, including some other information, such as the place of birth, the institution in which the victim was placed, the date of transport, and so on.[58] Of course, the archive did not grant access to the victims' files as such and the information they contain can only be accessed individually and is subject to many conditions.

2.3.3 Post-mortem Protection of Jewish Victims from the German Town of Minden and the Risk of Exposing Jewish Origin Under the Current Threat of Rising Anti-Semitism

Until recently, with regard to the subject of the Shoah, the names of the victims of Nazi extermination were usually revealed without further ado. Today, in the context of increasing anti-Semitic attacks across Europe, more and more questions and doubts are raised over the disclosure of personal data of Jewish victims.

In 2019, the World Jewish Congress commissioned a study and a survey on anti-Semitism in Germany. According to the conclusions of this study, as of 2019, 27% of the population in Germany is anti-Semitic, and as for the German elite (the study criteria included a university degree and

[57] Körting, E. (2014, 1 July). Namennennung von Opfern der NS Euthanasie von 1939 bis 1945. Expert opinion. https://www.gedenkort-t4.eu/sites/default/files/media/file/gutachten_namensnennung_copyright_erhart_koerting.pdf

[58] Database online at: https://www.bundesarchiv.de/DE/Content/Downloads/Aus-unserer-Arbeit/liste-patientenakten-euthanasie.pdf?__blob=publicationFile

an annual income above EUR 100,000), 18% are anti-Semitic.[59] At the same time, anti-Semitic violent attacks have been on the increase in Germany in recent years,[60] however, a similar development is also evident in other European countries. According to a survey conducted by the EU Agency for Fundamental Rights in 2018, a total of 39% of respondents said that they had experienced some form of anti-Semitic harassment in the last five years.[61]

In the context of the recent rise in anti-Semitism, the explosive nature of the question of whether to reveal the identities of citizens of Jewish origin, including those who have long since passed away, most often Jews murdered during WW2, is a growing concern. A prime example is the case of the disclosure of the personal data of people of Jewish origin from the German town of Minden and its vicinity in North Rhine-Westphalia. In 2013, the Minden municipal archives published a database containing personal data of citizens of Jewish origin, most of whom were murdered by Nazi Germany between 1939 and 1945; however, the database also included those not affected by the Holocaust.[62] The database can be used to trace—in some cases in detail—the dates and places of birth and death, home addresses, and movement of persons during their lifetime, place of emigration, if applicable and known, as well as other data.

Some of the survivors then contacted the Landesbeauftragte für den Datenschutz und die Informationsfreiheit Nordrhein-Westfalen (the State Commissioner for Data Protection and Freedom of Information of North

[59] The conclusions of the study were presented, for example, by Ronald S. Lauder, World Jewish Congress President, in his article Lauder, R. S. (2019, 25 October). In Birthplace of Nazism, "Never Again" Must Really Mean "Never Again". *Frankfurter Allgemeine Zeitung*. https://www.faz.net/aktuell/feuilleton/debatten/in-birthplace-of-nazism-never-again-must-really-mean-never-again-16449527.html?printPagedArticle=true#pageIndex_2. Statistics: https://de.statista.com/statistik/daten/studie/1041402/umfrage/umfrage-in-deutschland-zur-zustimmung-zu-antisemitischen-aussagen/

[60] The data is collected by the German Federal Ministry of the Interior. Statistics: https://de.statista.com/infografik/18013/antisemitische-gewalttaten-in-deutschland/

[61] European Union Agency for Fundamental Rights. (2018). *Experiences and perceptions of antisemitism. Second survey on discrimination and hate crime against Jews in the EU*. https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-experiences-and-perceptions-of-antisemitism-survey-summary_en.pdf, p. 9.

[62] Database "Jüdisches Leben in Minden und Umgebung" is currently partly published online: https://juedisches-leben.kommunalarchiv-minden.de/

Rhine-Westphalia) and opposed the publication of the database.[63] In 2015, the database was temporarily withdrawn pending clarification. In his opinion and without explicitly naming the Minden Municipal Archive, the Commissioner highlighted several problematic points or violations of the law.[64] He mentioned, inter alia, the lack of a legal basis for such disclosure, the lack of any restrictions limiting the use of the database to scientific purposes, the failure to take into account the "legitimate interests of data subjects", and violation of the right of the persons concerned to informational self-determination by failing to provide their consent to the disclosure of the data. He also brought up the possibility of using the context of the database to deduce data on living persons.

However, the case of the Minden database of the Jewish population was not over. In October 2015, representatives of several parties concerned, including the Jewish community, met with the mayor of Minden.[65] The conclusion of the meeting was clear: Work on the database should continue, including the publication of at least some of the data collected. The City of Minden approached the Commissioner for Data Security and Freedom of Information with a different position on the database. Eventually, in November 2016, a joint meeting was held and an agreement containing several points was reached. First, the database was renamed and instead of the potentially discriminatory "Mindener Juden" it now bears the name "Jüdisches Leben in Minden und Umgebung". Part of the collected data is presented publicly and the rest is used only for internal archival purposes. The database does not contain any data on living persons or data that might lead to such persons; this claim, however, is in my opinion not entirely substantiated. At the request of the next of kin of the persons concerned, data on their relatives shall be removed.

As demonstrated above with the examples of the archival records of the "euthanasia" programme in Nazi Germany or the regime's Jewish victims,

[63] Vinzenz Lübben summarises the development of this case as of 2018, Lübben, V. (2019). Stolperfallen im Netz, pp. 151–169.

[64] Landesbeauftragter für Datenschutz und Informationsfreiheit Nordrhein-Westfalen. (2015). *Zweiundzwanzigster Datenschutz- und Informationsfreiheitsbericht des Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen Ulrich Lepper für die Zeit vom 1. Januar 2013 bis zum 31. Dezember 2014.* https://www.ldi.nrw.de/system/files/media/document/file/22_dib.pdf, pp. 88–91.

[65] Lübben, V. (2019). Stolperfallen im Netz, pp. 167–168. Cf. Klaus Graf, K. (2018). Datenbank zum Jüdischen Leben in Minden wieder online. Published 30 January 2018. https://archivalia.hypotheses.org/70175

even the period of 80 years after the creation of the records together with the death of the persons concerned are insufficient and may not be enough to prevent legitimate concerns about the potential harm to personality rights by disclosing and publishing some of their data. Although German archival legislation currently explicitly allows for the disclosure of archival material and search tools, including digitisation instruments, archives must still respect the aforementioned principle of preserving the legitimate interests of individuals.[66]

There is no simple answer to the question of whether, in order to protect personality rights, including those of the deceased, some files should remain permanently closed, or whether they should be destroyed as the most reliable form of data protection. For example, the case law of the German Federal Court of Justice and the Federal Constitutional Court does not take this into account and the courts base their decisions on the principle of the data "disappearing sensitivity", which also manifests on the level of the "fading memory" of the deceased by their survivors, as we have seen above. Other legislations use this principle in a similar manner. For example, in the USA, the law gives the Archivist of the United States, that is, the head of NARA, the right to assess the sensitivity of data contained in federal-level archives that might potentially violate the privacy of living individuals and to disclose such data in case they decide that "enough time has passed that the privacy of living individuals is no longer compromised".[67]

Yet, there are national legislations that assume a certain form of permanent post-mortem personality protection; Australia can be used as such an example. The Australian Family Law Act prohibits the disclosure of information on identifiable persons from records used in family law proceedings.[68] Moreover, the Australia-wide general legislation regulating privacy and personal data protection in the country, unlike, for example, the European Union, does not explicitly limit its reach to living persons and does not stipulate a clear period after which privacy protection ceases to

[66] Bundesarchivgesetz, § 3 (1). Individual state archival laws contain similar provisions.

[67] 36 Code of Federal Regulations, § 1256.56. https://www.govinfo.gov/app/details/CFR-2011-title36-vol3/CFR-2011-title36-vol3-sec1256-56, (b) (1).

[68] Family Law Act 1975, No. 53, 1975, Compilation No. 88. https://www.legislation.gov.au/Details/C2019C00182, Sec. 121.

apply.[69] Yet, it should be added that some Australian states do in fact provide post-mortem protection milestones. For example, the definition of personal information in New South Wales does not include persons deceased for more than 30 years.[70] Any data about persons who died more than 30 years ago are no longer considered personal data. Tasmania limits the reach of personal data, and therefore their protection, to a slightly lesser extent, in this case to 25 years after a person's death.[71] The Northern Territory provides post-mortem protection of only five years, again by limiting the reach of the concept of personal data by defining the term "person" to five years after their death.[72]

However, the real question is, whether in some cases certain categories of records and information should remain withheld permanently. One example that can be mentioned are records of divorce court proceedings (which, incidentally, also fall within the Australian Family Law Act). They often contain very sensitive information that should without much doubt remain closed to the public eye. In the USA, access to information belonging to the category of divorce records has been addressed by Laura W. Morgan, who argued against the general accessibility of these files.[73] Another example, albeit more controversial and now increasingly criticised, is the practice in some countries of sealing closed

[69] Privacy Act 1988, No. 119, 1988. https://www.legislation.gov.au/Details/C2014C00076. For general privacy and data protection in Australia in relation to archiving, cf. Iacovino, L., Todd, M. (2007). The long-term preservation of identifiable personal data: a comparative archival perspective on privacy regulatory models in the European Union, Australia, Canada, and the United States. *Archival Science*, 7, 107–127. https://doi.org/10.1007/s10502-007-9055-5, pp. 122–124.

[70] Privacy and Personal Information Protection Act 1998, No. 133. https://legislation.nsw.gov.au/view/whole/html/inforce/current/act-1998-133, Sec. 4-3a.

[71] Personal Information Protection Act 2004 (Tas). https://www.legislation.tas.gov.au/view/html/inforce/current/act-2004-046, Sec. 3.

[72] Information Act 2002 (NT). https://legislation.nt.gov.au/en/Legislation/INFORMATION-ACT-2002, Sec. 4. and further 4A and 4B.

[73] Morgan, L. W. (2001). Strengthening the Lock on the Bedroom Door: The Case Against Access to Divorce Court Records On Line. *Journal of the American Academy of Matrimonial Lawyers*, 17, 45–67. https://cdn.ymaws.com/aaml.org/resource/collection/F5239802-0DED-4BAC-9F7E-AC93E2DB4D4D/strengthening_the_lock_on-17-1.pdf. Some US states implement closure periods for access to divorce records; among all the US states, the strictest divorce privacy protection is applied New York State where the period is 100 years. See Consolidated Laws of New York, Domestic Relations Law, Sec. 235. https://codes.findlaw.com/ny/domestic-relations-law/dom-sect-235.html

adoption records so that the link between the biological parents and their offspring cannot be traced.

Some archival legislative systems set infinite closure periods, or explicitly declare certain types of records as inaccessible and permanently withheld. However, such indefinite periods are imposed for categories of records concerning the production and use of nuclear, biological, or chemical weapons and other weapons of mass destruction, as is the case, for example, in the French archival system.[74] Germany also allows for archives to be permanently withheld. However, the justification uses a more general wording: At federal level, the Archives Act stipulates that access to archival records is denied (at any time, i.e., indefinitely) if "there is reason to believe that using these records would harm the well-being of the Federal Republic of Germany or one of its states".[75] Harm to the "well-being" of the state then includes such matters as internal and external security, relations with other states and international organisations, defence, civil protection, protection of the constitution, and so on. As the primary concern in these and similar cases is not the protection of personal data, personality, and privacy, I will not elaborate these reasons for permanently withholding records in any more detail. This issue, that is, in what respect should some archival records remain permanently inaccessible, whether archives should begin to include the data minimisation perspective in the specific process of archival appraisal, and whether they shall consider intentional and legal destruction of personal data before their transfer to the archives, will be covered in Chap. 8.

Let us conclude the summary of the situation concerning personality protection and disclosure of personal data in the German archival system by looking at specific material of the former East German State Security Service (Stasi), for which an independent archive had been established by law. The material in question contains extremely sensitive personal data and records that usually never see the light of the "public" day. In many respects this material corresponds to that still created today by intelligence

[74] Code du patrimoine [Heritage Code] of 20 February 2004, Sec. L213-2, item II. https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006074236/2022-06-06/

[75] "Grund zu der Annahme besteht, dass durch die Nutzung das Wohl der Bundesrepublik Deutschland oder eines ihrer Länder gefährdet würde." Bundesarchivgesetz, § 13 (1-1). For an interpretation of this provision cf. Becker, I. Ch., Rehm C. (Eds.). (2017). *Archivrecht für die Praxis. Ein Handbuch*, pp. 166–167.

services around the world, whose archives, with hardly any exception, remain completely and permanently closed to the public.

2.4 Archives of the Former East German State Security Service (Stasi): A Model for Applying the Concept of "Legitimate Interests" in Archival Practice—Purpose of Consultation, Interest of Science, and Privileged Access

Some of the problematic situations mentioned above, which archives face almost every day, show how difficult it is to protect those persons who have left their "imprint" in archival sources. The German or Austrian models attempt to address this issue in particular by introducing the concept of "legitimate interests" of data subjects. However, as shown above, this model can be characterised by considerable vagueness and legal uncertainty. This means that archives are left with a very wide range of options as to how to interpret the need to care for the "legitimate interests" of persons as embodied in archival sources and how to translate this need into the actual procedural settings of care for their protection.

One of the possible and at the same time very specific ways in which archives can deal with the issue of personality protection in archival records as well as the issue of vagueness of the term "legitimate interests", is the approach taken by the German archival sector and more specifically by the Stasi Records Archive (Stasi-Unterlagen-Archiv) in the case of access to a specific group of materials, namely the records of the former East German State Security Service (the Stasi).[76]

The Stasi Records Archive is now housed in one of the buildings of the giant complex of the former headquarters of the DDR Ministry for State Security (Ministerium für Staatssicherheit), the dreaded Stasi. What was originally a subtle single-structure headquarters in 1950, when the infamous ministry was established, grew into an extremely large and closed-to-the-public complex of 52 buildings that has significantly changed the

[76] The legal basis is the special Stasi Files Act (Stasi-Unterlagen-Gesetz). Among the many publications on the Stasi itself, cf. in particular the texts published by the office of Federal Commissioner for the Records of the State Security Service of the former German Democratic Republic (Bundesbeauftragte für die Stasi-Unterlagen der ehemaligen Deutschen Demokratischen Republik). For the Stasi in summary, see, for example, Gieseke, J. (Ed.). (2011). *Die Stasi 1945–1990*. Pantheon.

character of the entire Lichtenberg district in Berlin. At its peak, it housed 7000 employees out of a total of approximately 90,000 direct Stasi employees across the DDR. However, we must not forget the huge number of so-called unofficial collaborators, in German terminology referred to as "inoffizielle Mitarbeiter", abbreviated as "IM", which totalled approximately 189,000 by 1989 at the time of the end of the totalitarian East German regime.[77]

Note should also be made of the total number of Stasi employees at its headquarters. Among the records destroyed by the Stasi itself at the end of its existence were summary materials relating to the headquarters, including staff rosters. Estimates of the number of employees at the headquarters were thus made mainly on the basis of the number of buns baked (the Stasi headquarters had its own bakery) and consumed in a working day, taking into account the estimated average number of buns consumed by one person.

The Stasi Records Archive represents an atypical archive, especially as it manages the records of a very specific creator. It also stands out among other archives due to the extraordinary public interest in the records it maintains. Let us look at some general statistics.[78] The Stasi Records Archive, including the materials of the regional offices, keeps a total of 111 linear kilometres of archival material, of which approximately 40% is stored at the Berlin headquarters. Of the total 111 km preserved, 51 km were archived by the Stasi itself, while another 60 km were found disorganised in the offices of Stasi employees. These records were organised by the Stasi Records Archive and now about 91% of this number has been processed and made available. However, a rather special and unique part of the surviving documentation is the unprecedented number of records destroyed by the Stasi during the period of the collapsing regime, which

[77] For "unofficial collaborators" of the Stasi, including statistical estimates of their number, a figure on which German historians differ, cf. in particular the third part (devoted exclusively to statistics) of the three-volume Müller-Enbergs, H. (2012). *Inoffizielle Mitarbeiter des Ministeriums für Staatssicherheit. Teil 1: Richtlinien und Durchführungsbestimmungen*. Ch. Links; Müller-Enbergs, H. (2011). *Inoffizielle Mitarbeiter des Ministeriums für Staatssicherheit. Teil 2: Anleitungen für die Arbeit mit Agenten, Kundschaftern und Spionen in der Bundesrepublik Deutschland*. Ch. Links; Müller-Enbergs, H. (2008). *Inoffizielle Mitarbeiter des Ministeriums für Staatssicherheit. Teil 3: Statistiken*. Ch. Links. https://www.bstu.de/assets/bstu/de/Publikationen/E_Mueller-Enbergs_Inoffizielle_Teil3.pdf

[78] Cf. https://www.bstu.de/ueber-uns/bstu-in-zahlen/#c2391

were, however, preserved in the form of shredded fragments and which the archive has been working on restoring for a long time.

Since the beginning of the archive existence in 1990, as of 30 June 2019, a staggering 7,263,501 requests have been addressed to the archive for consultation or access to its archival records, of which 3,282,078 were made by citizens! This represents an average of over 100,000 requests from citizens per year and a total of about 240,000 requests per calendar year. The Stasi Records Archive is also able to provide data on the development of research interest. While in 2011 and 2012 there were still over 80,000 requests from citizens, in 2013–2015 the numbers were between 60,000 and 70,000 and in 2016–2018 the numbers dropped to about 45,000–49,000 requests. These astonishing figures, however, correspond with the similarly surprising total number of Stasi Records Archive employees of totalling 1440 at the headquarters and including branches (as of 1 January 2019)!

A characteristic feature of the access to Stasi archival records is the high specificity of the rules of access to archives maintained in the Stasi Records Archive as well as the complexity of the aspects taken into account when deciding on granting access to Stasi material. Although closure periods are one of the tools used in the process of opening access to Stasi records, the whole system is primarily built on the consideration of several levels. The first aspect is the person of the researcher requesting access to the archival records (= "for whom the archives are intended"). The second aspect considers the category of persons concerned in the archives, that is, whether they are victims of the regime, Stasi employees, and so on (= "who the archives concern"). Other aspects are also considered. These include in particular the purpose of consultation, that is, whether it is for personal use, research purposes, media, and so on. But the considerations also look into how the information obtained will be further used by the researcher (scholarly publication or another professional output, publication in the media, personal use only, etc.). One more very specific criterion is also taken into account, namely how the information contained in the archives was obtained.

The last aspect concerning the manner in which the information was obtained by the record creator, that is, in this case the Stasi, rarely appears in the practice of granting access to archives. This shows the specific nature of the Stasi, which served both as a secret state police and as an intelligence service with internal as well as external operations. As such, it obtained and collected data (not only) on the citizens of the former DDR,

including highly sensitive data. Many of the Stasi methods violated basic human and civil rights, especially the protection of personality and privacy, whether it be wiretapping, violations of domestic freedom, secrecy of correspondence, and so on.

To this day, intelligence services, even in developed democracies, are reluctant to disclose their records and usually do not do so at all or only disclose absolute torsos of "their" material.[79] They even resist the actual transfer of records they maintain to public archives. In some cases, they even have the legal authority to do so and do so on perfectly legitimate grounds. These include, in particular, the necessary confidentiality of intelligence activities and, along with this, the protection of intelligence sources, which in some countries is one of the reasons for extending the records classification periods, if such exist. This is the case, for example, in the USA in the latest Presidential Executive Order on classified information issued by President Barack Obama.[80] The protection of intelligence sources is also one of the reasons used by the British intelligence service, MI6 (Secret Intelligence Service), to justify not disclosing any of its records without any time limit, starting in 1909, when it was set up, until present day and even into the future as MI6 does not envisage transferring any of its records to the British National Archives.[81]

In this respect, the situation with the former Stasi records is quite the opposite. The protection of the identity of intelligence sources and the identity of Stasi employees is not a reason not to disclose Stasi material. The only reason is the protection of the personality rights of the persons concerned in the archival records. The strongest protection is offered to those who were affected by the regime or third parties, while Stasi employees and collaborators remain the least protected; in their case, the protection only covers their private and intimate lives.

The Stasi archives also explicitly apply post-mortem protection of personality and privacy; it does so by applying closure periods recognised for

[79] For more bibliographic references, see also Čtvrtník, M. (2022). Classified Records and the Archives. *Archival Science*, 2022, 129–165. https://doi-org.ezproxy.lib.cas.cz/10.1007/s10502-021-09370-3

[80] Executive Order 13526 (Classified National Security Information) of 29 December 2009, Sec. 1.5 (a).

[81] Cf. The National Archives, Intelligence and security services. https://www.nationalarchives.gov.uk/help-with-your-research/research-guides/intelligence-and-security-services/#5-mi5-and-mi6-records. Cf. also Cobain, I. (2016). *The History Thieves*. Portobello Books, p. 244.

a group of persons affected by the regime or third parties, amounting to 30 years after the date of death.[82] However, for the purposes of scientific research, these periods may be reduced to 10 years after the death of the person concerned. These periods, however, do not apply to Stasi employees and collaborators, and to public figures, political office-holders, public officials, and so-called persons of contemporary history ("Personen der Zeitgeschichte"). However, in parallel to the system of closure periods, the already mentioned "legitimate interests" of the people come into play in the case of the documents of the former Stasi as well as in the case of the records of other public archives in Germany. The "legitimate interests" are not limited by any fixed period, although, based on the case law of the German Federal Supreme Court and the Constitutional Court cited above, their protection is not indefinite. Some form of protection is recognised for all categories of persons, including Stasi collaborators, "persons of contemporary history" and, of course, persons affected by the regime. Naturally, the appraisal standards are not identical. The strongest protection is indisputably applied to those affected by the regime, whereas when it comes to Stasi collaborators and employees, only their intimate lives are protected.

In conclusion, the model of personality and privacy protection in the case of the Stasi records maintained in the Stasi Records Archive is built on the principle of multi-criteria assessment of access requests. Personality protection is not provided by the simple application of certain closure periods. While these are also implemented as one of the tools, they are complemented by and combined with other criteria.

The model of access to Stasi archives is characterised by high specificity of the access rules. In principle, it is based directly at the legislative level but the possibility of such a specification of the conditions of access is facilitated by the fact that it concerns a very narrow range of archival record groups and the data contained therein. This makes it all the easier to define precise rules of access. At the same time, it is necessary to bear in mind that the records in question were created by an organisation which combined the role of the secret police and the activities of today's intelligence services operating both internally and externally. They are therefore records which, in other circumstances, would never have been disclosed to the public. Their disclosure was driven by the change of the regime and

[82] Stasi-Unterlagen-Gesetz, § 32.

the need of the newly formed democratic society to come to terms with its own totalitarian past.

In spite of this, the access model can in many ways be inspiring for other categories of archives. This is also true in spite of the specific place the Stasi Records Archive holds in the network of German archives; this archive and its activities, together with the law defining its work, have in some cases become a precedent for the procedures, or rather some specific controversial cases of access to archival records maintained in other German archives, as we have seen in the case of the mental health records of the German actor, Klaus Kinski.

However, the multi-criteriality of the aspects taken into account and assessed when deciding on the disclosure of archival records implemented as a tool for the protection of personality and privacy, including post-mortem protection, is appropriate and, in certain—albeit obviously differently modelled—circumstances, applicable in other countries, not only within the European Union.

In the following chapter, let us look at several different tools used by some other archival systems in Europe to protect personality rights and privacy of those concerned in archival materials. In doing so, I will focus on France and the United Kingdom, which together represent quite contradictory legal systems of common and continental law.

CHAPTER 3

Personality Rights, Privacy, and Post-mortem Privacy Protection in Archives: France and United Kingdom

Personality protection in the context of archiving has a specific feature, namely that it is often impossible to clearly determine whether or not a particular case involves a living person. For this reason, archival law introduces mechanisms in which the protection of both the living and the deceased intertwine. A typical and most striking example is the institute of closure periods. This chapter introduces the tool of closure periods in international comparison using what is probably the most elaborate system developed in the French archival sector. The precisely structured system of closure periods in France has a number of inspirational moments that can be used in a wide range of other archive systems across countries that often suffer from significant deficiencies in this field.

Closure periods, however, are mentioned in this chapter primarily in the context of the analysis of other personality and privacy protection tools relating to the archival sector.[1] But similarly, some other protection mechanisms address the living and the deceased inseparably, as is the case, for example, of the French system of derogations to access, under which it is often impossible to determine whether the persons concerned are living or deceased. Alternatively, some archival mechanisms for the protection of personality and privacy may be applied similarly to living and deceased

[1] Closure periods are discussed in detail in Čtvrtník, M. (2021). Closure periods for access to public records and archives. Comparative-historical analysis. *Archival Science*, 21(4), 317–351. https://doi.org/10.1007/s10502-021-09361-4

M. Čtvrtník, *Archives and Records*,
https://doi.org/10.1007/978-3-031-18667-7_3

persons, such as the public interest test, which will be addressed in detail using the example of the United Kingdom. In this chapter we take a detailed look at the sophisticated UK system of public interest testing in the area of access to information, records, and archives, and the protection of data they contain, which takes place on several levels. One of those levels is directly tied to the so-called historical records, the main collection of which is maintained in archives.

3.1 France: General and Individual Derogations and Differentiated System of Closure Periods—Liberal-Centrist Approach

The French archival system applies several tools to protect the personality and privacy of the actors of archival materials. One of the tools at the basic level, it is the system of closure periods. On the one hand, France liberalised access to records, in a ground-breaking move in 2008, when it removed these general periods which prevented access to the archives for 30 years after the record was created.[2] Not only in this respect, when France has followed a much more liberal trend than most other countries, but also through the introduction of other tools, the conclusions reached by Livia Iacovino and Malcolm Todd cannot be seen as valid, even though their study was published just before the removal of the 30-year closure periods.[3] However, France has maintained several closure periods for certain selected groups of archives.[4]

[2] Closure periods have been removed by an amendment to the Code du patrimoine [Heritage Code] (Code du patrimoine of 20 February 2004. Ordonnance no. 2004–178 du 20 février 2004 relative à la partie législative du code du patrimoine) that also gives legal framework to present-day archiving. Cf. Loi n° 2008–696 du 15 juillet 2008 relative aux archives, amending Sec. no. 213–1 in the original text of the Code du patrimoine of 20 February 2004. On the protection of personal data in France with overlaps into international comparison, cf. the monothematic issue of Gazette des archives: *Archives et coopération européene: enjeux, projets et perspectives. Les données personnelles, entre fichiers nominatifs et jungle Internet*. La Gazette des archives, 215, 2009(3).

[3] Iacovino, L., Todd, M. (2007). The long-term preservation of identifiable personal data: a comparative archival perspective on privacy regulatory models in the European Union, Australia, Canada, and the USA. *Archival Science*, 7, 107–127. https://doi.org/10.1007/s10502-007-9055-5, p. 117.

[4] Closure periods for individual categories of records are specified in Code du patrimoine, Article L213–2. On the perspective of public administration relationship with the public, cf. Code des relations entre le public et les administrations, Article L311–5.

The specific access regime subject to closure periods applies to those groups of archives that enter the field of personality protection from different sides. Records containing matters of medical privacy constitute a special group of material. These may be disclosed 25 years after the death of the person concerned. If the date of death is unknown, the period is determined to 120 years after the date of birth.[5] In the broadest sense, however, the protection of personality is to be implemented by the provision declaring a time limit for access to archives concerning a person's private life ("*protection de la vie privée*"). This period is 50 years after the creation of the record.[6] Apart from this general period, for certain types of records concerning personal privacy, the periods are even longer. At the earliest, 75 years after their creation or 25 years after the death of the person concerned, records of a statistical nature collected by means of questionnaires and containing data on a person's privacy may be disclosed.[7] The same period also applies to access to police records, general part of court files, and registers of births and marriages. In the case of minors, the period is extended to a full 100 years.[8] The extremely long 100-year period (or 25 years after the death of the person concerned) applies to certain court files, such as those relating to intimate sex life. Hervé Lemoine (the highest representative of French archival sector in 2010–2017) and Bruno Ricard, in 2019 the newly appointed Director of the French National Archives, with an allusion to GDPR, aptly called these closure periods protecting records relating to private life "temporary right to be forgotten" ("droit à l'oubli temporaire").[9]

As we can see, France is implementing a very detailed and structured system of closure periods, which is defined in the Heritage Code (Code du patrimoine), that is, directly in the legislation regulating the archival sector. However, this system of closure periods is not the only means by which the protection of personality in archives is implemented. The second level of protection is represented by the French specific system of access to public archives under the so-called accès par dérogation.

[5] Code du patrimoine, Art. L213–2-I, Sec. 2.
[6] Code du patrimoine, Art. L213–2-I, Sec. 3.
[7] Code du patrimoine, Art. L213–2-I, Sec. 4.
[8] Code du patrimoine, Art. L213–2-I, Sec. 5.
[9] Lemoine, H., Ricard, B. (2018). Les données personnelles dans les archives publiques françaises. Loi, accès et sécurité. In K. Van Honacker (Ed.), *The right to be forgotten vs the right to remember*. VUBPRESS Brussels University Press, p. 71.

3.1.1 France and the Model of General and Individual Derogations

Bearing in mind that the issue of balancing two principles and citizen rights, that is, protection of personality rights and privacy, on the one hand, and open access to public records and information on the other, is always at the heart of the problem, French archiving and the public administration in general introduced a second institute to counterbalance the restrictiveness of closure periods. As early as the 1970s, France passed a law on improving the relationship between public administration and the public, declaring a radical openness of access of records created by public administration to citizens.[10] Yet, this trend of promoting a radically liberal, open, and transparent access to records produced by public administration can be observed in France for much longer, at least since the Enlightenment and the French Revolution.

The French specific system of access to public archives under the so-called accès par dérogation is intended to provide a sufficient counterbalance of free access to information on one side and data protection, including protection of personality and privacy, on the other. Under certain circumstances, it allows access to archival records subject to closure periods. However, this system itself seeks to implement the protection of personality and privacy. This is reinforced, among other things, by the fact that it distinguishes two types of access under derogations, namely general derogations and individual derogations, with the latter forming the larger part.[11] Under **individual derogations**, access is granted exclusively to a particular requestor (it is strictly prohibited for the requestor to enter the research room accompanied) after taking into account not only the nature of the requested records but also the personality of the researcher, their motivation for access, and purpose of research. The right to decide on access is then reserved directly to the relevant ministries. The basic principle when assessing requests is that access is provided to the extent that

[10] Loi n° 78–753 du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal [Act No. 78–753 on Administrative Relations with the Public of 17 July, 1978]. The fonds of accessible documents are defined early on in Sec. 1.

[11] Code du patrimoine, Art. L213–3-I. On the system of derogations cf. Limon-Bonnet, M.-F. (2014). Le régime des dérogations. In S. Monnier, K. Fiorentino (Sous la dir.), *Le droit des archives publiques, entre permanence et mutations.* La Gazette des archives, 234(2), 29–45.

the interest in consulting the records does not cause serious harm to the interests the law intends to protect.[12] This includes, among other things, the protection of the personality of those concerned in the archives. Summary statistics show that,[13] on average, every year the French public archives receive between 3000 and 5000 requests for individual derogations, and the percentage of requests granted has oscillated around 90% in the last decade.

The second option is the approval of a "**general derogation**" ("dérogation générale"), which opens the archival material in question to all requestors or, in some cases, to entire categories of requestors or research purposes (scientific and historical research, public statistics). Overall, however, very few such derogations have been granted in the history of the French archives, and the vast majority of the material dates from the period during or just after World War II. This fact was most recently criticised by Christine Nougaret, the then vice president of the Superior Council on Archives (Conseil Superieur des Archives), the advisory council of the Minister of Culture and Communication for the field of archiving.[14] But as early as 1996, an extensive report edited by Guy Braibant, commissioned by the then French Prime Minister Édouard Balladur, made one of the recommendations aimed at increasing the openness of archival holdings to extend the scope of the general derogation institute to the most recent documents, those that were still subject to the 30-year closure period in France at the time and which were not yet subject to general derogations.[15]

[12] Code du patrimoine, Art. L213–3-I.

[13] Observatoire des dérogations. Last updated 31 March 2020. https://francearchives.fr/article/38082

[14] Nougaret, Ch. (2017). *Une stratégie nationale pour la collecte et l'accès aux archives publiques à l'ère numérique. Rapport à Madame Audrey Azoulay, Ministre de la Culture et de la Communication*. (2017, 24 March). https://francearchives.fr/file/b0d6555950508ab637adb10ece33d381644d6d37/2017_03_24_RAPPORT_DEFINITIF_NOUGARET.compressed.pdf. Draft measure No. 23, p. 32.

[15] Braibant, G. (Ed.). (1996). *Les Archives en France: rapport au Premier ministre*. La Documentation française (Collection des rapports officiels). https://www.vie-publique.fr/sites/default/files/rapport/pdf/964093000.pdf. Recommendation No. 22, p. 125. The report itself, together with other supporting materials, successive versions, related correspondence, and so on, is part of the French Archives nationales archival collection, Premier ministre; Organismes rattachés directement; Mission de réflexion sur les archives en France (Mission Braibant) (1995–1996), id: 20000520/6–20,000,520/7, cotes 12 and 13.

To my knowledge, only 23 of these general derogations have been granted in total since 1979.[16] I am only aware of four such cases of derogations granted after 2015. For the purpose of illustration, let us look at some of the approved general derogations.

In 2009, census archives were opened under this regime up to and including the 1974 census. However, this access was not unlimited, but the materials were made available only for the purposes of public statistics and scientific or historical research, not for the purpose of new use of the data, especially for commercial purposes.[17] Thus, the same exemptions that appear in the European General Data Protection Regulation (GDPR)[18] in relation to allowing specific regimes for the processing of personal data resonate here as well. If this general derogation were not approved, a period of 75 years would apply, that is, as of 2020 the 1936 census would be the "youngest" accessible (in the twentieth century, census in France took place in 1901, 1906, 1911, 1921, 1926, 1931, 1936, 1946, 1954, 1962, 1968, 1975, 1982, 1990, 1999). A specific access was granted for the 1946, 1954, 1962, 1968, 1975 census—for these censuses, which are subject to access under general derogation, only consultation is allowed, only in the archives research room, and not remotely via the web.

In 2015, a full 70 years after the end of World War II (!), access was provided to the archives of extraordinary courts under the Vichy regime and the period of Provisional Government of the French Republic (1944–1946), archival fonds of the central administration of the Ministry of Justice related to cases of extraordinary courts under the Vichy regime and the period of Provisional Government of the French Republic, together with police investigation materials from 1939 to 1945, police investigations from 1945 to 1960 relating to matters from 1939 to 1945, prosecution and trial of war crimes in the French occupation zones in

[16] By 2017, the data was collected by Mallet, J. (2018). Les dérogations générales. 31 January 2018. https://siafdroit.hypotheses.org/764

[17] Arrêté du 4 décembre 2009 portant dérogation générale pour la consultation des listes nominatives du recensement général de la population. JORF n° 0288 du 12 décembre 2009, texte n° 48 [Decree of 4 December 2009 on general derogation concerned the census records].

[18] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Germany and Austria, and finally the archives of the war and maritime courts from 1939 to 1945.[19]

The extremely long time it took to open material so vitally important for French history from the time of World War II and just after its end, is very surprising, all the more so because it took place in a country with a continuous democratic regime and strong liberal tendencies in the field of archiving, which resonate, inter alia, in the aforementioned abolition of the general 30-year closure periods, that apply, even if their lengths may slightly differ, in a considerable part of the world. In this context, it is worth noticing the analogy with the current opening of Vatican archives as in March 2020, Pope Francis II opened access to archives from the time of the pontificate of Pius XII (1939–1958) maintained in the Vatican Apostolic Archive.

In 2017, the opening of archival records from the Klaus Barbie trial, also known as the "Butcher of Lyon", attracted considerable attention among the French public.[20] Klaus Barbie, a German member of the SS and SD, who, during World War II, operated in the occupied Netherlands and was later assigned to France, where he was stationed in Lyon as the head of the local Gestapo from 1942–1944; he became known for his extreme brutality, torturing women, children, and members of the resistance. After the war, he cooperated in Germany with the US and British secret services and benefited from their protection (his value consisted mainly in infiltrating and spying on the Communist Party in Bavaria). After the War, however, France did not strive hard to have Barbie extradited, presumably due to concerns among some senior French officials that Barbie's testimony about their activities, such as cooperating with the Gestapo during the war, might discredit them. As a result, Barbie was not extradited to France. He then lived in Bolivia and in 1966 became a paid associate of the West German secret service, the Bundesnachrichtendienst (BND); among other things, he was involved in the arms trade of the Bundesrepublik with Latin America, as German historian Peter Hammerschmidt proved a

[19] Arrêté du 24 décembre 2015 portant ouverture d'archives relatives à la Seconde Guerre mondiale. JORF n°0300 du 27 décembre 2015, texte n° 2 [Decree of 24 December 2015 on opening of archives relating to WWII].

[20] Arrêté du 30 juin 2017 portant ouverture des archives du procès de Klaus Barbie. JORF n°0156 du 5 juillet 2017, texte n° 22 [Decree of 30 June 2017 on opening of archives of Klaus Barbie trial]. Archival fonds from the Klaus Barbie trial in detail in Galland, B. (2018). Le procès de Klaus Barbie, entre archives, témoignage et éthique. *La Gazette des archives*, n° 249, 2018(1), 163–177.

couple years ago.[21] In the 1970s, however, Nazi hunters tracked him down in Bolivia, and in 1983, Bolivia finally extradited Barbie to France. The trial began in 1987, during which time Barbie's testimony revealed that quite a few respected citizens had collaborated with the Nazis. In the same year, he was given a life sentence. Klaus Barbie died in prison in 1991. The very disclosure of archives from France's first-ever trial of crimes against humanity[22] was greatly accelerated by the French public opinion.

Another notable case of approved general derogation concerned the archives relating to the case of Maurice Audin (1932–1957). Maurice Audin was a French mathematician at the University of Algiers, a member of the Algerian Communist Party and a participant in the struggle for Algerian independence from France in the Algerian War (1954–1962). In 1957, he was arrested by the French and later officially declared missing. It was not until 2014 that France officially acknowledged that he had died in prison, and it was not until 2018 that French President Emmanuel Macron officially admitted that Audin had been tortured in prison and had either been executed or tortured to death.[23] Audin was among those affected by the cruel inhuman conduct of French troops in Algeria, which, after all, eventually led to a reversal of French public opinion and the decision of the then French president, Charles de Gaulle, to act towards the recognition of Algerian independence. Audin's body was never found.[24] It was as late as 2013 that access was provided to the first part of the records related to the Maurice Audin case[25] in the form of a general derogation; and it was not until 2019 that access to entire documentation was opened, following President Macron's declaration of 13 September 2018 on the death of Maurice Audin, in which he agreed to opening all archives

[21] Hammerschmidt, P. (2014). *Deckname Adler. Klaus Barbie und die westlichen Geheimdienste*. S. Fischer.

[22] Galland, B. (2018). Le procès de Klaus Barbie, entre archives, témoignage et éthique, p. 167.

[23] Déclaration du Président de la République sur la mort de Maurice Audin (2018, 13 September). https://www.elysee.fr/front/pdf/elysee-module-950-fr.pdf

[24] Maurice Audin case has most recently been summarised, also in the context of the specific phenomenon of the so-called transitive justice by Thénault, S., Besse, M. (Eds.). (2019). *Réparer l'Injustice: l'Affaire Maurice Audin. Institut francophone pour la justice et la démocratie*. Institut francophone pour la justice et la démocratie.

[25] Arrêté du 1er février 2013 instituant une dérogation générale pour la consultation d'archives publiques relatives à la disparition de Maurice Audin. JORF n°0046 du 23 février 2013, texte n° 25 [Decree of 1 February 2013 on general derogation for opening of public archives concerned the disappearance of Maurice Audin].

relating to persons who disappeared during the Algerian War, including the Audin case material.[26]

Most of the general derogations relate to the archives maintained in the French National Archives. However, they can also be utilised by the Ministries of Defence and Foreign Affairs for "their" archival records. Thus, not long ago in 2018, access was provided to materials preserved in the Archives of the Ministry of Defence of France relating to the Minerve submarine case, which went missing with 52 sailors on board in 1968.[27] The disclosure of the then exactly 50-year-old archives (until then, the archives were only opened in 2007 for Christophe Agnus, the son of one of the drowned officers based on an individual permission of the French president of that time, Nicolas Sarkozy[28]) was initiated by Hervé Fauve, the son of the submarine commander. The shipwreck was not found until July 2019. However, the open archives containing, among other things, documents from the investigation into the sinking of the submarine did not provide any further evidence to establish the cause of the shipwreck.

In both individual and general derogations, the possibility of reproducing materials, including the modalities of using the researcher's own reproduction devices, cannot be excluded in advance. In the case of individual derogations, the researcher's access request should also indicate whether they intend to reproduce the records, which is then commented on not only by the records creator, but also by the Service interministériel des Archives de France (SIAF), the central French governing body for archives under the Ministry of Culture and Communication.[29] In case the researcher disagrees with the decision, the matter may ultimately be examined, on request, by the Committee on Access to Administrative Documents (Commission d'accès aux documents administratifs, CADA), whose task is to oversee the implementation of the rules on free access to

[26] Arrêté du 9 septembre 2019 portant ouverture des archives relatives à la disparition de Maurice Audin. JORF n°0210 du 10 septembre 2019, texte n° 26 [Decree of 9 September 2019 on opening of public archives concerned the disappearance of Maurice Audin].

[27] Arrêté du 4 juin 2018 instituant une dérogation générale pour la consultation d'archives publiques relatives à la disparition du sous-marin "Minerve" le 27 janvier 1968. JORF n°0137 du 16 juin 2018, texte n° 9 [Decree of 4 June 2018 on general derogation for opening of public archives concerned the disappearance of submarine "Minerve"].

[28] Information provided by Guibert, N. (2019, 5 February). La marine va rechercher l'épave du sous-marin "Minerve". *Le Monde*.

[29] Circulaire DGP/SIAF.AACR/2010/010 du 29 juillet 2010. Dérogations aux règles de communicabilité des archives publiques règles générales et procédure.

official records and public archives, as well as the specific area referred to in France as the "new use of public information" ("réutilisation des informations publiques") used in French legislation. Although the French terminology distinguishes between the terms "communication" and "consultation", even in the case of individual "consultation" of records in the CADA research room, the Code on the relationship between the public and the administration (Code des relations entre le public et les administrations) does not exclude the possibility of the researcher using their own reproduction device, such as a smartphone, tablet, camera, and so on.[30]

Specific access to archives under individual and general derogations for the whole public or certain categories of researchers is one way to implement efforts to protect personality, including private life, while providing access to archival records to the extent possible. Although some of the presented tools, applied for example in French archives, may seem to be an appropriate solution to the whole problem, the situation is complicated and complex and the seriousness of the risks of personality protection in archives is not negligible. For example, the premature disclosure of census records for individual consultation inside the archives research rooms raises significant questions. In this case, France implemented the model of general derogations and in 2009 provided premature access to the census data up to and including 1974. Unlike many other countries, France does not anonymise these materials. I shall provide a detailed analysis in comparative international perspective of access to census archives in Chap. 7.

3.2 United Kingdom: Public Interest Test, Proportionality of Interests, Common Law, and Confidentiality—Decentralist Approach

Is it justified, and if so in what sense, to describe the British model as a decentralist approach to opening access to archival records and protecting personal data and privacy therein? What are its specifics?

The year 2000 marked a turning point in the policy of access to public records, archives, and information in general, as the Freedom of

[30] Modalités de communication. Commission d'accès aux documents administratifs. Published 10 July 2018. https://www.cada.fr/administration/modalites-de-communication. The conclusions on this issue presented in Mallet, J. (2018). Les dérogations générales are therefore not entirely accurate.

Information Act (FOIA) was passed.[31] The Act has taken over the competence to regulate access to information and, with it, to public records. Unlike the French model, the British model does not create a system of structured, precisely defined periods for access to particular categories of information and records. A specific feature of the British model is the introduction of a multi-layered and multi-stage public interest test, which takes place at several points within the records management and is performed by different entities. There are several different forms of testing.

3.2.1 Public Interest Test: Freedom of Information Exemptions

At the first level, the testing is based on the general right of the public to virtually immediate access to information. However, the FOIA provides for a set of certain categories of information constituting exemptions from this requirement of immediate access. These exemptions are of a dual nature. First, there are the so-called absolute exemptions.[32] In their case, the public authority is not obliged to disclose the information and does not have to carry out any further assessment. These exemptions include, for example, information accessible by other means, court records, and information held in relation to court proceedings, information provided in confidence, and certain other information including personal information for the lifetime of the persons concerned. The second group consists of "qualified exemptions", which include, for example, information intended for future publication, health and safety information, environmental information, personal information relating to a third party, business interests, and certain additional information.

For these qualified exemptions, an elaborate public interest test process, implemented by public authorities including archives, has crystallised over time in the United Kingdom and is worthy of closer attention.[33] In addition, the British system has divided all exemptions into two basic categories. The first consists of exemptions based on the type of information concerned ("class-based exemptions"). In this case, the relevant public authority does not have to provide further arguments as for why it will not

[31] Freedom of Information Act of 30 November 2000. Ch. 36.

[32] Freedom of Information Act 2000, Sec. 2 (3).

[33] For a comprehensive overview of public interest test, cf. material prepared by the Information Commissioner's Office (ICO). The Public Interest Test. https://ico.org.uk/for-organisations/guidance-index/freedom-of-information-and-environmental-information-regulations/the-public-interest-test/

disclose the information, what interests would be harmed by the information disclosure, and therefore does not have to carry out a public interest test. Almost all absolute exemptions are "class-based". The second category are exemptions based on harming certain interests ("prejudice-based exemptions"), in which case the public authority must demonstrate that and how disclosure of the requested information or record harms the interests specified in the relevant exemption.[34]

The public interest test itself consists in a public authority weighing the harm that disclosure would cause to the legitimate interests against the public interest served by disclosure of the information, always considering current circumstances and context.

Public interest test is carried out independently by each relevant public authority, which is an important element of the British decentralised model. The specificity of this model is then reflected in the existence of a considerable number of methodologies and codes of practice. The need for them is also given by the fact that public interest testing is a process that the British Anglo-American common law shapes not only by statutory provisions but in a significant way also by the case law created by the judicial system through precedents. One of the significant precedents in the area of public interest testing for access to information, records, and archives and for assessing prejudice-based exemptions is the 2006 case of Christopher Martin Hogan and Oxford City Council v. the Information Commissioner, which is also regarded as an important reference by the UK Information Commissioner's Office (ICO), the United Kingdom's independent authority for information rights, access to information and privacy.[35]

When testing the public interest, the public authority must take into account a wide range of public interests. On the side of the public interest in information accessibility, there are, among other things, moments such as the consideration of transparency. "There is a general public interest in

[34] On FOIA exemptions cf. The National Archives material Freedom of Information Exemptions (2016, reviewed 2019), which also provides an overview table specifying individual exemptions and their categories, including specific periods. https://www.nationalarchives.gov.uk/documents/information-management/freedom-of-information-exemptions.pdf

[35] Christopher Martin Hogan and Oxford City Council v. the Information Commissioner, Appeal Numbers: EA/2005/0026, EA/2005/0030, 17 October 2006. Other important case laws in this area are summarised in ICO, The Public Interest Test.

promoting transparency, accountability, public understanding and involvement in the democratic process."[36] Another reason for making information accessible is the public interest in a topic that has a broad social impact, such as the implementation of public policies. Other motives may also be the possibility of controllability, which is conditioned by the availability of all relevant data, the promotion of good decision-making by public bodies and the like. If, for example, there are suspicions of maladministration, breaches of the law, and so on, the public interest in open information becomes very important compared to the countervailing public interest in, for example, protecting the personal data of third parties, business interests, and so on.

In the case of "prejudice-based exemptions", which include areas such as foreign relations, defence, economy, public affairs, business interests and the like, the aforementioned case of Christopher Martin Hogan and Oxford City Council v. the Information Commissioner plays an important role in British law. The ICO, referring to the court judgement in this case, has outlined the procedure that should be applied in the case of a prejudice test.[37] First, the public interests at stake in the case in question must be identified. In the second step, the substance of their hypothetical harm should be identified, the basic issue here being "to be able to show that some causal relationship exists between the potential disclosure and the prejudice and that the prejudice is … 'real, actual or of substance'".[38] The causal link should then have a logical basis and should not be a mere hypothetical assumption. Finally, the likelihood that such harm would occur should be assessed. In doing so, the circumstances in which such harm could occur, the degree of certainty with which this harm could be caused, and the frequency of the potential occurrence should be considered. British common law does contain precedents that have grappled with how to precisely define the concept of likelihood of harm, how to measure it,

[36] ICO, The Public Interest Test.

[37] Information Commissioner's Office (ICO). (2013). *The Prejudice Test. Freedom of Information Act.* https://ico.org.uk/media/for-organisations/documents/1214/the_prejudice_test.pdf, p. 5–6.

[38] Christopher Martin Hogan and Oxford City Council in the Information Commissioner, Sec. 30, p. 8.

differentiate it, and determine its role in testing for potential harm.[39] The United Kingdom's ICO drew on a judgement in the court case that differentiated, in principle, between two basic measures of probability. The stronger measure occurs when it is more likely that harm would occur if the information is disclosed than that it would not (the "would" option).[40] The lower probability applies when, even though there is a serious risk of harm, it is not possible to say whether the likelihood of harm in the event of disclosure is greater or lower than 50% (the "would be likely" option). One of these two options should be explicitly mentioned and justified by the public authority deciding not to disclose the information.

At the very heart of the public interest test for qualified exemptions, or prejudice-based exemptions, is the process of weighing the various arguments and public interests by public authorities, detecting the weight of each, and disclosing the information if the public interest in disclosure prevails.[41] The weighing takes into account criteria such as the likelihood of harm to the relevant public interest and the seriousness of the potential harm. The ICO mentions one court case from 2010 in which the authority itself was involved.[42] It was a dispute over the disclosure of data on animal experiments carried out at Oxford University. The University did not want to disclose certain data on these experiments on the grounds that it could endanger the safety of some of their staff by protectionist extremists in the form of bombings or arson. The court acknowledged this, stating that the risk to university employees outweighed the harm to the public interest in disclosure.

This weighing of the various public interests can be expressed in other words as a proportionality test. A similar proportionality test has crystallised in British law in other areas of data protection, including personal data protection and a specific principle with which British law operates, namely the duty of confidentiality. Nevertheless, these tests are not

[39] For example, John Connor Press Associates v. Information Commissioner EA/2005/0005, 25 January 2006; Mr. Justice Munby in R (on the application of Lord) v. Secretary of State for the Home Office [2003] EWHC 2073, (Admin), 1 September 2003; John Connor Press Associates v. Information Commissioner EA/2005/0005, 25 January 2006); Christopher Martin Hogan and Oxford City Council v. the Information Commissioner. As cited in ICO. (2013). *The Prejudice Test. Freedom of Information Act.*

[40] ICO. (2013). *The Prejudice Test. Freedom of Information Act*, Sec. 27–39, pp. 8–11.

[41] Ibid., Sec. 53–69, pp. 22–28.

[42] People for the Ethical Treatment of Animals Europe (PETA) v. Information Commissioner and University of Oxford EA/2009/0076, April 13, 2010.

identical, and in some respects their emphasis goes in the opposite direction, as will be seen shortly.

3.2.2 Breach of Confidentiality: Public Interest Test as Proportionality Test

When deciding on access to records, archives, and data protection, public institutions, including archives, have to take other perspectives into account and perform the public interest test at other levels as well. The "duty of confidentiality" is an important element. Here, too, the specificity of British law, namely the area of British common law, comes into play in a significant way. The principle of confidentiality is, however, also reflected at the level of the law, since one of the notable exemptions to the right of access to information is situations where the opening of information provided to a public authority by an individual, but also by another public authority, would mean a failure to respect the confidentiality envisaged and assumed by the individual or authority when communicating with the addressee.[43] At the same time, it is an exemption which is not limited in time but unlimited in duration. For this reason, archives must also take into account the duty of confidentiality and test public interest in situations if a possible breach of confidentiality is involved.

This, of course, does not mean that every piece of information exchanged between citizens and public authorities is confidential. This is where the British common law comes into play, in which the concept of confidentiality and breach of confidentiality has crystallised. In principle, the information must have the quality of confidentiality. This means that it must not be trivial, it must not be accessible in any other way, it must be worthy of protection in the sense that someone has a genuine interest in keeping the content of the information confidential.[44] At the same time, the disclosure of such information would be actionable. Although confidentiality of information is an absolute exemption under FOIA (see above), even in its case, a public institution should conduct a public interest test and consider whether the public interest in breaching confidentiality outweighs the public interest in a particular case. If a public institution

[43] Freedom of Information Act 2000, Sec. 41.

[44] Cf. Information Commissioner's Office (ICO). *Information Provided in Confidence (Section 41). Freedom of Information Act.* https://ico.org.uk/media/for-organisations/documents/1432163/information-provided-in-confidence-section-41.pdf

can rely on "public interest defence" by opening certain information otherwise provided in confidence, British common law provides for non-actionability.[45]

This is a very complicated area of law that is constantly evolving in view of the continuous changes in the common law, and has recently evolved quite dynamically. The ICO summarises the development of important judicial precedents in this area, particularly after 2000, and recent developments in the UK courts' perception of confidentiality.[46] As recently as the 1990s, British courts generally recognised situations in which the public interest in opening information outweighed the duty of confidentiality; these were exceptional cases when access to the information would produce evidence of breach of law, misconduct, corruption, and the like. At the turn of the millennium, the existence of similar serious cases was challenged by the courts. Soon after the new Human Rights Act was passed,[47] which implemented the European Convention on Human Rights into British law, further significant developments occurred. Newly, the courts have begun to take more substantial account of the right to protection of private and family life, but on the other hand also the competing right to freedom of expression, access to information and its dissemination, that is, the rights defined in the European Convention.[48] This eventually led to the public interest test becoming a proportionality test. As one of the court statements succinctly put it: "Before the Human Rights Act came into force the circumstances in which the public interest and publication overrode a duty of confidence were very limited. The issue is whether exceptional circumstances justified disregarding the confidentiality that would otherwise prevail. Today the test is different. It is whether a fetter of the right of freedom of expression is, in the particular circumstances, 'necessary in a democratic society'. It is a test of proportionality."[49]

Today, therefore, two public interests are weighed against each other: On the one hand, the public interest in providing access to information, and on the other, the public interest in maintaining its confidentiality.

[45] ICO, Information Provided in Confidence, Sec. 41 (71–73), p. 21.

[46] ICO, Information Provided in Confidence, Sec. 41 (74–87), pp. 21–23.

[47] Human Rights Act 1998 of 9 November 1998. Ch. 42.

[48] Rights are defined in Articles 8 and 10 of the European Convention on Human Rights as amended by Protocols Nos. 11 and 14 supplemented by Protocols Nos. 1, 4, 6, 7, 12, 13 and 16. (1950). https://www.echr.coe.int/documents/convention_eng.pdf

[49] Court of Appeal, HRH Prince of Wales v. Associated Newspapers Limited (2008), 57 (67). As cited in ICO, Information Provided in Confidence, Sec. 41 (79), p. 22.

However, as the ICO points out, the public interest test in this case is different from the public interest test for qualified FOIA exemptions as discussed above. In the system of qualified exemptions, the public interest works in principle in favour of opening information, the closure of which—that is, obtaining a FOIA exemption—will only occur if the public interest in its non-disclosure prevails. In the case of the duty of confidentiality, the opposite is the case: The public interest in maintaining confidentiality is presumed to prevail, except in situations in which it would appear that opening access to the information would carry more weight in the relevant circumstances.[50]

The public interest grounds for breaching the duty of confidentiality are multiple and it is impossible to provide an exhaustive list. Nevertheless, let us take a look at just a few of them. One of them is the public interest that—as the ICO defines it—"public authorities remain transparent, accountable and open to scrutiny, for example where disclosure would further public understanding of, and participation in the debate of issues of the day; enable individuals to understand decisions made by public authorities affecting their lives and, in some cases, assist individuals in challenging those decisions; or facilitate accountability and transparency in the spending of public money."[51] Another situation in which confidentiality can be breached is when a breach of law, abuse of authority or corruption is revealed. In such situations it is not necessary to be certain, but according to the methodology of the British authority on access to information and its case law, a serious suspicion based on a reliable source is sufficient.[52] Another reason for breaching confidentiality is, for example, the public interest in protecting security.

This, naturally, does not mean that the duty of confidentiality should be disregarded. On the contrary, too free handling could lead to a breach of trust of individuals or legal entities entrusting information to public authorities. It is therefore always necessary to look at the wider context and consider, as the ICO highlights, "how the relationship of trust operates to serve the public interest".[53]

[50] ICO, Information Provided in Confidence, Sec. 41 (81), p. 22.

[51] ICO, Information Provided in Confidence, Sec. 41 (83), p. 22.

[52] ICO with reference to the judgement of the Tribunal Decision in Moss v. the ICO and the Home Office (EA/2011/0081, 28 February 2011). See ICO, Information Provided in Confidence, Sec. 41 (86), p. 23.

[53] ICO, Information Provided in Confidence, Sec. 41 (91), p. 24.

It should also be added that in the United Kingdom there exist a number of categories of personal data, or records containing such data, whose confidentiality is explicitly declared and therefore are subject to special protection under certain specific regulations, which the archives need to take into account when considering whether or not to disclose the information requested. Indeed, there are a number of other specific regulations in the United Kingdom setting out specific access systems and restrictions for certain special categories of data, far from being limited to personal data. In 2005, the then Department for Constitutional Affairs found a total of 210 such regulations preventing access to information.[54]

Staying in the area of personal data, a typical example is data relating to sexual offences, in whose case a specific law directly stipulates that no data that could lead to the victim's identification may be disclosed during the victim's lifetime.[55] The same is the case for data on abortions,[56]sexually transmitted diseases,[57] medical records in general, and some other similar circumstances.

But even in these cases, British law leaves room for public interest considerations. Thus, even in the case of medical records—although the common law considers the information in them to be confidential—the same common law has established the practice that in exceptional cases the public interest in opening such information prevails and the duty of confidentiality can therefore be breached. This is also consistent with the UK Department of Health Code of Practice on Confidentiality in Medical Records, which defines the public interest in this area to mean that under certain specific circumstances, the public interest in providing access to data may outweigh the individual interest in maintaining confidentiality.[58] In doing so, the data controller must assess the potential harm that may

[54] Review of Statutory Prohibitions on Disclosure, Department for Constitutional Affairs 2005. https://webarchive.nationalarchives.gov.uk/ukgwa/+/http://www.dca.gov.uk/StatutoryBarsReport2005.pdf, p. 1. While this inventory is no longer entirely up-to-date, it does provide some insight into the breadth and complexity of the law entering the field of personality protection in the United Kingdom.

[55] Sexual Offences (Amendment) Act 1992, Sec. 1 (1).

[56] Abortion Regulations 1991, Regulation 5: Restriction on disclosure of information.

[57] National Health Service (Venereal Diseases) Regulations 1974, Regulation 2: Confidentiality of Information.

[58] Department of Health. (November 2003). *Confidentiality. NHS Code of Practice.* https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/200146/Confidentiality_-_NHS_Code_of_Practice.pdf, p. 6, Sec. 30, p. 13, Sec. 38, p. 15.

occur to both parties and interests (the interest of the society vs. the interest of the individual) by opening the data. At the same time, it clearly points out that in situations when there is no explicit consent of the person concerned to the disclosure of information relating to them and when there are no legal situations in which the data are to be disclosed for various official purposes, there must be a genuine "overriding public interest" in such disclosure to third parties.[59] Such a public interest was then found by the common law in cases as preventing, detecting, or enabling the conviction of a serious crime, preventing harm or damage to another person. In any case, a detailed record shall always be made of the entire process of such disclosure, with detailed justification. In addition, where possible, such disclosure should always be consulted with the individual concerned.

The British legal system also covers specific situations, such as breaches of confidentiality in cases of whistleblowing by employees, in similar and precisely defined cases (suspected breach of the law, risk to health or safety of persons, risk of damage to the environment and some others).[60]

Naturally, situations such as the disclosure of personal data from medical records for scientific research are also reflected. The British Department of Health's Code of Practice gives an example of disclosure in the following cases.[61] The key here lies in the application of the principle of proportionality. For example, in a situation that would involve a disproportionate effort to obtain consent from the patient and in which, at the same time, the likelihood of harm to the patient's interests by disclosing their medical data for research purposes would be negligible, the materials may be opened for research purposes without the patient's consent.

The British Department of Health later issued further guidance on how to apply the principle of disclosure of medical records in situations in which exists an overriding public interest in such disclosure.[62] It describes

[59] Department of Health. (November 2003). *Confidentiality. NHS Code of Practice*, Sec. 11, p. 7, Sec. 14 (b), p. 23, Sec. 28, p. 34, Sec. 30–34, pp. 34–35.

[60] Public Interest Disclosure Act 1998.

[61] Department of Health. (November 2003). *Confidentiality. NHS Code of Practice*, Sec. 34, p. 35.

[62] Department of Health. (November 2010). *Confidentiality: NHS Code of Practice. Supplementary Guidance: Public Interest Disclosures*. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/216476/dh_122031.pdf. Cf. also Health and Social Care Information Centre. (2014). *Code of Practice on Confidential Information*. https://digital.nhs.uk/binaries/content/assets/legacy/pdf/8/9/copconfidentialinformation.pdf

the entire procedural process, gives details on what a public interest assessment should look like, what information needs to be gathered, and provides specific examples. The confidentiality of personal data can be breached, for example, when a patient refuses to inform their sexual partner that they suffer from a sexually transmitted disease. It characterises how to proceed when assessing what constitutes a serious crime, that constitutes one of the grounds on which confidentiality can be breached. Finally, it provides some specific scenarios that can occur and describes how to deal with them.

3.2.3 "Historical Records" and Archives: Second-Level Testing

At an imaginary second level, ensuring data protection or access to information and records, including the proportionality test of public interests, is carried out at the level of so-called historical records. If such is the case, the archival system common in most countries usually comes into play, namely the system of closure periods. In the United Kingdom, a public record becomes "historical" 20 years after its creation, regardless—and that is essential—whether it is in live administration or has already been transferred to the archives for permanent preservation. The vast majority of these historical records were deprived of the possibility of becoming exemptions to the rule of open information, and the law has thus made public records with the status of historical records accessible to the public.[63] In its original version, the law set a period after which public records become "historical"; the original period was 30 years, which was subsequently reduced in 2010 to the currently still valid 20 years.[64] The same period also applies to the obligation to transfer records of permanent historical value to the archives for permanent preservation.[65] A reflection on the seriousness of the issue of closure periods and their (disproportionate) duration is also evident in the documentation created by the activities of the Advisory Council on National Records and Archives, be it meeting minutes, memoranda, correspondence, and other documentation. The

[63] Freedom of Information Act 2000. Ch. 36, Sec. 63–64.

[64] Constitutional Reform and Governance Act of 2010. Ch. 25, amending the periods given in Sec. 62 (1) of the UK Freedom of Information Act of 2000. Ch. 36, Sec. 62 (1) defining the so-called historical records. In doing so, it is necessary to take into account the following Sec. 63, which imposes a general obligation to provide information from "historical records".

[65] Public Records Act 1958. Ch. 51, Sec. 3 (4).

roles of the Advisory Council on National Records and Archives will be discussed below.[66]

The status of "historical records" thus fulfils the function of one of the key guarantees of the timely opening of public records and society's information; at the same time data protection also applies at this stage and at the stage of management of historical records. How do both considerations play out?

They appear as possible exemptions, as we have already discussed above. Both public authorities and citizens can request them. We will now stay within the sphere of records and archives in the care of the British National Archives. A key role is played by the "Advisory Council on National Records and Archives", an independent advisory body on records maintained by the British National Archives.[67] Based on the Council's opinions, the final decision regarding such requests is then made by the Secretary of State for Digital, Culture, Media and Sport.

The Advisory Council on National Records and Archives assesses, in principle, three possible basic situations of exemptions from access to public historical records and, at the same time, carries out the second wave of triple testing and weighing of the public interest. The following three situations commonly occur:

a. Public entities (in this case within the competence of the National Archives) may request an extension of the 20-year period after which they should transfer their records to the archive (applications for retention).[68]

[66] Cf., for example, The National Archives. Series PRO 42. (1959–1986). Advisory Council on Public Records, specifically for example PRO 42/50: Memoranda. See, for example, the memorandum from 2 March 1970 "Accelerated opening of second world war records". Cf., inter alia: PRO 42/51 – Memoranda; PRO 42/75: Memoranda; PRO 42/23: Access to records and introduction of 30-year rule.

[67] On Advisory Council on National Records and Archives, established already in 1958 (according to the Public Records Act 1958. Ch. 51, Sec. 1 (2)), see its website https://www.nationalarchives.gov.uk/about/our-role/advisory-council/. The annual reports published in the recent years are also available via this link. The National Archives in the United Kingdom holds a considerable amount of records created by or relating to the Advisory Council. Cf. not only Series PRO 42. (1959–1986). Advisory Council on Public Records, some interesting information can also be found in the Records of the Cabinet Office (CAB) series, for example, CAB 184/401: Disclosure of official information.

[68] For an example request for extension of retention of public records, see, for example, The National Archives. Series PRO 70. (1982–2003). Public Record Office: Lord Chancellor's Instruments: Retention by Department under Public Records Act 1958. Here for example: PRO 70/58: Retention of Public Records; PRO 70/66: Retention of Public Records.

b. Second, the same public entities may request the transfer of historical records to the archive in a closed form in a state of non-disclosure to the public (applications for closure), that is, request an extension of the period for making historical records available to the public.[69] This point is actually the second stage of the assessment of "qualified exemptions" from general access to information, as introduced in the British law by the Freedom of Information Act (FOIA) and discussed above. Or rather, it is an assessment of the legitimacy of the exemptions by a second independent authority. In the first phase, it is the record creator who requests the application of a qualified exemption and assesses its legitimacy. The second phase occurs when the creator transfers "historical records" (usually 20 years after their creation) to the archive and requests a qualified exemption even after their transfer. At this point, the scene is entered by the Advisory Council on National Records and Archives whose competence it is to assess such requests. At least at a central level, the British National Archives seeks to achieve the earliest possible disclosure of archival records to researchers by persuading creators to apply exemptions only to the minimum extent necessary and for the shortest possible period of time, with the proviso that they should (but need not) set a specific point at which the records can be opened to the public, or a point at which further review can take place.[70] In cases when it is not possible to determine the exact moment of providing access to the archives at the time of their transfer, the National Archives and the Advisory Council seek to apply the "rolling 10 years" rule, that is, the reasons for restricting access to the archives should be re-examined every 10 years.[71] A new review also occurs when a research request is made for access to restricted material.

[69] Handling the requests for extension of closure periods represents a significant agenda for the Advisory Council, as demonstrated by the archival collection generated by its activities. Cf. The National Archives. Series PRO 42. (1959–1986). Advisory Council on Public Records. On the extension of closure periods see, for example, PRO 42/45: Minutes of meetings (1969–1976); PRO 42/50: Memoranda: AC [69]1 - AC [72] 9; PRO 42/64: Memoranda: AC [77] 1 - AC [81] 13; PRO 42/57: Correspondence and papers: Access to public records; PRO 42/75: Memoranda: AC [84] 1 - AC [83] 21; PRO 42/23: Access to records and introduction of 30-year rule; PRO 42/77: Access to public records.

[70] Principles for Determining the Access Status of Records on Transfer. (2019). The National Archives. https://www.nationalarchives.gov.uk/documents/information-management/principles-for-determining-the-access-status-of-records-on-transfer.pdf, p. 4.

[71] The National Archives. (2019). *Closure Periods.* https://www.nationalarchives.gov.uk/documents/information-management/closure-periods.pdf, p. 2.

c. Natural persons: researchers may request access to historical records subject to exemptions and still restricted to the public.[72]

In all three of these cases, the Advisory Council weighs the public interest for and against granting an exemption, either in the form of an extension of the period for transferring records to the archives under (a), or in the form of an exemption from access to records under (b), or an exemption from opening otherwise restricted records (c).

But what does this general setting look like in some specific situations and applications? For example, most requests under (c) usually seek access to investigation or court files of criminal cases, most often historical murder cases.[73] In such cases, the Advisory Council commonly weighs the public interest in disclosure of the material against the potential harm to the victims or their relatives. For unsolved crimes, the risks to the successful completion of criminal proceedings in the future are also taken into account. A large part of FOIA requests under (c) seek disclosure of information that, if opened, could harm the safety or physical or mental health of an individual.[74] There is also interest in information whose disclosure could harm international relations or ongoing criminal proceedings. In terms of the number of requests, for example, in FY 2016–2017, the Advisory Council handled 400 FOIA disclosure requests under (c), almost half as many as the year before. When granting or refusing access, the Advisory Council usually requests an up-to-date opinion, including a specific justification by the record creator, and, if necessary, the opinion of the relevant department of the National Archives. In a large number of cases, the Advisory Council accepts the arguments put forward by the record creator.

In the case of (a), the reason for a large part of the authorities' requests for an extension of the period for transfer their records to the archives, is

[72] Documentation of the Advisory Council's decision-making regarding these requests is preserved in the archival records of the Advisory Council. Cf., for example, The National Archives. PRO 42. (1959–1986). Advisory Council on Public Records. PRO 42/21: Advisory Council Series – Memoranda.

[73] Advisory Council on National Records and Archives. *16th Annual Report 2018–19*, p. 8. https://www.nationalarchives.gov.uk/documents/advisory-council-annual-report-2018-19.pdf

[74] Cf. Advisory Council on National Records and Archives. *14th Annual Report 2016–17*. https://www.nationalarchives.gov.uk/documents/advisory-council-annual-report-2016-17.pdf

the protection of security. A smaller percentage indicates protection of business secrets or ongoing public investigations as reasons.

For requests under (b), this is, as already mentioned, the second stage of the public interest test in the case of requests to disclose historical records even after they have been transferred to the archives. It is worth mentioning one particular figure. In the FY 2018–2019, the Advisory Council accepted a total of 86.5% of the requests from creators without further examination, that is, it was satisfied with the vast majority of the justifications provided by the creators, and this trend has also been evident in recent years.[75] In situations when requests were further examined, the Advisory Council usually only requested a more detailed justification and did not request a change in its own conclusion on the (in)accessibility of the material. Overall, the Advisory Council notes relative satisfaction with the justification of "qualified FOIA exemptions" by record creators, although it does identify some issues and sees improving the quality of justifications provided as one of its goals. At the central level, the National Archives stresses that this system must not be abused or overused by the record creators; the requests must be specific. For example, it should not occur that the record creator requests that broad subject groups of records be withheld simply because only a small part of the particular record group requires longer protection.[76]

Some statistical numbers are also interesting. For example, in FY 2018–2019—but the figures have been relatively similar in recent years—the Advisory Council received 5843 requests for the transfer of historical records to the archives in closed form, of which nearly 400 were questioned and further information was requested by the Advisory Council, resulting in only 13 requests being withdrawn by the relevant authority. In the same year, there were 970 requests for extensions to the 20-year period for transfer of records, of which only 4 were withdrawn following the Council's conclusions.[77]

More than a few of the above-mentioned forms of public interest testing in the case of an assessment by the Advisory Council on National Records and Archives as to whether or not to disclose records, are situations when the records in question also contain personal data.

[75] Advisory Council on National Records and Archives. *16th Annual Report 2018–19*, p. 6.

[76] Principles for Determining the Access Status of Records on Transfer, pp. 4–5.

[77] Advisory Council on National Records and Archives. *16th Annual Report 2018–19*, pp. 16–17.

Let us conclude by looking at some of the issues that fall squarely within the area of disclosure and protection of personal data, not only in British archives but in public administration in general.

3.2.4 Protection and Disclosure of Personal Data in UK Archives and Public Administration

For the protection of personal data in records and archives and closure periods, the protection generally applies during the lifetime of the person concerned (closure period of lifetime). British archival science after the turn of the millennium concluded—in view of the usually very difficult task of ascertaining whether or not the person concerned in the archives was still alive—that it would rely on a certain exhaustive number of years corresponding to the average life expectancy, and decided on a period of 100 years.[78] Frequently in cases when the age of the person is unknown, the default assumption has been that the person concerned was 16 years old at the time of the record creation—if an adult is concerned. Under certain circumstances, personal data may be disclosed earlier. One situation in which this may be the case is when it is made available for the purposes of science and historical and statistical research. However, a number of rules, as primarily defined by the UK Data Protection Act, must be followed.[79] In general, the right to privacy must not be violated and the principle that disclosure is fair, lawful, and transparent must be respected. In case personal data are disclosed, all safeguards must be complied with and, in principle, such disclosure must not cause substantial damage or distress to the data subject. Although the British Data Protection Act does not explicitly define the term "substantial damage or distress", methodological materials or British common law do characterise

[78] The National Archives, the Society of Archivists, the Records Management Society, and the National Association for Information Management. (2007). *Code of Practice for Archivists and Records Managers under Section 51(4) of the Data Protection Act 1998*. https://cdn.nationalarchives.gov.uk/documents/information-management/dp-code-of-practice.pdf, Sec. 4.1.5, p. 28.

[79] Data Protection Act 2018. On the archiving of personal data and their protection in archives, cf. methodological material document by the British National Archives. *Guide to Archiving Personal Data*. (August 2018). https://www.nationalarchives.gov.uk/documents/information-management/guide-to-archiving-personal-data.pdf. As a side note, it needs to be mentioned that the procedures for access to information and records in Scotland differ slightly under the Scottish Freedom of Information (Scotland) Act 2002.

it in some way. They see substantial damage mainly in terms of financial loss or physical harm, and they understand substantial distress at the mental level, for example, when emotional or mental pain, significant distress or resentment is caused to the subject, or when a legitimate impression is given that an immoral act has been committed.[80] Passages from the British Freedom of Information Act can also be used; these define one of the exemptions to the right of access to information as data that would jeopardise a person's physical or mental health or safety.[81]

The protection of personality and personal data in records and archives is included within the scope of the duty of confidentiality and the public interest test, as discussed in detail above. However, this obligation represents only one of a number of other circumstances, conditions, that is, a part of the context in which the basic mechanism for testing the proportionality of the public interest in disclosure or non-disclosure takes place. The British Data Protection Act frames the whole process by the obligation that personal data must be processed lawfully and in a fair, proportionate way.[82] But what does it mean?

It is again the British decentralist approach that leaves such an assessment to individual public authorities, in one case to the archives. Archives have to consider a number of phenomena and related circumstances when deciding whether to disclose records containing personal data.[83] They must take into account the nature of the information that is to be disclosed, that is, assess its sensitivity with regard to the potential risk of harm to the public interest of the person concerned. The age of the information and its context are assessed, bearing in mind that the sensitivity of the information fades with its "age", which the overall assessment should also reflect. The person whose data is concerned must not be forgotten. A different approach is applied in the case of working documents of political and public figures, on the one hand, and personal matters and records of a purely private nature, on the other. Another important factor is, whether

[80] "[S]ubstantial damage would be financial loss or physical harm; and substantial distress would be a level of upset, or emotional or mental pain, that goes beyond annoyance or irritation, strong dislike, or a feeling that the processing is morally abhorrent." The National Archives. (August 2018). *Guide to Archiving Personal Data*, pp. 15–16. See also p. 31–34.

[81] Freedom of Information Act 2000, Sec. 38 (2).

[82] Data Protection Act 2018, Sec. 2 (1).

[83] A certain summary can be found in The National Archives. (August 2018). *Guide to Archiving Personal Data*, Sec. 77–84, pp. 32–35.

the information has already been made available to the public, as such data should typically be available to the public.

Another circumstance that is usually placed on the scales of the proportionality of interests test is the manner in which the information is disclosed. A stricter regime and much more careful research must be carried out in cases when the data are to be disclosed to the general public, for example, on the web, and are not intended only for individual access, for example, in the archive research room. Ease of access to information thus stands out as one of the factors.[84] The argumentation on this point by the British National Archives is also remarkable. The difference is largely determined by whether the general disclosure, for example on the web, allows the use of fulltext search tools and it is thus possible, for example, to search archives, records, or information by names of persons or other criteria. One significant threat may also be mentioned, that of the increasingly significant risks associated with the use of automated remote methods of reconnaissance and mining of (personal) data made available in the online environment.

Similar forms of retrieval and mining of (personal) data, on the other hand, would not be possible in the context of individual access to records in, for example, the archive research room, assuming the absence of, for example, indexes or other search aids, especially those published in fulltext online. In the analysis of the British National Archives in the light of the Data Protection Act, the possibility of a mere individual consultation would meet the requirement of "fair and proportionate" access to data subjects, whereas online publication with the new option of remote searching of personal data would not. The reason for why access would no longer be fair and proportionate in this case is that by using name search tools in online access, the researcher may not be sufficiently aware of the archival context or age of the information found.[85]

On a side note, a similar moment occurred in a recent case in the Czech Republic; in 2019, legal columnist Tomáš Pecina was fined CZK 50,000 by the Office for Personal Data Protection for publishing a database of court hearings containing information about the date of the hearing, the

[84] The National Archives. (August 2018). *Guide to Archiving Personal Data*, Sec. 79–81, p. 34.

[85] The National Archives. (August 2018). *Guide to Archiving Personal Data*, Sec. 79, p. 34.

location, the name of the judge, and the names of the participants.[86] He obtained this data from publicly available content published in a database operated by the Ministry of Justice, which, however, includes data on ongoing or future hearings. He also published non-pseudonymised judgements of the Supreme Administrative Court, which also publishes them, but in full non-pseudonymised form only for 14 days, whereas in Pecina's database their full wording was available permanently. Pecina's database could also be searched by the names of the parties or judges, while the database of the Ministry of Justice only allowed searches by case file numbers.

When considering access to archival material—as the British National Archives points out—particular attention needs to be paid to photographs, drawings, and the like. Even photographs that are not linked to specific names may carry personal data, for example in that they show the persons concerned in certain situations (arrest, medical treatment, etc.). Similarly, personal data can be found in materials such as maps, plans, but also in digital records where one would not expect to find them, such as geographic databases. However, when assessing whether or not to disclose records, the record creators and the archives should also assess the data credibility, its accuracy, and completeness.[87] The implementation of the European Convention on Human Rights into the British legal system through the Human Rights Act 1998 has also had an impact on British law, and it is gradually reflected in the common law.

3.2.5 Post-mortem Personality Protection in the United Kingdom

Finally, let us briefly mention the phenomenon of post-mortem personality protection in the United Kingdom. Unlike, for example, Germany—as

[86] Příkaz Úřadu na ochranu osobních údajů [The Office for Personal Data Protection Order], ref. no. UOOU-05226/19–3 of 5 February 2020. The case is described in Pánek, J. (2020, 7 February). Justiční aktivista dostal pokutu 50 tisíc za databázi soudních jednání [Judicial activist fined 50,000 for court hearings database]. https://www.idnes.cz/zpravy/domaci/tomas-pecina-databaze-soudnich-jednani-archivace-data-jmena-urad-osobni-udaje.A200207_075022_domaci_iri

[87] National Archives, the Society of Archivists, the Records Management Society, and the National Association for Information Management. (2007). *Code of Practice for Archivists and Records Managers under Section 51(4) of the Data Protection Act 1998*, Article 4.9.4, p. 37.

we have seen above—there is no general post-mortem protection, which also applies to the archival sector.[88] The FOIA does not provide a specific exemption from access to information for deceased persons. In the case of a FOIA exemption for personal information, the exemption then applies only to living persons. Post-mortem protection is thus only partially implemented in certain contexts and using other tools, some of which we have discussed in a different context above. It includes in particular the duty of confidentiality.

The duty of confidentiality in relation to the deceased is most often invoked in the United Kingdom in the case of medical records and information about the deceased's health, but cases involving other records have also been addressed by the courts. An important factor is whether the information in question was originally received from the deceased person or from another public authority, as one of the conditions for exempting confidential information from FOIA stipulates.[89] In addition to medical records, the British ICO mentions banking or social care records as examples of record categories that may be subject to confidentiality even after a person's death.

Cases can be found in the common law in which post-mortem personality protection at the level of the duty of confidentiality has been recognised. Let us mention one illustrative court case for all: In the case of Bluck v. the ICO and Epsom and St Helier University NHS Trust,[90] the plaintiff, the mother of the deceased daughter, requested access to sensitive personal data from the medical records of her deceased child. The

[88] On the phenomenon of post-mortem personality protection in the United Kingdom cf. Harbinja, E. (2017). Post-mortem privacy 2.0: theory, law, and technology. *International Review of Law, Computers & Technology*, 31(1), 26–42, https://doi.org/10.1080/13600869.2017.1275116; Edwards, L., Harbinja, E. (2013). Protecting Post-Mortem Privacy: Reconsidering the Privacy Interests of the Deceased in a Digital World. *Cardozo Arts & Entertainment Law Journal*, 32(1), 83–130. On the situation in the British common law cf., for example, pp. 102–103. See also two interpretations prepared by the ICO: Information Commissioner's Office (ICO). *Information Provided in Confidence (Section 41). Freedom of Information Act*. https://ico.org.uk/media/for-organisations/documents/1432163/information-provided-in-confidence-section-41.pdf; Information Commissioner's Office (ICO). *Information about the deceased*. Freedom of Information Act. Environmental Information Regulations. https://ico.org.uk/media/for-organisations/documents/1202/information-about-the-deceased-foi-eir.pdf

[89] Freedom of Information Act 2000, Sec. 41.

[90] Bluck v. Information Commissioner and Epsom and St Helier University NHS Trust. UKIT EA – 2006 – 0090, 17 September 2007.

defendant medical facility refused to release the data, claiming that some of the information was confidential. The plaintiff argued that this information had already lost its confidentiality since it had been published in the press, in the court statement, disclosed in correspondence with the plaintiff and so on. The Court therefore examined the records in question in the course of the proceedings and concluded that they contain information which had not yet lost its confidentiality and shall therefore not be disclosed to the plaintiff. At the same time, this judgement contains a detailed analysis of the question whether and in what form the duty of confidentiality can continue after the death of the person concerned (in the section "Did the Duty of Confidence Survive the Death of Karen Davies?").

In addition to the conclusions on very little support under case law, the court decisions were significantly impacted by one of the arguments put forward by the ICO: One practical consequence of a concept that would link the end of the duty of confidentiality to the death of the person concerned would be that "any medical practitioner would then be legally entitled to publish information from the records of a deceased patient, possibly for financial gain". Finally, it is worth mentioning one more point mentioned by the court: "The basis of the duty in respect of private information lies in conscience". The court referred to the case of Coco v. A. N. Clark (Engineers) Ltd. and quoted the words of a High Court judge, Robert Edgar Megarry: "The equitable jurisdiction in cases of breach of confidence is ancient; confidence is the cousin of trust. The Statute of Uses, 1535, is framed in terms of 'use, confidence or trust'; and a couplet, attributed to Sir Thomas More, Lord Chancellor avers that 'Three things are to be held in Conscience; Fraud, Accident and things of Confidence'."[91]

Finally, the post-mortem protection and disclosure of personal data of the deceased in the United Kingdom also echoes the specificity of the British system; when assessing whether or not information about the deceased can be disclosed, even in cases of information provided in confidence, the data controller has to apply the public interest test and consider whether the public interest in disclosing the relevant information does not prevail in any particular case.

In the context of all public interest testing, and a number of assessments of whether or not archives or "living" records should be disclosed,

[91] Coco v. A. N. Clark (Engineers). Ltd. [1968] F.S.R. 415, 1 July 1968.

the British approach is characterised by one very important and distinctive feature, namely that the identity and character of the requestor or researcher and their motivation for requesting disclosure are not taken into account. This represents an emphasis explicitly opposed to the setting that is applied, for example, in the case of the disclosure of archival material of the former state security in Germany in the Stasi Records Archive (Stasi-Unterlagen-Archiv) within the Stasi-Unterlagen-Gesetz. Here, the identity of the researcher plays a very important role and is put on the scales when assessing whether or not the records will be disclosed. In contrast, the United Kingdom's ICO underlines within the FOIA: "Arguments that the information may be misunderstood if it were released usually carry little weight".[92] It relies on the intent of the FOIA in that disclosure of information under FOIA means making it available to everyone, the entire public, and not just one particular researcher. And it also takes into account some case law.[93] In doing so, the ICO stresses that the public interest test is to also consider the public interest of the requestor.[94]

3.3 Conclusion

In summary, the analyses to date show that at the heart of the issue of access to archival records containing data concerning personal privacy and other protected areas of an individual, there is a question of achieving a balance between data accessibility and their protection, while also preserving flexibility in the face of the evolving public interest in access to information. There are several models to address this issue. The above French solution represents a kind of centralist model for managing access to records and archives. First, there exists a central, detailed, and structured system of closure periods, imposing those periods on all entities for a certain part of public records, but the general 30-year closure periods have been eliminated. This system is complemented by a further centralist element approving individual or general derogations; the decision is once again made by a central ministerial body, which in the case of the absolute majority of public archives is the above-mentioned Service interministériel des Archives, or two other ministries of defence and foreign affairs.

[92] ICO, The Public Interest Test.

[93] Christopher Martin Hogan and Oxford City Council v. the Information Commissioner, § 61.

[94] ICO, The Public Interest Test.

At the same time, France represents a large group of countries that underwent a period of oppression imposed largely from the outside. A substantial part of the archives that were open to the general public in France even before the determined general period, originated from the period of Nazi occupation of France and the Vichy regime, which is also the case of Germany, where the specific access regime affects the archives surviving the activities of the security forces and repressive authorities of the former East Germany, as demonstrated above on the example of the disclosure of Stasi records. Central European countries went through two periods of dictatorship, first Nazi, then Communist. These countries then typically open the archives from both these historical periods in a special regime, earlier and on a more liberal scale than would generally be required. This access once again focuses on archival records created by the ruling forces of power and those organisations that participated in the repression.[95]

All these countries thus faced a similar challenge when they needed to come to terms with a previous period of oppression or a totalitarian period of their history, and to do so it was essential for them to gain access to primary historical sources. The motivation for such opening of sources is poignantly expressed in the introduction of the preamble to the Czech Act on the Institute for the Study of Totalitarian Regimes and the Security Services Archive: "Those who do not know their past are doomed to repeat it".[96]

In this context, however, it should be stressed that in France, providing access under the specific regime of derogations to selected, often "sensitive" archives typically happens with a substantial time lag, usually many decades, when the impact of providing access to them in real life, shaping

[95] In the case of the Czech Republic, the special access regime is determined legislatively mainly pursuant to Sec. 37 (11) of Act No. 499/2004 Coll. on Archiving and Records Management amending certain other acts [Zákon o archivnictví a spisové službě a o změně některých zákonů] of 30 July 2004. In addition, the specific regime for the disclosure of the former State Security Service files from the communist totalitarian period is governed by Act No. 140/1996 Coll., on the disclosure of files created in the course of activities on the part of the former State Security Service, and some further acts of 26 April 1996 (Zákon č. 140/1996 Sb., o zpřístupnění svazků vzniklých činností bývalé Státní bezpečnosti ze dne 26. dubna 1996).

[96] Zákon č. 181/2007 Sb. ze dne 8. června 2007, o Ústavu pro studium totalitních režimů a o Archivu bezpečnostních složek a o změně některých zákonů [Act No. 181/2007 Coll. of 8 June 2007 on the Institute for the Study of Totalitarian Regimes and the Security Services Archive, and on Amendments of some Acts].

society's views, and executing public policies are already very limited. This is a striking difference as compared, for example, with the Czech Republic as one representative of post-communist countries, which opened "sensitive" materials from the communist era very soon after its collapse and made them available as early as the period of transitional justice and the emerging new democracy.

However, it is also possible to find quite different models and one of them is applied in Britain. Its most prominent characteristic is something that resonates in some way in virtually every developed archival system, but which the British model of access has placed at the centre as the main pillar of the whole edifice of personality and privacy protection, including the area of archiving—public interest and proportionality testing of individual public interests. Unlike the French centralist solution, however, the United Kingdom heads in a considerably more decentralist direction. Moreover, the British model highlights one of the fundamental problems that almost every advanced system of access to archives must face in the end. It is the question of an appropriate and sufficiently transparent setting of control and decision-making mechanisms and an adequate guarantor, the body that shall monitor and decide on situations of specific access to archives.

The specificity of the British model of access to archives and data protection lies in the establishment of multiple, multi-layered, and multi-faceted testing and examining public interest in the area of access to public records and archives. This is done in several phases; the first phase is carried out by the record and information creator, and the second phase then in the case of *historical records* (i.e., in the British legal system, records created more than 20 years ago) by the archives and at certain points at the national level by a specialised independent body: the Advisory Council on National Records and Archives. This Council gives voice not only to administrative officers and representatives of the broad spectrum of public administration but also to archivists, historians, and journalists, that is, professional groups substantially represented within the Advisory Council. This diversified network is also joined by the ICO, the United Kingdom's independent authority set up to uphold information rights, access to information, and privacy protection that provides its opinions, analyses, guidance materials, as well as legal actions. Ultimately, however, the entire justice system has a very important say, as common law and judicial precedents also form an important part of the British legal system.

In summary, the British approach is characterised by multi-faceted control and the existence of a range of mechanisms that guarantee the application of multiple public interests entering the field of access to records and information from different sides and perspectives. At the same time, the British system has a very elaborate and sophisticated notion of *public interest* in the area of access to information, records, and archives and the protection of data contained therein. A distinctive feature is the diversified system of testing at different levels and from different perspectives: testing public interests and their proportionality; testing the justification for the application of exemptions from the general right of free and immediate access to information; testing proportionality when assessing whether to breach the obligation of confidentiality; or testing the risks of harm to various interests entering the field defined on the one hand by the desire for maximum possible openness and transparency of public authorities, and by the need to protect data that deserve such protection, including the protection of personality on the other.

All these tests have a common denominator: Developments at all levels over the last two decades or so have led to the need to seek balance and proportionality in taking account of the somewhat conflicting public interests in access to and protection of information. At the same time, the British system is characterised—in contrast to, for example, the French more centralist approach—by a decentralist approach, where the public authority itself, in one case the archive, is the basic actor in the multi-layered assessment of access not only of information from "living" records but also of archival records. The British system allows it a very wide competence and expects its responsibility in testing, weighing, and assessing the diverse public interests in this field. However, thorough control mechanisms are in place, not only at the judiciary level but also in the form of expert advisory bodies, for example, for institutions at the national level it is the *Advisory Council on National Records and Archives.*

Finally, the British system seeks to implement equal access to requestors for access to public information and archival records, as the British Prime Minister Harold Wilson tried to promote in the 1960s when he cited the risk of creating animosity between a certain group of "vetted" historians

as one of the arguments against allowing access.[97] The person of the researcher and their motivation should play virtually no role in the decisions on access to information. Underlying this attitude is the fact that the British system wants to see a responsible and intelligent citizen who does not need to have the contents of records and archives interpreted, explained, and possibly not made available, all for fear that the information in them might be misunderstood. Along with this, the British approach—unlike the above French model, which differentiates between general and individual derogations—works with the understanding that even when information or archival records are disclosed to one particular person, it is done with the knowledge that in such a case it can be disclosed to anyone else. This is also inherent in the intent of the British model, which continually stresses that access to information/archives should be framed at a general level by a fundamentally public and not private interest in opening a relevant piece of information. The British model of access to public information, records, and archives thus finds alien the concept to which the British themselves refer to as "privileged access" taking into account the person of the requestor and differentiating modalities of access to records according to the identity of the researcher, as implemented, for example, by the German Stasi-Unterlagen-Archiv.

All of the above-mentioned characteristics of the policy of access to public archives, as well as records and information, and at the same time their protection, can, at least in some respects, become quite inspiring for other archival systems, especially those that still lack a sufficiently well-developed policy and procedural setup for access to archives and data protection in them.

[97] Harold Wilson argued, among other things, that: "It would not be easy to devise a procedure for selecting 'established' historians which would not cause resentment and perhaps, in the long run, undo the goodwill generated by a decision in principle to allow freer access". Wilson, K. (Ed.). (1996). *Forging the Collective Memory. Government and International Historians through Two World Wars.* Berghahn Books, item 6b, p. 291.

CHAPTER 4

The Paradox of Archiving: Personality Protection and a Threat in One—Archives and Child Sexual Abuse

On a general level, it has always been the case that the best form of protection of certain data is simply to destroy the data in question or the medium. Misuse of personal data in records and archives can often occur a considerable time after their creation, as some of the examples mentioned above have indicated. Chapter 7, will provide more detail on several specific cases of such misuse and efforts to reduce personal data in records even before they are transferred to the archive for permanent archiving. These will concern mainly census records and their management. In this context, it is not without relevance to argue that any archiving, that is, long-term preservation of data with a vision of the preservation hypothetically lasting indefinitely, always poses a potential threat to the protection of personality and privacy of citizens.

In the coming years and decades, archiving will have to expose the issue of long-term and even permanent preservation of records more in the perspective of the risks of misuse of the data that archives maintain in their vaults. In this respect, archives mirror the phenomena that can be observed in the management of "live" records and information, and the all-too-apparent growing risks of data misuse, particularly in the online environment. In the future, archives as well as record creators will need to more carefully consider the protection of personality and privacy, especially from the perspective of data (including personal) preservation as such, and this perspective should also be considered much more strictly in the application of legal procedural tools of records and data destruction within the

M. Čtvrtník, *Archives and Records*,
https://doi.org/10.1007/978-3-031-18667-7_4

retention and shredding procedures carried out by the archives and record creators. This particular topic will be addressed later in Chap. 8.

Perspectives on the protection of the individual are usually based primarily on the question of how a person and their personality rights may be harmed by the retention and disclosure of data concerning this particular individual. Hence the intentions of the European GDPR to allow for the "minimisation" and "storage limitation" when it comes to personal data and the correlating "right to be forgotten" ("right to erasure"). Although these intentions apply primarily to data controllers other than archives, most often of private law provenance, they also apply to archives.

Along with this trend, however, the opposite perspective proportionally fades, which is the starting point of the following subchapter: Apart from the risks associated with the preservation and disclosure of personal data, archiving in the public interest is also one of the tools by which the protection of personality rights can be implemented, even enhanced. Permanent preservation of certain categories of personal data is not only necessary for various future research purposes and official interests, as Terry Cook pointed out in his study for UNESCO in the early 1990s,[1] but in some cases such preservation becomes the key guarantee of the protection of personal as well as other human and civil rights. I will demonstrate this thesis on some specific cases. An analysis of the opposite situation, in which personal data, especially in archival records, have been misused, will be discussed in more detail in Chap. 7.

[1] "There are certain categories or classes of records containing personal information which should be preserved by archivists around the world. These records may not necessarily be stored physically in the national archives and may be created by state or provincial and local or municipal governments. Nevertheless, their importance to research by providing the core demographic profile of the nation, to individuals' legal rights, and to government administration is incontestable. Archivists should collectively ensure that these categories of personal information records are safeguarded." Cook highlights in particular civil registers, land registers, census records as well as some other record categories. Cf. Cook, T. (April 1991). *The archival appraisal of records containing personal information: A RAMP study with guidelines.* PGI-91/WS/3. Paris.

http://www.nzdl.org/gsdlmod?e=d-00000-00---off-0hdl--00-0----0-10-0---0---0direct-10---4-------0-1l--11-en-50---20-about---00-0-1-00-0--4----0-0-11-10-0utfZz-8-10&cl=CL1.1&d=HASHe14ace1b9d178e777de9c9.8&gt=2, Sec. 22.

4.1 Odenwaldschule and Records Testifying to Sexual Abuse of Children: Premature Archival Records Management

In 2010 Germany, a case emerged of widespread, systematic, and long-term sexual abuse of children since the 1990s by the teaching staff, including the headmaster, at the Odenwaldschule reform school in the Hessian town of Heppenheim.[2] The school went bankrupt as a result of these facts coming to light, and in this context the question of what would happen to the school's surviving records began to be addressed. For the most part, these were records for which the retention periods had not yet expired, that is, materials that should normally remain with the creator and, if that was not possible, a liquidator should be the one to take care of them, ensure their preservation until the end of the retention period when the records could be transferred to the relevant archives or legally destroyed if deemed without value.

However, such a development did not occur. Immediately after the case broke out, some sensitive personal data were leaked to the public. This became one of the reasons why the Hessian State Archives in Darmstadt stepped in to store the school records. Following a consultation with the State Prosecutor's Office, the Hessen Archives decided to take over the school records before the expiry of the retention periods, with the proviso that the final archival selection would be made after they had expired. In the case of the Odenwaldschule records, the Hessian State Archives took on the role of the so-called intermediate archives (in German terminology, a "Zwischenarchiv"), that is, a place on the borderline between a registry managing actual "living" records and a historical archive preserving definitive, historical archives. At the same time, the archive is already beginning to address the question of whether it will eventually proceed to the permanent archival preservation of all of the approximately 5500 student files, or whether it will reduce their quantity. Developments in the demand for the

[2] On this case, cf. a contribution at the German Archival Congress in Rostock in 2018 Kistenich-Zerfaß, J. (2018). Überlieferungsbildung, Erschließung und Nutzung im gesellschaftspolitischen Fokus: Der Bestand "Odenwaldschule" im Hessischen Staatsarchiv Darmstadt. Conference: Verlässlich, richtig, echt: Demokratie braucht Archive! 88. Deutscher Archivtag in Rostock. Cf. Čtvrtník, M. (2019). "Spolehlivé, správné, pravé—demokracie potřebuje archivy!". 88. německý archivní sjezd v Rostocku 2018 ["Reliable, correct, true—democracy needs archives!". 88th German Archival Congress, Rostock 2018]. *Archivní časopis* [*Journal on Archives*], 69(3), 295–314, p. 311.

records in question will certainly play a role. Currently, there are several research projects that would like to use these materials. Still, the situation of scientific research in 10 or 20 years is hard to predict.

The timely scientific extraction of the data contained in the Odenwaldschule records was ultimately the second factor that led the Hessian Archives to accept the school records for premature archiving. The Archives also received materials that would otherwise have been destroyed in the shredding process.

The documents and archival records of sexual abuse are one of those groups of historical sources that raise the acute question of the relationship between the actors themselves and the materials that testify about them. It was thematised in 2016 by the newly established German Independent Commission for the Processing of Child Sexual Abuse (Unabhängige Kommission zur Aufarbeitung sexuellen Kindesmissbrauchs); its 2019 meeting gave the floor to Max Mehrick, a former pupil of a private boarding school in Hessia where he was a victim of sexual violence. From the victim's perspective, Mehrick sees the surviving school records as part of the abuse itself, which further supports the exercise of power by the then perpetrators and undermines the dignity and self-determination of the victims. "That, what humiliates is archived together with the record."[3]

Mehrick's view of archived sources highlights a perspective that is often neglected by archivists and researchers, namely: What is the relationship of the actors themselves to the material telling about them? Would these actors wish someone else would see and read the records?! This question affects a large part of archival wealth, and at the same time it invades the field of personality and privacy protection of the actors of archival records.

In doing so, it reveals some fundamental differences between the groups of records and the motivations of their actors. There is a difference between the interest of the representatives of political power, the minister, the mayor, the high state official not to disclose "their" materials and the interest of the victim of sexual violence. In the first case, the public interest of transparency and controllability of the exercise of public political power clearly prevails; on the contrary, in the latter case the protection of the personality and privacy of the actors must be taken into account and the

[3] Tagung "Archive und Aufarbeitung sexuellen Kindesmissbrauchs". Unabhängige Kommission zur Aufarbeitung sexuellen Kindesmissbrauchs, Darmstadt 2019. https://www.aufarbeitungskommission.de/meldung-27-03-2019-tagung-archive/.

victim's right "to be forgotten" needs to be considered; this term is being increasingly used in the context of European law since the GDPR introduced the "right to be forgotten" as one of the rights of EU citizens, applicable to records of private and public entities under certain conditions. Similarly, the situation is quite different when it comes to access to the archives of divorce cases, where the primary concern is to preserve the confidentiality and privacy of the persons concerned, and, for example, the files of a criminal tribunal dealing with crimes against humanity, where the society's right to know what crimes have been committed and how law and justice have dealt with them clearly prevails.

In the case of the Odenwaldschule records, the Hessian Archives has chosen, at least for the time being, a solution that combines two notions. On the one hand, the Archives is aware that society has a right to know as much information as possible about a school that has become one of the prominent symbols of child sexual abuse in Germany. For this reason, it has decided to digitise and make available as much of the school's documentation as possible and publish the digitised versions on the web, and to do so as soon as possible. These include mainly the school's organisational regulations. On the other hand, it must respect the protection of the personality of the pupils, a significant number of whom have been victims of sexual abuse in the past. Files relating to pupils will remain inaccessible and will only be used for research purposes, investigations, or other official purposes. Of the total amount of over 270 linear metres of preserved records (of which 60 linear metres are photographs), approximately two thirds are available to the public as of 2020.[4]

The case of the Odenwaldschule records demonstrates that archiving does not only pose a potential risk of future unauthorised or at least ethically questionable intrusions into the privacy and protected sphere of personality of those concerned in the records, but it also fulfils the role of protecting them. The motivation for the premature transfer of the records containing data on sexual abuse was to protect the personality of the abused children on two levels: first, to prevent any unjustifiable leak of the data to the public; second, to analyse these extremely serious crimes as thoroughly as possible, both officially and scientifically, with the aim of eliminating them to the greatest extent possible in future.

[4] Odenwaldschule archival fonds (OSO), 1880–2015, HStAD Bestand N 25, Hessisches Staatsarchiv Darmstadt. The fonds description: https://arcinsys.hessen.de/arcinsys/detailAction.action?detailid=b8034.

The Odenwaldschule case has shown that public archives in Germany are, in principle, a trustworthy place for public administration and society to store even very sensitive material. Although archives take custody of records for the most part only when their greatest sensitivity has passed, this is far from always the case, as illustrated by many of the cases I have touched on so far. Public archives, like any other entity, acquire this credibility only through the long-term responsible and secure care of the material entrusted to them. In the following section, also in connection with the archiving of records testifying to child sexual abuse, I will point out quite the opposite, a case when archives and in particular their founder and administrator, in this case the Roman Catholic Church, have suffered a massive loss of credibility in the last quarter century or so.

4.2 Church and Child Sexual Abuse: Access to Archives as a Form of Protection

"In the administrative office of the Diocese of Altoona-Johnstown, across from the Bishop's Office was an unmarked door containing multiple filing cabinets and boxes. This unmarked door was between the large reverent portraits of Bishop James Hogan and Bishop Joseph Adamec. Some of the filing cabinets were marked "Priests Personal", "Deceased Clergy", "Priests who left the Clergy", and "Confidential Litigation Files". Some of the boxes were marked "Luddy Litigation" and "To Be Opened Only by the Bishop or Secretary of Temporalities". Inside the filing cabinet marked "Confidential Litigation Files", Special Agents found files for Priests who were accused of sexual misconduct. The filing cabinet held four drawers, all four drawers had files. The "Secret Archive" was a safe contained in a cabinet in the Bishop's Office. This safe was under lock in which only the Bishop had the key. This safe contained one file pertaining to a Franciscan Friar, Brother Stephen Baker. Another room contained a filing cabinet marked "Confidential Litigation Files". This filing cabinet was also four drawers and contained files labeled by the victim's names. As Special Agents of the Office of Attorney General stood inside an organization devoted to the tenets of scripture and morality, they found themselves surrounded with evidence of an institutional crisis of child sexual abuse. Agents did not find a couple files in a drawer which alleged child molestation, but rather boxes and filing cabinets filled with the details of children being sexually violated by the institution's own members […] Approximately 115,042 documents were removed from the Diocese. This total does not include

the electronic data seized pursuant to the warrants. Within these documents were the hand written memoranda of Bishop James Hogan; letters and documents of Bishop Joseph Adamec; numerous sexual abuse victim statements; letters from sexual abuse victims; correspondence with offending priests and internal correspondence. […] The Diocese of Altoona-Johnstown was in possession of a massive amount of data detailing a dark and disturbing history."[5]

This is how the police search of the office of the Bishop of the Diocese of Altoona-Johnstown in the state of Pennsylvania, USA, was conducted. Stephen Baker, the Franciscan friar whose file was locked in the "secret archive" and whose case was at the heart of the subsequent extensive Pennsylvania-wide investigation, had been dead for several years at the time the report was released, having committed suicide in 2013 after his crimes of multiple child sexual abuse came to light.

Serious allegations of a huge number of cases of child sexual abuse by Catholic clergy in the state of Pennsylvania led to the convening of a grand jury. Its extensive investigation was conducted in every diocese of the Roman Catholic Church in the state of Pennsylvania and resulted in two exhaustive reports: the first the 147-page 2016 report cited above detailing sexual abuse in the Diocese of Altoona-Johnstown, and the second a 2018 summary concerning the remaining Pennsylvania dioceses of Allentown, Erie, Greensburg, Harrisburg, Pittsburgh, and Scranton, totalling a breath-taking 884 pages.[6]

The investigation confirmed massive sexual abuse by approximately 350 clergy and other church officials continuing for over seven decades in the state of Pennsylvania. The findings showed that of the approximately 5000 priests in the period under review, approximately 8% were credibly accused of sexual abuse by victims; more than 1300 children were affected. The reports revealed the unimaginable scope of sexual abuse cases in the Pennsylvania dioceses and unveiled the deliberate and systematic concealment of cases from the public and law enforcement by church dignitaries, among them the appointed bishops at the time, Joseph Adamec

[5] Commonwealth of Pennsylvania. Office of Attorney General. (March 2016). *A Report of the Thirty-Seventh Statewide Investigating Grand Jury*. http://www.bishopaccountability.org/reports/2016_03_01_Pennsylvania_Grand_Jury_Report_on_Diocese_of_Altoona_Johnstown.pdf, pp. 10–11.

[6] Commonwealth of Pennsylvania. Office of Attorney General. (2018). *Report I of the 40th Statewide Investigating Grand Jury*. Redacted By order of PA Supreme Court 27 July 2018. https://www.attorneygeneral.gov/wp-content/uploads/2018/08/A-Report-of-the-Fortieth-Statewide-Investigating-Grand-Jury_Cleland-Redactions-8-12-08_Redacted.pdf.

(a descendant of Slovak immigrants to the USA) and James Hogan. Although the grand jury ultimately did not bring charges (due to the deaths of the perpetrators, their high age, the inability of the traumatised victims to testify, etc.), the published results of its investigation radically exposed the massive nature of the crimes committed, including the deliberate efforts of high church dignitaries to cover these up.

The Pennsylvania child sex abuse scandal eventually came to a head after Cardinal Donald William Wuerl, bishop of the Diocese of Pittsburgh from 1988 to 2006, then archbishop of Washington, one of the church's dignitaries who, according to the report, covered up child abuse in his diocese and appointed clergymen with serious allegations of sexual abuse to other priesthood offices,[7] resigned from office in 2018. While accepting the resignation, Pope Francis was very lenient in his comments towards the resigning Wuerl and his role in the whole affair, and he praised Wuerl's work in general. This move outraged some of the abuse victims.

This book does not intend to recapitulate the sufficiently publicised cases as such, it rather wants to highlight the significance of the phenomenon of preservation and access to records, including archives.

The perception we saw in the previous section with Max Mehrick, one of the victims of sexual abuse at the Odenwaldschule boarding (not church) school, that the surviving school files are part of the abuse itself and further support the exercise of power by the perpetrators at the time, is rather unique and would only be justified if the sensitive files remained in the custody of the institution where the abuse took place. But this was not the case with the Odenwaldschule, which ceased to exist and whose records were transferred into the care of the public Landesarchiv. Moreover, as the Australian inquiry has shown, and which will be discussed below, the Australian victims themselves saw the inaccessibility of records testifying about their sexual abuse as a greater problem than the continued retention of such records.[8]

The underlying problem is the very status of ecclesiastical records as these are not categorised as public but rather as private ones. For this

[7] Commonwealth of Pennsylvania. Office of Attorney General, *Report I of the 40th Statewide Investigating Grand Jury*, passim, for example, pp. 222–229, 232, 244, and other parts of the report.

[8] Royal Commission into Institutional Responses to Child Sexual Abuse. (2017). *Final Report, Recordkeeping and information sharing*, vol. 8. Commonwealth of Australia. https://www.childabuseroyalcommission.gov.au/sites/default/files/final_report_-_volume_8_recordkeeping_and_information_sharing.pdf, p. 11.

reason, they are not normally subject to the legislative requirements imposed on public records and archives, in particular the obligation of preservation, the obligation to offer each record to the public archive for retention and to leave it to the public archive, as a public authority, to decide which records are to be archived and which can be destroyed. Public control over church records is therefore extremely limited at this level and can only be exercised by public entities in the context of investigation mandated by law enforcement authorities or when the Church itself allows it. This situation also applies to the specific so-called secret archives existing in the Roman Catholic Church.

Archives, including the "secret archives" are codified in the Codex Iuris Canonici in Canon 486–491.[9] The Codex requires each diocese to establish its own diocesan archive "in which instruments and written documents which pertain to the spiritual and temporal affairs of the diocese are to be safeguarded after being properly filled and diligently secured" (Can. 486, § 2). The Codex also lays down rather strict rules on access to archival records maintained in the archives.

In addition to this "unclassified" archive, each diocese also establishes a "secret archive" with a different and much stricter access regime. While the keys to the "ordinary" archives are held not only by the bishop but also by the chancellor, and access can be granted by the bishop, the chancellor or the director, the key to the secret archives is held by only the bishop. Unlike an unclassified archive, in the case of a secret archive, the Codex Iuris Canonici does not explicitly provide for the possibility of granting access to other persons. While records may be removed from unclassified archives for a short period of time, again with the permission of the bishop or the director of the curia and the chancellor, it is expressly forbidden to remove any documents from the secret archive or safe (Can. 490, § 3). The secret archive must be secured so that it cannot be moved.

The Codex Iuris Canonici is brief on the content of secret diocesan archives. They hold records that are supposed to remain secret. They should maintain, inter alia, records establishing the warnings or rebukes or other documents evidencing some sort of reprimand (Can. 1339, § 3). They hold criminal investigation files and related documentation under canon law (Can. 1719). In the context of the utterly inadequate provisions in relation to the secret archives, a single provision indicates the content of the secret archives in relation to records documenting sexual abuse by

[9] *Codex Iuris Canonici (CIC)*, 1983.

Church officials: “Each year documents of criminal cases in matters of morals, in which the accused parties have died or ten years have elapsed from the condemnatory sentence, are to be destroyed. A brief summary of what occurred along with the text of the definitive sentence is to be retained” (Can. 489, § 2). A significant part of the secret archives of the Roman Catholic dioceses thus consists of records and archives concerning “criminal cases in matters of morals”, in other words, material testifying to cases of sexual abuse in particular. It is these documents that constitute the key documentary evidence enabling the reprehensible acts committed by church officials to be substantiated.

The archiving of Church records in the context of the protection of personality rights and the absolute failure of the Church to address the issue of child sexual abuse exhibits several fundamental flaws that have throughout time contributed significantly to the massive and worldwide expansion of this criminal activity perpetrated by Church officials. These are in particular: The hierarchy concentrated in the role of the bishop is too strong and not limited by sufficient control mechanisms. Only the bishop has access to the secret archives. In relation to the function of the archive and the secret archive, there are virtually no control mechanisms established both from outside and from within the Church. Finally, up to and including 2019, the access to records relating to sexual abuse was significantly restricted by the application of the so-called papal secrecy under canon law. It was only Pope Francis who removed the papal secrecy from the records relating to cases of violence and sexual assaults committed under threat or abuse of authority, cases of abuse of children and vulnerable persons, child pornography, and the failure to report or cover-ups by bishops, superior generals, and other top Church officials.[10] This step should lead to greater cooperation between church authorities and the state and law enforcement authorities in detecting and proving the crimes in question.

All these moments manifested in most of the gradually proven cases of sexual abuse in the Church, usually at the level of concealing these crimes, often by bishops as the exclusive custodians of this “sensitive” information, which was to be maintained in secret archives. Bishops often

[10] Rescriptum ex audientia SS.MI: Rescritto del Santo Padre Francesco con cui si promulga l’Istruzione Sulla riservatezza delle cause, cause (2019, 17 December). With reference to the Apostolic Letter Issued Motu Proprio by the Supreme Pontiff Francis “Vos Estis Lux Mundi” (2019, 7 May). Art. 1 referring to Art. 6.

transferred the offenders to other locations, allowing them to continue this serious criminal activity.

Ultimately, the fundamental flaw lies in the Codex Iuris Canonici and the rules it sets for the record preservation centrally for all church archives. First, records of "criminal cases in matters of morals" are for the most part not intended for permanent archiving, but on the contrary they are determined for destruction after the expiry of the retention periods. After these periods, only the final judgments and a brief summary of the facts are retained. Second, all material other than these final judgments and brief summaries is subject to a retention period of 10 years following the closing of the case by way of a conviction by the ecclesiastical court, or it is subject to immediate destruction following the death of the offender. It is obvious that this period is extremely short. It is completely inconsistent with the often very long interval after which a victim of abuse is able to testify, press charges, and take appropriate legal action, nor does it correspond in principle to the statute of limitations for child abuse offences under criminal law. What is more, statutes of limitations for these categories of crimes are being extended throughout the world in recent years and in some cases they have been eliminated altogether. In Germany, for example, the most recent extension took place in 2015; the period is now 20 years, but only starts when the victim turns 30. In 2013, the Netherlands abolished all statutes of limitations for serious sexual abuse offences, with the minimum penalty of eight years. The United Kingdom has no statutes of limitations for such crimes.

The excessively short retention periods of material relating to cases of sexual abuse maintained in secret diocesan archives have been criticised by the Australian government-established Royal Commission into Institutional Responses to Child Sexual Abuse, dealing with child abuse throughout society not only in the Church. In its final comprehensive extensive report in 2017, it provided a total of 189 recommendations (80 of which related directly or indirectly to the Catholic Church) and in one of them it proposed that the Australian Catholic Bishops Conference petitions the Holy See to amend the relevant provisions of the Codex Iuris Canonici so that records are not destroyed after the death of the perpetrator, or 10 years after their canonical conviction, but that this period be

extended to 45 years.[11] It needs to be noted that the Commission recommends the same 45-year retention period for records relating to child sexual abuse of all institutions, not solely the Church.[12] The Commission has also recommended that the National Archives of Australia and other regional archives and public records custodians establish retention (shredding) periods of at least 45 years for records that may provide evidence of child sexual abuse (ibid., Recommendation 8.2).

The Australian Catholic Church reacted promptly to the Commission's recommendations and accepted and supported the vast majority of them, including the extension of the retention periods[13] (it did have doubts, however, regarding the seal of confession and it left two crucial recommendations to be further discussed with the Holy See: (1) breaking the seal of confession when the content of the confession is the testimony of a sexually abused child; (2) when the confession is made by the perpetrator of sexual abuse against a child, should absolution be granted only after the perpetrator has turned himself in to civil [non-canonical] law enforcement authorities?[14] Especially in the case of the latter recommendation, it is very surprising that it has not been applied in the confessional practice of the entire Roman Catholic Church for a long time). Already in 2018, it approached the Holy See to make the relevant adjustments in the canon law and to extend the retention periods to a minimum of 45 years, taking into account, among other things, the extending statute of limitations for offences of sexual abuse of minors. At the same time, the Australian Catholic Bishops Conference will prepare a new methodology recommending a retention period of at least 50 years for these records.

For comparison, we can mention yet another enormously large research study commissioned by the Association of German Dioceses and

[11] Royal Commission into Institutional Responses to Child Sexual Abuse. (2017). *Final Report. Religious Institutions*, vol. 16, Book 1, Commonwealth of Australia. https://www.childabuseroyalcommission.gov.au/sites/default/files/final_report_-_volume_16_religious_institutions_book_1.pdf, Recommendation 16.17, p. 75.

[12] Royal Commission into Institutional Responses to Child Sexual Abuse. (2017). *Final Report, Recordkeeping and information sharing*, vol. 8, Recommendation 8.1, p. 22.

[13] Australian Catholic Bishops Conference and Catholic Religious Australia's Response to the Royal Commission into Institutional Responses to Child Sexual Abuses. (August 2018). https://www.catholic.org.au/acbc-media/media-centre/media-releases-new/2139-acbc-and-cra-response-to-the-royal-commission/file, p. 16.

[14] Australian Catholic Bishops Conference and Catholic Religious Australia's Response to the Royal Commission into Institutional Responses to Child Sexual Abuses, Recommendation 16.26, p. 21.

published in 2018 by an independent consortium of several different research organisations in the fields of criminology, mental health, and gerontology. It should be noted, however, that the researchers did not have direct access to the incriminated records and could only rely on the data supplied by the individual dioceses via questionnaires. The report covered the period from 1946 to 2014 and used data from personal and investigative files on 38,156 clergymen of the Roman Catholic Church. Of this number, 1670 clergymen were found to have allegations of sexual abuse of minors, representing a total of 4.4 % of the clergy from that period.[15] There were 3677 documented minor victims. But the total number will almost certainly be higher, given the destruction of an undetected number of files, as I will specify below. Based on the documented cases, there were a total of 2.5 victims, that is, alleged accusations per one offender. In an analysis of the surviving criminal files of the canonical criminal proceedings, this ratio was found to be as high as 3.9 victims per one accused cleric.

Based on empirical research, the report shows that the impacts and burdens that victims bear for a very long time and often their entire lives are very high;[16] it also provides important and explicit findings regarding the loss, non-preservation, and tampering with the records that are important for our research. Based on the statements of the German Roman Catholic dioceses, the resulting statistics suggest that 7.4 % of the dioceses do have a history of clergymen destroying records containing references to the sexual abuse of minors and 48.1% of the dioceses (13 dioceses in total) cannot rule out such record destruction.[17] This figure is of far greater significance than the research report deems relevant. Almost half of the dioceses must have implemented poor record management procedures as they are unable to confirm whether any materials were destroyed and, if so, what materials and when were destroyed. The research report highlights, that one of the key factors behind the failure to ascertain the fate of the records was the absence of a requirement to paginate personnel files in dioceses. Any additional changes in personnel files are thus not identifiable, and "file tampering was and is uncontrollable and cannot be ruled

[15] *Sexueller Missbrauch an Minderjährigen durch katholische Priester, Diakone und männliche Ordensangehörige im Bereich der Deutschen Bischofskonferenz. Projektbericht.* (2018, 24 September). https://www.dbk.de/fileadmin/redaktion/diverse_downloads/dossiers_2018/MHG-Studie-gesamt.pdf, p. 5.

[16] Ibid., pp. 316–317.

[17] Ibid., p. 40.

out". The reality is that the vast majority of files are not paginated and it is impossible to determine the extent of tampering.[18]

It is surprising how the German Bishops' Conference interpreted the results of the research report on the report web presentation. It concludes that the concerns regarding too short retention periods and premature destruction of records relating to criminal proceedings in cases of sexual abuse are not justified. Quite surprisingly, the representative body of the Roman Catholic Church in Germany itself is unable to accurately characterise the contents of the secret diocesan archives and expresses hesitation as to the extent to which there actually are case files in matters of morals according to canon law or whether these are more likely to be references to moral offences that did not lead to canonical criminal proceedings.[19] Regardless of the existence of the research report, it is the German Bishops' Conference itself that should know best exactly what the contents of the archives are, including the contents of secret archives of their dioceses.

Francophone Canada has recently chosen yet another model than that of Australia or Germany. In 2019, Montréal Archbishop Christian Lépine appointed the retired judge of the Superior Court, Anne-Marie Trahan, to lead a working group charged with investigating crimes of abuse of minors in the Church from 1950 to 2019.[20] The investigation was initiated by the Church itself. In doing so, Canada chose a person who, on the one hand, emerged from the structures of the non-canonical judiciary and, on the other, stood already outside and, in addition, was significantly involved in church structures, most recently as she sat on the executive council of the Order of Malta of Canada. The ex-judge was given direct access by the Archbishop to the diocesan regular and secret archives. Unfortunately, Anne-Marie Trahan passed away in 2019 and the Archbishop of Montréal will be looking for her successor.

[18] Ibid., p. 252.

[19] Cf. Deutsche Bischofskonferenz, FAQ zur MHG-Studie. https://www.dbk.de/themen/sexueller-missbrauch/faq-mhg-studie/.

[20] See Archbishop's open letter Lépine, Ch. (2019, 27 March). Agressions Sexuelles Faire La Lumière. https://plus.lapresse.ca/screens/bf9f1586-e3ef-4be6-a215-ee24dd05b616__7C___0.html?utm_medium=Facebook&utm_campaign=Microsite+Share&utm_content=Screen&fbclid=IwAR23nBcZLXws4oGGMSxVnklLx8g7yYnD2fbQCwb6DL1uKB4N6KkMgFn-shY. Cf. also Gloutnay, F. (2019, 27 March). Abus sexuels: ce que pourraient révéler les archives diocésaines. https://presence-info.ca/article/societe/abus-sexuels-ce-que-pourraient-reveler-les-archives-diocesaines/.

Unfortunately, Canada brings yet one more sad case for analysis. In recent years, Canada has been shaken by the gradual revelations of the horrors of what has come to be referred to as the genocide or cultural genocide of Indigenous peoples, particularly within the Indian residential school system. It is not the intention of this book to analyse the history of this process, which was designed to isolate Indigenous children from their own culture and religion and assimilate them into the emerging dominant Canadian culture. The shocking findings gradually show not only the enormous extent to which this process has been carried out, but also the violence and atrocities committed against these children by the religious institutions administering the system. In July 2022, Pope Francis II visited Canada to formally apologise to all the Indigenous victims on behalf of the Church. However, the fact crucial for our analysis is the way in which documentation and archiving of materials related to the residential school system was handled.

In 2007, the National Centre for Truth and Reconciliation (NCTR; located at the University of Manitoba in Winnipeg) was established and it is gradually taking shape as a special archive that intends to permanently store the maximum of relevant residential school records collected by the Truth and Reconciliation Commission of Canada and thus contribute to the creation of complete history and legacy of Canada's residential school system. It intends to collect either originals or copies of as much existing documentation as possible testifying to the residential school system and its victims. Federal authorities and other institutions, including some church institutions, are gradually transferring some of their records either through the Truth and Reconciliation Commission or directly to the NCTR, and negotiations are ongoing.[21] In this respect, the NCTR is a documentation centre and, in a way, an archive. Records archiving in the NCTR and providing access to victims and society as a whole is a tool for implementing the protection of the rights of Indigenous peoples in Canada.

In Ireland, the then acting judge, Yvonne Murphy was appointed to lead the investigation into the sexual abuse of minors in the Dublin Archdiocese and a Commission of investigation was appointed by the Department of Justice. The investigation carried out between 2006 and

[21] Canada shares Residential School documents with National Centre for Truth and Reconciliation. (2022). https://www.canada.ca/en/crown-indigenous-relations-northern-affairs/news/2022/01/canada-shares-residential-school-documents-with-national-centre-for-truth-and-reconciliation.html.

2009 resulted in the so-called Murphy Report, concerning diocesan archives, including secret ones; yet, considering the extraordinary 720-page length of the report, it is astonishing that they are only mentioned very briefly.[22]

The Commission of investigation set up by the Australian government, a consortium of research organisations commissioned by the German Roman Catholic Church conducting a research project, the model of Francophone Canada, where the Church commissioned a retired judge to conduct a comprehensive extra-judicial investigation, or the direct commissioning of an acting judge, as the situation was in Ireland, they all represent different ways of how to reflect the intense public pressure, especially in the last quarter century, to open the Roman Catholic Church archives, and the secret diocesan archives in particular. Throughout the process of opening up this horrifying and deplorable reality in the Church, it has become clear that in order to carry out a comprehensive investigation, it is absolutely necessary to be able to access records in the Church archives, provided that the records in question have survived. The Canadian NCTR is a memento that archiving and disclosure of records can become a very important tool for the protection of victims.

4.2.1 Public-yet-Private Records and the Process of "Publicization" of Private Records

Church records and archives which in some way bear witness to the crimes of child sexual abuse, as well as other crimes falling within the scope of non-canonical criminal law, ultimately raise a remarkable question regarding the status of these records as such. Although church records are generally considered private rather than public, in the case of records testifying about crimes in the diction of general criminal law, this question is much more controversial.

A number of cases outside the Church have led to serious disagreements regarding the status of records, particularly those created by top elected political representatives. It is only in recent decades that this issue has begun to be systematically addressed in developed democracies, albeit with varying outcomes; in any case, however, more precise boundaries are being set up between purely private and public records, and society's claim

[22] Commission of Investigation. (July 2009). *Report into the Catholic Archdiocese of Dublin*. https://www.gov.ie/en/publication/13804-report-by-commission-of-investigation-into-catholic-archdiocese-of-dublin/.

to publicity has strengthened for a number of record categories that were previously perceived as private.[23]

The category of church records testifying about crimes, including sexual abuse, represents records in a way lying on the borderline between private and public comprising both, private as well as public record features. Although these records originated from the activities of a private entity, society, in view of the crimes committed and, what is more, the attempts to cover them up, claims access to them and, in a sense, demands that they be subject to the requirements imposed on public records and archives. This also applies to other situations in which, for example, law enforcement authorities have the right to seize private records, that is, to make a public claim to them by granting access to a public authority. In a sense, in these and similar situations, it is possible to talk about a process that I would call "record publicization" meaning that an originally private record becomes public in certain respects. One of the characteristics of such a process is that it is not permanent and can be reversible. In many cases, private records seized as evidence in criminal proceedings are returned to their original owners once the proceedings are over.

4.3 Conclusions from the Analyses of Preservation and Archiving Records Testifying About Child Sexual Abuse and Recommendations

– Inaccessibility of records to the victims of sexual violence. This issue is explicitly implied by the conclusions of the quoted report of the Australian commissions of inquiry.[24] Victims should henceforth have access to files that testify about violence against them, even if these include originally "private" church records. The inspiring aspect of the case of Indian residential schools is the effort of the government, including public archives, to give access to the maximum extent possible both to the victims and to society as a whole to the records documenting and testifying to the

[23] This particular issue is addressed in Čtvrtník, M. (2021). Public versus private status of records and archives and analysis of the implications for their access. An example demonstrating top political representatives of political power in the USA, France, and Germany. *Archival Science*, 2021. https://doi.org/10.1007/s10502-021-09375-y.

[24] Royal Commission into Institutional Responses to Child Sexual Abuse. (2017). *Final Report, Recordkeeping and information sharing*, vol. 8, p. 11.

cultural genocide and the full range of the most serious crimes committed by mainstream Canadian society, in this case by means of residential schools, against Canada's first inhabitants, not only children but also their parents.

- General competence to decide on access to records maintained in diocesan secret archives is vested only in the bishop, as follows from the Codex Iuris Canonici. This exclusive competence of bishops to regulate access to diocesan secret archives should be removed from the canon law.
- Allowing church dignitaries, especially bishops, to arbitrarily decide on the destruction of records testifying about child sexual abuse. The control mechanisms particularly with regard to records management in—especially secret—archives are absolutely minimal. It is advisable to introduce such mechanisms in future and limit the almost exclusive authority of bishops in the management of diocesan—especially secret—archives, including their power over the destruction of records maintained in such archives.
- Inadequately short retention periods for records maintained in Church archives relating to crimes committed by Church leaders.
- Poorly set appraisal of the archival-historical value of records relating to the crimes of religious leaders, as a large part of the records concerning crimes and other offences of religious leaders is not intended for permanent archiving. Only the final judgement delivered by ecclesiastical courts in criminal proceedings under canon law together with a "short summary of the facts" is permanently preserved. In non-canonical criminal law, major crime files are at least selectively, but in some cases completely permanently archived in public archives due to their highly significant historical and archival value. A typical example is the material related to Jack the Ripper. Records that have survived to this day—for example, the correspondence of the London Metropolitan Police during the period of the Ripper murders and during the investigation, the Ripper's alleged letters to newspapers, and so on—are still, more than 130 years later, carefully preserved in The National Archives and their historical and educational value is incalculable.
- It is worth considering whether some parts of the records maintained in church archives, which could be understood in the diction of this text as records lying on the borderline between private and public, should be transferred to public archives for permanent

> archiving. Moreover, they are often much better suited for permanent or very long-term archiving than church archives; and they could probably also be a better guarantee of timely and lawful availability of records.

And this brings us closer to what lies behind the intention to release to public archives the records of the Odenwaldschule private school, where massive sexual abuse of minors also occurred and which was addressed in the previous part of the text. In addition to preventing data leaks, the reason was the timely use of the data for official and scientific purposes, that is, opening access (although not, of course, for the general public). Unfortunately until recently, church institutions have, virtually without exception, denied access to records of crimes, including those related to the sexual abuse of minors, usually with both illegal and immoral incentive to cover up such crimes.

To conclude at the end of this chapter: Personal protection in the archives (and beyond), as I have attempted to demonstrate using some examples of the fate of records relating to child sexual abuse within various entities, may in some situations be best achieved by destroying sensitive personal data and making them permanently inaccessible; however, in certain situations, this protection does quite the opposite—it allows access to archival records and permits a timely and, with respect to personality and privacy protection of the victims in particular, controlled and regulated access to records and archives that testify to human rights violations.

One of the key tools for the protection of personal and privacy rights in archives, as well as in records management, is embodied in a law that is gradually being more and more frequently mentioned and has recently become one of the new rights guaranteed to the citizens of the European Union. It has already been mentioned at several points in this and previous chapters. It is often called “the right to be forgotten”. It also has significant relevance in the area of post-mortem personality and privacy protection. It stands at the imaginary opposite pole to another right associated with the principle of free access to information, the “right to know”. “The right to be forgotten” will be the main topic of the following chapter.

CHAPTER 5

The Right to (Not) Be Forgotten, Right to Know, and Model of Four Categories of the Right to Be Forgotten

Motto:

"Do the interests of the living outweigh those of the dead? … Does the privacy of living persons override the importance of historical research and does the right of access give way to the right to forget?"[1]

Eric Ketelaar

In 2008, the Landesarchiv Berlin released Klaus Kinski's mental health records from 1950, when the actor was hospitalised for three days at the Karl-Bonhoeffer-Nervenklinik in Berlin.[2] Without exaggeration, this case can be regarded as a—fortunately very rare—example in the field of archives demonstrating how poor management of personal data in archives can look, and showing violation of basic principles of personality protection by archives as custodians of vast amounts of personal, including extremely sensitive, data of citizens. The following chapter may thus open with the question: Even posthumously, did Klaus Kinski have the right to have his (mental) health condition forgotten? In other words, did he have

[1] Ketelaar, E. (1998, 23 October). Archivalization and archiving. Unpublished inaugural address as Chair of Archivistics. University of Amsterdam, p. 6. As cited in: Harris, V. Knowing right from wrong: the archivist and the protection of people's rights. *Janus*, 1999(1), 32–38, p. 33.

[2] For a detailed discussion of the case of the disclosure of Kinski's medical records, see Chap. 2.

M. Čtvrtník, *Archives and Records*,
https://doi.org/10.1007/978-3-031-18667-7_5

the right to prohibit society access to his medical history and learn about his mental health problems?

However, we can also mention another case. In 2010 Germany, a case emerged of widespread, systematic, and long-term sexual abuse of children since the 1990s by the teaching staff, including the headmaster, at the Odenwaldschule reform school in the Hessian town of Heppenheim.[3]

Not surprisingly, the school went bankrupt shortly thereafter, and after some personal data were leaked to the public, the Hessen Archives, following a consultation with the State Prosecutor's Office, decided to take over the school records even before the expiry of the retention periods. The intention of the premature transfer of extremely sensitive materials to the archive, which began in 2015, was to enable the maximum possible and timely extraction of the data in the records containing data on sexual abuse, that is, providing access, not only for the purposes of the investigation but also for various research purposes. The transfer also includes a number of records that would probably have been legally destroyed in the shredding process had it not been for the occurrence of those horrific acts. Nevertheless, this situation was completely opposite to the Klaus Kinski case. One of the reasons why the archive took over the highly sensitive materials prematurely was to protect the personality of the victims, as the records transfer was preceded by cases of leaks of data from the incriminated documents to the public.

The intention of transferring the records into the archive was made to enable the maximum possible extraction of the data they contain and thus their accessibility, however the whole system of such accessibility had to strictly respect the protection of the personality of those concerned. Where does the right to be (not) forgotten stand here? When compared to similar cases of other schools, the archiving of an unprecedented volume of material conveys that society is demanding the right to memory (similar to the right to know, the right to information), and that likewise, those affected have a right to have society remember inhumane instances of tarnishing the law and harming people. Did victims of sexual violence have the right to have the despicable acts committed against them remembered?

Both at the level of the most basic civil and democratic rights declared at the constitutional level and specifically in the field of archiving, there has long been a fundamental tension between two principles: On the one hand, it is the right to the protection of personality, privacy, private sphere,

[3] For a detailed discussion of the case of the Odenwaldschule records, see Chap. 4.

specifically expressed also in the form of the right to protection of personal data and restriction of their disclosure. On the other hand, there is the right of access to information, freedom of inquiry, and similar rights, which can be summarised under the common denominator of the right to know.[4] This dichotomy, in a specific and in a way analogous sense, is also at the level of the relationship between the right to be forgotten and, conversely, the right to be remembered and not forgotten.

Encounters and, in many cases, clashes between these two principles on both levels of meaning have changed in recent years and have intensified, including in court decisions. What implications does it have for archiving, for the creation and preservation of collective memory in society, and for the relationship to one's own history? What are the implications of the current development of the legal order for the archival sector, within the European Union, especially in connection with the adoption of the General Data Protection Regulation (GDPR), specifically at the level of the application of the right to be forgotten as one of the new rights of the European citizen, which, however, has much deeper and older roots than

[4] The issue of access to information, particularly in the field of archives and archiving, is dealt with in other chapters of this book, including references. The question of the relationship between access to archives and data protection is addressed in an older but agelessly excellent text by MacNeil, H. (1992). *Without Consent. The Ethics of Disclosing Personal Information in Public Archives*. Society of American Archivists, Scarecrow Press. On access to archival records in a broader perspective, with particular emphasis on Belgium and France, it is worth paying attention to Vandevorde, É. (Ed.). (2005). *La communication des archives. De la communication à l'accessibilité*. Bruylant-Academia. An interesting earlier study prepared for UNESCO concerning the relationship between archives and access: Blais, G. (1995). *Access to archival records. A review of current issues. A RAMP study*. UNESCO. Access to public information and records not primarily focusing on archiving has been recently summarised in Blanke, H.-J., Perlingeiro, R. (Eds.). (2018). *The right of access to public information. An international comparative legal survey*. Springer-Verlag. https://doi.org/10.1007/978-3-662-55554-5. For the European Union, cf. Rossi, L., Vinagre e Silva, P. (2017). *Public access to documents in the EU*. Hart Publishing.

the existence of the GDPR?[5] How does the newly established right to be forgotten manifest in the field of archiving? What impacts and potential risks can be expected when applying this newly formed right of (not only)

[5] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (GDPR). https://eur-lex.europa.eu/eli/reg/2016/679/oj. A comprehensive analysis of data protection legislation at the European Union level, including the issue of the right to be forgotten under the GDPR, is presented in the *Handbook on European data protection law*. (2018). Publications Office of the European Union. https://doi.org/10.2811/343461. There are a number of publications on the right to be forgotten not only under the GDPR. Among the recent works, I will only mention the legal comparative perspective taken by Werro, F. (Ed.). (2020). *The right to be forgotten. A comparative study of the emergent right's evolution and application in Europe, the Americas, and Asia*. Springer. https://doi.org/10.1007/978-3-030-33512-0. A comprehensive analysis of European data protection legislation, in particular the GDPR, is provided in Lambert, P. (2017). U*nderstanding the new European data protection rules*. CRC Press. In relation to the GDPR with an emphasis on the United Kingdom, cf. Lambert, P. (2019). *The right to be forgotten: interpretation and practice*. Bloomsbury Professional. https://doi.org/10.5040/9781526510136. For a comparative perspective with special reference to Canada, cf. Cofone, I. N. (Ed.). (2020). *The right to be forgotten. A Canadian and comparative perspective*. Routledge. https://doi.org/10.4324/9781003017011. Cf. also Jones, M. L. (2016). *Ctrl + Z. The right to be forgotten*. New York University Press. In francophone literature, see, for example, Bensoussan, A. (sous la dir. de). (2018). *Règlement européen sur la protection des données. Textes, commentaires et orientations pratiques*. Bruylant. However, there are fewer analyses of the right to be forgotten specifically in relation to the archival domain and archiving. Cf. in particular Van Honacker, K. (Ed.). (2018). *The right to be forgotten vs the right to remember*. VUBPRESS Brussels University Press. Cf. also Čtvrtník, M. (2018). Právo být (ne)zapomenut. Výmazy dějin, inflace historických pramenů, ochrana soukromí, vy(zne)užívání dat a prekérní situace archivů v mladém 21. Století—podněty k diskusi [The right to be (not) forgotten. Erasure of history, inflation of historical sources, protection of privacy, (mis)use of data and the precarious situation of archives in the early twenty-first century—stimuli for discussion]. *Archivní časopis* [Journal on Archives], 68(3), 266–297. In the period shortly before the GDPR was issued, its advent and intentions, including the implications for archiving, were brought to light by a publication emanating from within the European Commission, published by the Commission's Joint Research Centre: Ghezzi, A, Guimarães Pereira, Â., Vesnić-Alujević, L. (Eds.). (2014). *The ethics of memory in a digital age. Interrogating the right to be forgotten*. Palgrave Macmillan. An international comparative perspective can be found in the study by Vavra, A. N. (2018). The Right to be forgotten: an archival perspective. *The American Archivist*, 81(1) (Spring/Summer), 100–111. Long before the GDPR, the relationship between the right to be forgotten and the right to know was mentioned by Ketelaar, E. (1995). The right to know, the right to forget? Personal information in public archives. *Archives & Manuscripts*, 23(1), 8–17. Cf. also Harris, V. (1999). Knowing right from wrong: the archivist and the protection of people's rights. *Janus*, 1999.1, 32–38.

the European citizen to archival practice? A very important precursor to all these issues is the fact that the responsibility for personal data management and for the protection of the personality and privacy of those whose footprints can be found in the records and archives, lies with all the actors: archives and archivists, requestors for access to information, including scientific researchers.[6] This responsibility cannot be avoided and for this reason alone it is important to try to understand the right to be forgotten, the right to know and their complicated relationship.

5.1 The Right to Be Forgotten and the European General Data Protection Regulation (GDPR)

In recent years, there has been a clear tendency to increasingly protect the personal data of specific people in written material, both archival and non-archival. The contradictory and parallel existence of two basic principles, one of which advocates the accessibility of information and the other the protection of information linked to the protection of privacy and personality rights, including the protection of a name, reputation, and honour, is also reflected in European legislation and case law. The following two judgements represent a paradigmatic example of two completely opposing views in this field. First, there is the 2009 judgement of the European Court of Human Rights (ECHR), Section II,[7] in favour of broad and unrestricted access to information, or freedom of expression within the meaning of the European Convention for the Protection of Human Rights and Fundamental Freedoms.[8] On the other hand, there is the 2014 decision of the Court of Justice of the European Union (Grand Chamber) in

[6] The responsibility of archivists and researchers in the area of access to archives and data they contain was already pointed out by French archivists long before the GDPR came to existence. Cf. the monothematic issue of La Gazette des archives with the title *Transparence et secret. L'accès aux archives contemporaines* [Transparency and secrets. Access to contemporary archives]. See here, for example, Krakovitch, O. (1997). La responsabilité de l'archiviste: entre histoire et mémoire. *La Gazette des archives*, 177–178, 236–240. https://doi.org/10.3406/gazar.1997.3473; Gasnault, F. (1997). La vie privée. Table ronde. *La Gazette des archives*, 177–178, 197–218. https://doi.org/10.3406/gazar.1997.3473

[7] Kenedi v. Hungary (Application no. 31475/05). Judgment. Strasbourg. 26 May 2009.

[8] European Convention on Human Rights of 4 November 1950 as amended by Protocols Nos. 11 and 14 supplemented by Protocols Nos. 1, 4, 6, 7, 12, 13 and 16. https://www.echr.coe.int/documents/convention_eng.pdf

the dispute between Google and the Spanish Data Protection Authority.[9] This judgement, in turn, refers to the right to protection of honour and reputation and, already at that time, to the "right to be forgotten". In its judgement, the Court of Justice, in the context of the interpretation of the European Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, determined that internet search engines also function as data controllers and should behave and comply with their data protection obligations accordingly. However, it is the ECHR which, in its case law from recent years, particularly in relation to the interpretation of Article 8 "Right to respect for private and family life" of the European Convention on Human Rights, has also issued some fundamental comments regarding the right to be forgotten, including some cases concerning the relationship of archives and archiving to this right. This case law is discussed in more detail in Sect. 2.1 in Chap. 2. The right to be forgotten referred to in these judgements then brings us to the European regulation issued in 2016, which has generated an enormous response throughout the European Union, not excluding archival communities. Let us now take a closer look.

A European standard that has already raised great concerns in the archive industry before it came into force is the General Data Protection Regulation (GDPR). It is a regulation that takes precedence over the national legislation of the Member States of the European Union. Part of it is valid normatively and without the possibility of modification in national legislation, part of it can be adapted. The historical predecessor of the GDPR was Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. This Directive already contained some principles that were later developed by the GDPR. These included, for example, the notification obligation in the case of collection of personal data on individuals, the limitation of the purpose of processing personal data to the original purpose of the collection, the need of consent of the individual before any

[9] Google Spain SL. Google Inc. v. Agencia Espanola de Protecioón de Datos (AEPD), Mario Costeja González—Case C-131/12/. Decision of the Court of Justice of the European Union (Grand Chamber) of 13 May 2014. For an analysis of this judgement, see Lambert, P. (2019). *The right to be forgotten: interpretation and practice*. http://dx.doi.org/10.5040/9781526510136.chapter-002, pp. 13–20.

further sharing of their personal data with other entities, security considerations, the right of an individual to have access to their personal data collected by the data controllers, including the right to rectification, and the establishment of the general responsibility of data controllers for personal data management. While this Directive also introduced the principle of limiting the storage of personal data to a period not longer than necessary to fulfil the original purpose of the collection of such data, unlike the GDPR, it completely failed to take into account the public interest aspect of data archiving and the exemptions set out for archiving purposes.

The European GDPR most significantly reflects the growing tension between the protection of personal data on the one hand and the right of access to information and freedom of inquiry on the other. This tension is then most concentrated in one of the rights newly established by the GDPR, namely the right to be forgotten (right to erasure).[10]

Even before the release of the GDPR, some archivists and historians in Western Europe were already aware of the risks of the GDPR impact on archiving, supporting a petition by French archivists prior to the approval of the GDPR called "Adjourn the adoption of the regulation about personal data" ("Citoyens contre le projet de réglement européen sur les données personnelles #EUdataP").[11]

The petition referred mainly to legal and inheritance purposes, proving ownership and the like, which is difficult to achieve without specific people with specific names preserved in records. It also took into account another possible right of the citizens in a democratic state, the right of access to information. French archivists sent the petition all over Europe and collected more than 50,000 signatures. It was signed by archivists and historians all over Europe. The petition was victorious at the end of 2013 however, the European Council postponed the discussion of the GDPR project until 2015. Although the petition ultimately failed to prevent the publication of this European standard and thus the codification of a new right to be forgotten, it did lead to some not insignificant successes in incorporating some exemptions into the text of the regulation. So what exactly is the right that a citizen of the European Union acquires with this

[10] A brief reflection on the right to be forgotten from the time before the GDPR was approved was provided by Čtvrtník, M. (2014). Máme právo být zapomenuti?! [Do we have the right to be forgotten?!]. *Archivní časopis* [*Journal on Archives*], 64(2), 190–191.

[11] Petition text: https://www.archivistes.org/Au-nom-du-droit-a-l-oubli-quel

new right to be forgotten, and where does this right stand in relation to the right to information in the field of archiving?

The right to be forgotten (right to erasure) is defined in Article 17 of the GDPR as follows: "The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay", in particular where the personal data are no longer necessary for the purposes for which they were collected or otherwise processed.

If this were to remain the case, it would be an unmitigated disaster of immeasurable consequences for the entire archival and historical community and for the whole knowledge of history in general. Fortunately, a citizens' initiative and the above petition were at least partially successful.[12] The initiative has led to certain and very important limitations on the otherwise very broadly worded right to be forgotten in the final text of the GDPR. The right to be forgotten can be disapplied for several fundamental reasons.[13] In addition to, for example, to the public interest in the field of public health or the exercise of the right to freedom of expression and information, they also managed to establish archiving purposes in the public interest, scientific or historical research purposes, and statistical purposes as separate grounds for not exercising the right to be forgotten.[14]

Moreover, they also successfully exempted, among other things, historical research and archiving in the public interest from the so-called purpose limitation that the GDPR introduces. What exactly does this mean? The GDPR establishes the purpose limitation principle as one of the principles of personal data processing. According to this principle, personal data must be "collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes".[15] However, in the same paragraph of the otherwise generally formulated purpose limitation, it is further explicitly stated that "further processing for archiving purposes in the public interest, scientific or

[12] Lemoine, H. (2016, 27 May). #EUdataP: 3 ans après le début de la mobilisation. http://www.archivistes.org/EUdataP-3-ans-apres-le-debut-de-la-mobilisation

[13] GDPR, Art. 17 (3).

[14] "[F]or archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing." GDPR, Art. 17 (3)(d).

[15] GDPR, Art. 5 (1)(b).

historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes". Eo ipso, the purpose of archiving or historical research may be included within the purposes for which personal data may be collected.

Yet, there is another exemption to the general procedural setting of the processing of personal data, as defined in another provision of the general principles, which is equally important and perhaps even more important for archival and historical science. It is the principle of storage limitation. The wording states that personal data "must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed".[16] However, even in the case of the storage limitation principle, there is an exemption: "personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) […]".[17]

It would thus seem that the situation is quite obvious and archiving in the public interest has acquired the status of a legitimate purpose under the GDPR (purpose limitation principle), that is has been included among the domains for which the processing of personal data is explicitly permitted even without the consent of the data subjects, and at the same time has received a general exemption allowing it to process personal data for a period longer than the original purpose of processing (storage limitation principle). Yet, the situation is not as clear-cut as it might seem at first sight.

Even though they have earned exemptions from the generally formulated and applied principles of personal data processing, the purposes of archiving, scientific and historical research or statistical purposes are ultimately weakened and restricted in several key respects. This is most significantly reflected in two of the principles of personal data processing introduced by the GDPR, namely the "data minimisation" principle and the "storage limitation" principle.

Regarding the storage limitation principle, it is the fifth GDPR article defining the main principles for the processing of personal data, which introduces an additional rule concerning the possibility of maintaining personal data for a longer period than is strictly necessary for the original (usually official) purposes, namely for archiving in the public interest, for

[16] GDPR, Art. 5 (1)(e).
[17] GDPR, Art. 5 (1)(e).

historical or other scientific research or statistical purposes: The archiving purposes in the public interest, historical or other scientific research purposes, or statistical purposes apply—as the conclusion of the "storage limitation" principle reads—only "subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject".[18] What exactly does this very vague wording "appropriate technical and organisational measures" mean? It is only specified much later at the very end of the GDPR.

The key Article 89 of the GDPR, entitled "Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes", contains a somewhat complicated formulation: "Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner."[19]

Let us add that the GDPR, both here and in its entirety, is primarily concerned with pseudonymisation of personal data as defined by the GDPR itself, that is, in the sense of replacing personal data (e.g., a name) with another identifier for the purpose that the personal data cannot be further attributed to a specific personal data subject. In such a case, the possibility of re-establishing a hypothetical link between the personal data and their subject is preserved. The GDPR also very briefly refers to the possibility of data anonymisation, where the link between the personal data and its subject is irreversibly broken. However, it explicitly states that the GDPR does not apply to such anonymised data.[20] On the contrary, the GDPR primarily applies to pseudonymised data, precisely because such

[18] GDPR, Art. 5 (1)(e).
[19] GDPR, Art. 89 (1).
[20] GDPR, Rec. 26.

data retain a potentially retrievable link to persons as their subjects, thus still preserving the essential personal character.[21]

In any case, however, the core of the regulation, which is crucial for archival and historical science, is based on conditionality: If it is possible to erase the specific identity of a person, the obligation to de-identify a specific person applies, provided that the public interest of archiving and the scientific and historical research objectives or statistical purposes are not compromised. And this is where the very touchstone of the Regulation comes into play: Who will be the imaginary arbiter to judge whether the purposes pursued—for example, the archiving purposes in the public interest, scientific or historical research purposes, and so on—can be fulfilled even if the identifiability of the data subject, that is, the link of the data to specific natural persons, is broken? Will independent expert bodies be established? Will the assessor be a public authority, such as the ministerial department responsible for archives, or data protection authorities? What criteria will be used to assess this condition, since no specific criteria have been laid down in the legislation? Will it not be the courts and, in the last instance, the constitutional courts that will set the basic boundaries, define the terrain and essential rules in their judgements and rulings? What will be the case law of the courts that will one day resolve disputes as to whether the purpose of archiving, historical and other research, and statistical investigations can be circumvented when the link between archives and historical sources and specific persons is broken? To what extent will this reflect the current trend of increasing data protection? Should we expect that the interpretation of those provisions of the GDPR that open up room for very different interpretations of the right to be forgotten evolves accordingly? Will the effects of the implementation of the GDPR in the archival space only manifest on the level of providing access to researchers, and therefore only on the level of an even greater elimination of personal data on copies of archives presented to requestors, most often

[21] European Archives Group. (October 2018). *Guidance on data protection for archive services. EAG guidelines on the implementation of the General Data Protection Regulation in the archive sector*. https://ec.europa.eu/info/sites/info/files/eag_draft_guidelines_1_11_0.pdf, p. 34. For more detail on the relationship between pseudonymisation and anonymisation in the field of archiving, see Chap. 8. On the concept of pseudonymisation and its relationship to anonymisation within the GDPR cf. Mourby, M. et al. (2018). Are 'pseudonymised' data always personal data? Implications of the GDPR for administrative data research in the United Kingdom. *Computer Law & Security Review*, 34(2), 222–233. https://doi.org/10.1016/j.clsr.2018.01.002

by using the tool of data redaction? Or will the principle of data minimisation eventually be reflected in the increasing pressure for "hard" irreversible anonymisation, especially before the records are transferred to archives for permanent preservation?

A recent experience in the Czech Republic concerning the corpus of historical sources provides an illustrative example and proof that this is not a virtual problem. In 2011, the case of the (non-)preservation of the records of the 2011 Czech census opened in the wider media space. The request of the Czech Office for Personal Data Protection at that time was to anonymise personal data in the census records. This triggered a response from the National Archives, which pointed out that after anonymisation, the census forms would lose practically all their historically valuable informative value. Nevertheless, all the personal data in the census records were anonymised before being transferred, regardless of the assurances and guarantees given by the National Archives that it would not make the data from the census forms available to anyone. A detailed analysis of the treatment of personal data in census records in foreign comparative perspective is presented in Chap. 7.

In general, however, it can be stated that losing the possibility to identify persons in archival records (census records being only one illustrative example) together with the application of the right to be forgotten in the context of records management and archiving will, to a greater or lesser extent, leads to what can be described, with a little literary licence, as the gradual "depopulation of history".[22]

5.2 The Right to Be Forgotten Versus the Right to Memory, the Right to Know

European law through the GDPR intends to introduce a remarkable right—the right to be forgotten. In the near future, it is indeed not impossible that people, and therefore potential historical actors, will be allowed to systematically erase the traces they leave behind in reality and therefore in history. However, one may ask why the right to be remembered could not equally be created, written down, and codified? Why should not

[22] Cf. Čtvrtník, M. (2014, 6 September). Vylidnění dějin [Depopulation of history]. *Lidové noviny*, p. 22/IV (Orientace supplement); Čtvrtník, M. (2014). Zrušení § 37 archivního zákona a vylidnění dějin [Repeal of Section 37 of the Archives Act and the depopulation of history]. *Archivní časopis* [*Journal on Archives*], 64(4), 356–360.

citizens be able to claim that a certain imprint should be left in reality and in history? Such a right, however, need not be formulated merely as a person's right to preserve the memory of their own actions. It can also be defined in the sense that society as a whole also has the right to be remembered for the deeds and actions as members of that society, whether for their positive contribution or, conversely, their negative impact. At this point, the right that comes into play is the right of a society to hold its individual members accountable for their actions, the pursuit of justice, but also to enable the creation of a historical memory of the society, its historical consciousness, including coming to terms with its own past.

The problem can also be posed in another way: The European law has declared the right to be forgotten in the specific context of personal data management On the other hand, the right to preservation of documentary, cultural, artistic, scientific, intellectual value has not yet been anchored in the law (leaving aside the specific provisions of certain special legislation relating to, e.g., cultural heritage preservation, intellectual property rights, etc.)—apart from the statutory obligations usually imposed on public law creators to propose a certain part of their records for archival appraisal of documents and archives for storage, or, in some legislations, a certain corpus of records that should be permanently archived[23] (on the constitutional level, there is only the right to information, the right to freedom of research, etc.). We could also ask whether, in addition to the right to be remembered, the duty to be remembered, the duty of memory should also be formulated in a certain sense.

The right or, in a way, a kind of moral obligation of memory that society might require reflects the question to what extent not only the public entity, but ultimately the individual himself as a private person, has any right at all to dispose of his records that bear the traces of their actions. We know from history many famous cases where the creator of records and also of other objects of high cultural, artistic, intellectual, or scientific value, destroyed his own creations or asked for them to be destroyed, a wish very often unfulfilled. To mention probably the most famous of them: Max Brod, as is well known, not only did not destroy Kafka's texts against Franz Kafka's express wishes, but also began to publish them.

[23] In the Czech Republic, this is a provision of the Archives Act: Zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů [Act No. 499/2004 Coll., on Archiving and Records Management and on the amendment of selected acts] of 30 July 2004, Sec. 5 and Annex 1 and 2 to this Act.

Kafka, by this notorious will (including the wish to destroy the letters already sent by him and to him), actually asked to exercise something that in a way corresponds to the right to be forgotten, just as the GDPR implements it in a somewhat different context.

In the end, the fundamental question is the question of the ownership of records, works and creations, or the issue of their private or public status. This question remains even in the case—and precisely in the case—when the person in question is their creator himself. In the case of public figures, the situation would seem to be quite clear. If they create or receive records in the exercise of their public functions, the records do not, strictly speaking, belong to them. Yet, in the case of private persons or persons outside the exercise of public office, politics, and the like, the situation is much more complicated.

In layman's terms: Did Kafka have the right to destroy his manuscripts? And vice versa: Did Brod have the right to preserve and publish these manuscripts against Kafka's will? Victor Hugo had pointed out this problem much earlier: "A building has two things: its use and its beauty. Its use belongs to its owner, its beauty to everyone, to you, to me, to all of us. Its demolition is therefore ultra vires."[24]

Although Hugo's statement applies primarily to architectural monuments, it can be applied to any work of art or other general quality, including written monuments. And in a way, it reflects the complexities of ownership and disposition of dealing with written material of a non-artistic nature that has some significant value (scientific, intellectual, emotional, etc.) beyond its purely private significance for personal or family memory. But even here, in the apparently quite private sphere of the family, the closest relatives, the clan, the meaning of a record or other artefact extends or can extend beyond the boundaries of one particular individual. Documents may be valuable for family and family memory. We may once again ask: Do we really have the (moral) right to arbitrarily destroy written monuments of our ancestors? Is there not a family obligation to our ancestors and towards future generations—in this case to preserve family written memories?

[24] "Il y a deux choses dans un édifice, son usage et sa beauté. Son usage appartient au propriétaire, sa beauté à tout le monde, à vous, à moi, à nous tous. Donc, le détruire, c'est dépasser son droit." Hugo, V. (1832). Guerre aux démolisseurs. *Revue des Deux Mondes.* Période Initiale, t. 5, 1832, 607–622, p. 621. He published the first part in the *Revue de Paris* in 1825.

It is certainly obvious that the question of the applicability, feasibility, and possible legal enforceability of the rights of the society thus postulated, or the obligations of the creator of records and other artefacts, is quite different. Who can compel an author not to destroy his texts, a painter not to destroy his canvases the moment they have not yet left his studio? A quite different moment comes into play here, namely the moment of responsibility, and a responsibility quite different from the responsibility or obligation to comply with legal norms. We can therefore ask a question of principle: Does the creator of a work with a significant cultural, artistic, intellectual or scientific value (but also value bounded by the private sphere of family, clan, etc.) have the full right to freely (and possibly arbitrarily) dispose of "his" work?

However, the question of the ownership of "one's own" records, or their public or private status, is still very topical today, even for persons in the highest public offices. I address the problem of public and private status of records in detail, with an emphasis on demonstrating this issue in some complicated cases, in a separate study.[25] Here, just for the sake of illustration, let us mention, for example, that to this day American presidents claim at least some of the materials created during their presidency. It is, after all, a tradition that goes back to the time of George Washington. However, the ambiguous status between public and private and the problems of its determination are also present in other advanced democracies such as France and Germany, as is analysed in the text cited above.

The examples given of the fate of Franz Kafka's estate or the relationship of American presidents or top French or German statesmen to "their" records mirror the growing awareness in society of the right of memory, the right to be remembered. A right, in which it is expressed that there is something like a duty to remember the traces of one's deeds in reality. At the same time, today's societies are becoming increasingly aware that this right and duty is also subject to the most powerful of this world, and that it also affects in some way those who create work of art and values that reach beyond their own individual sphere.

Thus, the right to forget, the right to be forgotten and, on the other hand, the right to remember and the duty to remember, which extends far

[25] Čtvrtník, M. (2021). Public versus private status of records and archives and analysis of the implications for their access. An example demonstrating top political representatives of political power in the USA, France, and Germany. *Archival Science*, 2021, https://doi.org/10.1007/s10502-021-09375-y

beyond the motivation of the possibility of controlling the actions of public figures, meet in an interesting counterpoint. Archives and archivists, then, should constitute one of those places that should be involved in the proper balancing of such a struggle.

The clash between the right to be forgotten, the right to remember, and the right to know, takes place on another fundamental level: At present, there is an increasing call for the protection of privacy and private sphere of the individual, expressed strongly on the level of protection of personal data, on the other hand, there is also an increasing interference in personal privacy by both state authorities and private entities. Both, governments, including intelligence services, and private entities are increasingly making significant, widespread, and extensive intrusions into the private sphere, especially in concerning the traces we leave in the digital world. Often, the line where privacy ends and begins, the inviolability of which is usually guaranteed directly by the constitution, is blurred. Very well known are programmes such as PRISM, the US National Security Agency programme launched in 2007 to monitor electronic communications between citizens, the existence of which was revealed by Edward Snowden in 2013. We can also mention a similar secret programme, Tempora of the British secret service Government Communications Headquarters (GCHQ), launched in 2011, which monitors (and temporarily stores) not only telephone calls but also internet communications (emails, Facebook, etc.), again in a mass manner; this monitoring is not targeted at a specific suspect.

Recently, the USA has also been in the throes of a scandal over data from the website disruptj20.org, which served as a coordination point for opponents of President Trump who planned to organise protests on the day of his inauguration on 20 January 2017 (hence the name of the website).[26] The US Department of Justice required the site's provider to deliver in bulk the personal information of all visitors to the site (including names, addresses, phone numbers, email addresses, payment methods for services, credit card and bank account numbers, and records of the types of services used by the user), not just specific suspects. The US District of Columbia Superior Court ultimately ruled in October 2017 that the webmaster must provide data of registered users directly linked to the

[26] Cf. http://www.disruptj20.org/

Disruptj20 website, but does not have to hand over information about common—unregistered—visitors to the site.[27]

Orin Kerr, an American law professor, points out that the issue is really one of appropriate and permissible moderation in web viewing.[28] Kerr underlines the point that in the physical world the boundedness of private space, such as an apartment, is quite obvious and more or less unambiguous. Investigating authorities can enter a suspect's apartment if they have a warrant, but they cannot search other apartments in that building owned by other persons. But this clarity is blurred in the digital world. It is not clear whether a mass search of a particular website content and personal data corresponds to an imaginary specific suspect's apartment, or whether it is an entire house and thus an unwarranted invasion of the private space of persons not addressed as suspects.

In the Czech Republic, for example, the question of whether or not the Military Intelligence Service, one of the three Czech intelligence services, should be given the power to monitor text communications via mobile operators and internet communications via the web has been intensively debated in recent years. The amendment to the Military Intelligence Act was approved in 2021. In the original draft of the amendment, this intelligence service was to receive the power to monitor the content of mobile and internet communications as well. However, this provision was not approved during the legislative process and the Military Intelligence Service was given the ability to monitor only the metadata of internet communications in cyberspace, not the content itself.[29]

It is only natural that the state, including the secret services, must seek new tools to counter violations of the law, including terrorism, precisely when criminal activity is facilitated by the unprecedented development of communications and other technologies, especially in cyberspace.

[27] Superior Court of the District of Columbia, In the matter of the search of www.disruptj20.org that is stored at premises owned, maintained, controlled, or operated by DreamHost, Special Proceedings No. 17 CSW 3438. Order 10 October 2017.

[28] Kerr, O. (2017, 15 August). A closer look at DOJ's warrant to collect website records. *Washington Post*. https://www.washingtonpost.com/news/volokh-conspiracy/wp/2017/08/15/a-closer-look-at-dojs-warrant-to-collect-website-records/?utm_term=.395abbf5952d

[29] Zákon, kterým se mění zákon č. 289/2005 Sb., o Vojenském zpravodajství, ve znění pozdějších předpisů, a některé další zákony [Act amending Act No. 289/2005 Coll., on Military Intelligence, as amended, and certain other acts]. Sněmovní tisk 800. Novela z. o Vojenském zpravodajství [House Print 800. Amendment to the Act on Military Intelligence], Sec. 16 (d). Effective 1 July, 2021.

Perpetrators can much more easily organise and coordinate without the possibility of standard tools of control and supervision of their activities by the security forces. The state and intelligence services must adapt and therefore develop new tools, including surveillance. However, the question is how the boundaries of this surveillance should be set and established with regard to privacy protection.

The relationship between the right to be forgotten and the right to know and the right to memory is ultimately shaped in a specific way at the level of disclosure, as opposed to individual disclosure in, for example, archival research rooms. This is where the responsibility of the researcher, scientist, journalist, and so on for working with personal data and data concerning a person's privacy and intimacy comes into play in a fundamental way. Some legal systems, even within the European Union, explicitly allow for the disclosure of personal data without the consent of the individuals concerned. One of such systems can be found in Germany; at the federal level the country has allowed the disclosure of personal data without such consent on the condition that "it is necessary for the presentation of research results on events in contemporary history".[30] This, of course, does not mean that the researcher thereby obtains a universal placet permitting the publication of any personal data and in any form. Usually—and this is also true in Germany—not only civil but also criminal liability for the misuse of personal data is then established. There have already been some judgements, including from constitutional courts, which have held researchers responsible for the data they publish. A recent case heard by the Constitutional Court in the Czech Republic is illustrative. The 2017 Constitutional Court ruling states the researcher's responsibility for their own historical research.[31] On this basis, historian Eva Nečasová had to apologise to the daughters of Hugo Salm-Reifferscheidt for the claims she made in her book "Cui bono restituce?" published in 2006, and in the work "Cui bono restituce II" published a year later,[32] although these were a substantial minority of the claims challenged by the

[30] "Der Verantwortliche darf personenbezogene Daten nur veröffentlichen, wenn die betroffene Person eingewilligt hat oder dies für die Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte unerlässlich ist." Bundesdatenschutzgesetz vom 30. Juni 2017. BGBl. I S. 2097, § 27 (4).

[31] Nález Ústavního soudu ze dne 12. září 2017 [Constitutional Court judgement of 12 September 2017], case no. III. ÚS 3393/15.

[32] Nečasová, E. (2006). *Cui bono restituce?*. Český svaz bojovníků za svobodu.; Nečasová, E. (2007). *Cui bono restituce II*. Český svaz bojovníků za svobodu.

applicants. The Constitutional Court found, inter alia, that the historian "presented her findings in a manner which […] is capable of interfering with the rights of other persons in a court of law". The Court then went on to highlight that "freedom of scientific inquiry (as is the case with all human rights) also has its limits and ends where it conflicts with other constitutional rights (e.g. the right to life, human dignity); ethical standards are also a natural corrective to freedom of scientific inquiry."[33]

Once again we can see that when it comes to data disclosure and researcher's responsibility, there exists a fundamental tension between the right to know, the right to information and access to it and, on the other hand, the right to be forgotten, the protection of personal data, personality rights and privacy that can also be expressed in the relationship between scientific research and basic ethical and moral rules.

Whether it is the disclosure of information, individual access to it, or the preservation of information as such, the right to be forgotten comes into play in one way or another in all these situations. The following part will present a proposed model of the four categories of the right to be forgotten, which I will use not only to highlight the multi-layered nature of the right to be forgotten, but also to present it as one possible tool to be used for adapting access to information and protection policies in records management and archiving.

5.3 Model of Four Categories of the Right to Be Forgotten: Temporary Versus Permanent Right to Be Forgotten—Data Anonymisation and Pseudonymisation

In reference to the GDPR, prominent French archivists Hervé Lemoine and Bruno Ricard have recently used the expression "droit à l'oubli temporaire" ("temporary right to be forgotten") to refer to the moment when data telling about private life in France are inaccessible to the public for a certain period of time, based on the established closure periods.[34] This phrase is very well chosen. At the same time, I have used it as the initial

[33] Nález Ústavního soudu ze dne 12. září 2017 [Constitutional Court judgement of 12 September 2017], case no. III. ÚS 3393/15, Art. 27.

[34] Lemoine, H., Ricard, B. (2018). Les données personnelles dans les archives publiques françaises. Loi, accès et sécurité. In K. Van Honacker (Ed.), *The right to be forgotten vs the right to remember*. VUBPRESS Brussels University Press, p. 71.

inspiration to develop a model of the four categories of the right to be forgotten, which I will present in the following text.

The model of the four categories of the right to be forgotten is based on the underlying assumption that during the processing of data, including personal data, the destruction of records or the irreversible anonymisation of data is not the only way to exercise the right to be forgotten. Another way may be to prevent access to them. There are, as I will demonstrate below, essentially four basic forms in which the right to be forgotten can be applied. On this basis, it is possible to systematise four categories of the right to be forgotten.

In principle, there are four basic categories of the right to be forgotten, which I propose to name (in order of their strength):

1. a "permanent absolute" right to be forgotten
2. a "permanent limited" right to be forgotten
3. a "temporary absolute" right to be forgotten
4. a "temporary limited" right to be forgotten

Let us take a closer look at how the different categories of the right to be forgotten manifest in the archival sphere and in the archiving process. The implications of the individual categories of the right to be forgotten for the processes of data anonymisation and pseudonymisation in records management and archiving, including the policies of archival appraisal and records destruction, will be discussed in more detail in Chap. 8 in Sect. 8.2.2.

Let us start from what I call the weakest layer, that is, the "temporary limited" right to be forgotten. This layer corresponds to the vast majority of the material preserved in public and private archives. These are granted virtually permanent access for official purposes (hence the term "limited"), but denied access for private purposes for a certain period of time (hence the term "temporary"). Among the reasons for such restriction of access are the standard range of legal tools commonly used in legal systems around the world. These may be general closure periods or specific closure periods applied to selected types of records or data. Very often, specific closure periods are imposed for access to personal data and data relating to an individual and their privacy and personality. However, the protection of banking secrecy, classified information and the like also fall into the same category.

The second category is the "temporary absolute" right to be forgotten. This substitutes a specific situation that can be encountered in the archiving of private creators and has recently begun to make its way into the field of public archiving and public creators. Access is completely ("absolutely") restricted to all requestors for a certain period of time ("temporarily"). In the case of private entities, access is restricted by the will of the person handing over the material to the archive based on their free choice. Typically, such cases include personal estates. In this case, access to the archives is governed by the specific decision of the entity that transfers the material to the archives for archiving. Recently, however, there have also been some cases of archiving in the public interest, even for very important groups of public records. A crystalline example—analysed in detail in Chap. 7—is the time capsule tool, which Australia started to use for census documents in 2001 and which Ireland is implementing for the census in 2022 as well. The archives are sealed for a period of time (in this case 99 or 100 years) during which they cannot be accessed for any purpose, including requests from the courts. After this period, either the right to be forgotten ceases to be exercised altogether, or it moves into a different category.

The following two categories of the right to be forgotten, "permanent limited" and "permanent absolute", represent a stronger form of protection. Access to records and archives over which one of these two categories of the right to be forgotten extends its protective wings is permanently restricted. A very common and probably the most frequent reason for the application of one of the categories of the permanent right to be forgotten is the protection of an individual's personality and privacy. This also opens up the area of post-mortem protection of personality rights, privacy, and intimate sphere. This issue is discussed in detail in Chaps. 2, 3 and 4. I will thus mention it only briefly.

In the case of "permanent limited" right to be forgotten, the weaker of the two categories, access is permanently restricted, but only to certain groups of requestors. This is most often the case when access to archives or records is denied to private research requests, while access for legitimate official purposes is granted. In the case of public records before their archiving phase, this is true for records with infinite retention periods. These are very sporadic cases, but they do exist. In France, but also in some other countries, they include, for example, records containing information that could lead to the production and use of nuclear, biological, or

chemical weapons or other means of mass destruction.[35] Such documents will never be transferred to the archives and will remain open only to the creator or a very limited group of other authorised bodies.

However, at the level of archiving, a much more common reason for exercising the permanent right to be forgotten is to protect an individual's personal, private, and intimate spheres. At the same time, this is the level where post-mortem protection comes into play, that is, the protective layer that includes the protection of personality rights and the protection of the private and intimate sphere, applicable even after the death of the person. It is thus a level that is not normally covered by the rules dealing with the processing and protection of personal data, as these are usually only linked to the living. And here also lies one of the most important sources leading to the distinction between the permanent limited and permanent absolute rights to be forgotten. Their profiling can be very well illustrated by the model of personality spheres, which has its roots in Germany in a judgement of the Federal Constitutional Court.[36]

The model of personality spheres assumes the existence of three spheres, which can be imagined as three concentric circles of different diameters. The broadest social sphere represents a person's public life in a broad sense and includes the performance of their life in society, in public space, including work life (unless it is subject to specific confidentiality or at least not purely private), activities on open social networks, in media space, and so on. None of the categories of the permanent right to be forgotten applies to this sphere. A narrower circle is represented by the private sphere, which corresponds to life within the close circle of family, close friends, and private life in one's own home. This sphere can be entered under certain circumstances. If we compare it with the four-category model of the right to be forgotten, it correlates partly with the temporary right to be forgotten and partly with the permanent limited right to be forgotten. At the same time, it is a sphere in which the various public interests that come into play should be weighed and balanced when it comes to the question of whether information from this area can be opened for a particular purpose. And finally, we come to the intimate

[35] Code du patrimoine, Art. L213–2-II.

[36] Bundesverfassungsgericht. Beschluss des Zweiten Senats vom 14. September 1989, 2 BvR 1062/87. On the distinction of personality spheres in the German legal system, including other references, cf. Epping, V. (2010). *Grundrechte*. Springer, p. 273, Sec. 620.

sphere and personality; these represent the core and are or should be absolutely inviolable.

Among the four categories, the personal intimate sphere then corresponds to the "permanent absolute" right to be forgotten. In part, however, the permanent absolute right to be forgotten also extends to the private sphere, which, as Volker Epping rightly summarises, is always more akin to the intimate sphere than to the social sphere.[37] The space in which the "permanent absolute" right to be forgotten extends, manifests or should manifest itself clearly in the area of records management and archiving, in the sense that records/archives entering its dominion should be irreversibly destroyed as soon as possible—during the archival appraisal of records and shredding process at the latest.

The rule of destroying the records and data entering an individual's intimate and partly also private sphere does not need to apply only if the person concerned consents to their preservation, archiving and, where appropriate, disclosure or publication. A typical example is the aforementioned time capsule and its use in archiving census data in Australia and Ireland.

In the absence of such consent, archiving should be excluded altogether. The hypothetical use of irreversible anonymisation in order to permanently remove the link to a specific person could be considered partly in the private sphere. However, in the case of the intimate sphere, for security reasons and due to the risks of future misuse of data, potential deanonymisation and reidentification of a person, anonymisation is not a sufficient tool to exercise the permanent absolute right to be forgotten and it is indeed necessary to proceed to the destruction of records containing data on a person's intimate sphere as early as possible. The justification for this strict rule of destruction and the earliest possible destruction, is precisely the strongest layer of the right to be forgotten, which is permanent and does not fade with time, and absolute, meaning that no purpose whether private, official, judicial, any state interest, or any other "higher" interests will ever justify interference, violation, and breaking the barrier protecting this most sensitive and innermost area of the human being, this "core of personality protected by the inviolable dignity of man", as the

[37] "Teilweise wird noch auf die Privatsphäre abgestellt, die eine Zwischenstellung zwischen der vollkommenen Abgeschiedenheit und der Teilnahme am öffentlichen Leben einnehmen soll, wobei sie stärker zur Intimsphäre als zur Sozialsphäre geneigt ist." Epping, V. (2010). *Grundrechte*. Springer, p. 273, Sec. 620.

Federal Constitutional Court of West Germany called it at the turning point of the liberation of half of Europe from the despotic domination of the communist governments and the Soviet Union, just before the unification with the eastern liberated part of Germany.[38] We are faced, as the Court emphasised, with "the last inviolable sphere of private life-shaping, which is completely divested of public power. Even serious interests of the general public cannot justify interventions in this sphere."

5.4 Conclusion: The Need for (Not)forgetting: Archival Deflation—Preservation—Archives and Records Destruction

In the last few decades, the right to be forgotten has been equated with the right to be remembered, the right to memory and, in some respects, even the duty to be remembered. But let us look at the whole situation from a slightly different perspective. It is not only archives and archiving that are caught between certain paradoxes: There are several parallel realities that can be documented in the field of preservation and archiving of public and private records:

1. An enormous, unprecedented, and apparently unsustainable amount of records and archival material is being created, preserved, and archived. The extreme and in the long term apparently unsustainable growth in the volume of archived records is supported by statistical data provided in Chap. 6.
2. Archives are littered with many records that do not have (or have ceased to have) the enduring and permanent historical or other value that would make them worthy of permanent archiving; such records should not be maintained.
3. Records are preserved that should not be preserved for the reasons of data protection, in particular for the protection of personality and privacy, and which—within the above categorisation of the right to be forgotten—fall into the category of permanent absolute right to be forgotten. Such materials include a number of broad categories of records that contain such sensitive personal data that should never be disclosed to anyone (even for later official consultation purposes), let

[38] Bundesverfassungsgericht. Beschluss des Zweiten Senats vom 14. September 1989, 2 BvR 1062/87.

alone made public. For this very reason, these records should be designated for destruction as part of the archival appraisal of records and shredding process. This could include, purely as an example, certain parts of court files, typically divorce records and records concerning other areas of civil litigations in which the sensitive privacy of individuals is dissected. Considering the example of divorce records, once a court dispute has been finally settled, not even a lineal descendant should have the right to consult such files. Any future official purposes of consultation are irrelevant, since the file should have been included in the shredding process only when the official need had passed, and, moreover, the key principle of democratic law "ne bis in idem" must apply in court cases, that is, that one cannot rule twice on the same matter.

We can also mention those records whose creators wished for them not to be preserved. The above-mentioned example of Franz Kafka's estate is quite illustrative and at the same time very controversial. In such case, another factor enters the decision-making process: Additional context and it needs to be considered whether the records have significant cultural, artistic, scientific, or intellectual value, for which they should be preserved despite the wishes of the creator, and so on. At the same time, it is necessary to precisely assess whether the records are of a public or private nature. In some cases, typically in the case of top political figures, the records status may be borderline between public and private.[39]

4. On the other hand, it is often the case that the most important of records that should be archived, are destroyed. There is evidence that in some cases the most valuable records in terms of future professional research, but also of general social interest, are destroyed, a phenomenon referring in particular to the public scrutiny of the performance of politicians, officials, and public officials (it is not uncommon that records of many public administration agencies very often do not lose their administrative value even after the expiration of their retention periods).[40] Here, the archives should start to play a much more pronounced role as a control and supervisory body, actively seeking out intentional and unintentional losses of precisely those records that

[39] This topic is dealt with in detail in Čtvrtník, M. (2021). Public versus private status of records and archives and analysis of the implications for their access.

[40] Some such cases are discussed ibid.

should have been preserved permanently or in the long term but which, for various reasons—including cases of illegal destruction—are not preserved. In this context, it seems appropriate to profile one of the roles of the archives in the direction and function that is nowadays by analogy performed in the field of financial and tax control by the tax administration and by the customs administration in the field of customs control.

The paradoxes analysed above shape not only the form of the work of archives and archivists, but are also characteristic of any work with information in public as well as private sphere.

A broader discussion should be initiated not only within the archival community, but also across scientific disciplines in an interdisciplinary sense and, of course, communicating with the public administration and record creators, on the issues raised concerning the provision of two parallel and difficult to reconcile rights to the free flow of information and access to it, as well as the protection of data, including personal data, the protection of personality and privacy, and the quantity and nature of records transferred to archives.

The right to know, the right to memory and, in some respects, also the duty of memory will always clash with the right to be forgotten, in which the protection of an individual's private and intimate sphere occupies the largest space. The above model of the four categories of the right to be forgotten is one of the aids to navigating the eternal polarity and clash between the right to know and the right to be forgotten.

One of the messages of this chapter is that records management and archiving policies in the areas of data, personality, and privacy protection, and access to records and archives should take much more account of the right to be forgotten than has been the case to date. There is another resonating point, that an unprecedented and probably unsustainable number of records and archival material is being preserved and archived. At the same time, records are archived that should not be archived precisely for reasons of data protection, especially for reasons of personal rights and privacy. These topics will be elaborated in a comprehensive and more detailed manner in the following chapters. Finally, they will also present the possibility of how some of the data minimisation tools, such as anonymisation or pseudonymisation, can be linked to the model of the four categories of the right to be forgotten elaborated in this chapter.

CHAPTER 6

Archival Inflation and Reduction of Records, Data, and Archives

Archiving represents one side of the coin, whose inseparable other side is the principle of destruction and non-preservation of data. Archiving can never do without the complementary principle of data reduction.

In his otherwise remarkable reflections, Viktor Mayer-Schönberger recently built one of the points of his account on the thesis that, while during most of the history of civilisation, remembering was significantly more expensive and laborious than forgetting, the latter of the two being completely predominant, during the evolution of civilisation from the invention of the printing press, through the industrial to the digital revolution, remembering gradually became cheaper and easier, and today, for the first time in history, remembering and preserving information is cheaper and easier than forgetting, not preserving, deleting.[1] At the same time, he maintains that digital data preservation is now cheaper than analogue preservation.[2] In his analyses, however, Mayer-Schönberger omitted many crucial points and criteria that come into play. He completely ignored, among other things, the phenomenon of data leaks, hacker attacks, deliberate breaches of data protection, including the financial costs associated with such protection and, in some cases, the payment of extortion demands. He paid little attention to archiving and, along with

[1] Mayer-Schönberger, V. (2009). *Delete: The Virtue of Forgetting in the Digital Age*. Princeton University Press. The latter conclusion can be found on p. 196.

[2] Ibid., pp. 65–67.

M. Čtvrtník, *Archives and Records*,
https://doi.org/10.1007/978-3-031-18667-7_6

that, he completely ignored the fact that a large part of the documentation of public institutions, which are subject to archiving obligations in the public interest, is still created in analogue form, and it is not within the financial capacities of any state to carry out a mass conversion of the entire corpus of such materials into digital form. At the same time, no state is capable of archiving the created records in their entirety. Moreover, such a step would be counterproductive, as it would surround that very small part of valuable data with information ballast, and as a result, make it very difficult and in many cases impossible to retrieve valuable information in the future. Mayer-Schönberger's "digital remembering" represents and will represent only a part of the memory and source wealth of human civilisation.

The archival sector and archiving in the public interest represent a space where, paradoxically, the most massive reduction of public records and data produced mainly by public bodies takes place. At the same time, it is one of the most important areas where personal data are processed. Archival management of personal data has two specific features:

1. Personal data are preserved and managed by archives for a very long time. If we define personal data in the narrow sense of the legislation regulating the protection and processing of personal data, which usually relates personal data to living individuals, then the archives actually manage personal data throughout their entire existence. The reason is simple: To date, almost 100% of material preserved in both public and private archives is archived permanently.
2. This is related to the second formative feature of archival processing of personal data: During the long-term and to this day intentional permanent preservation of archived materials, over time, as archives and the records they keep "age" and become older, a phenomenon occurs that can be described on some level as the "depersonalisation" of archival records in proportion to the death of those concerned in the records. As it happens, the oldest archives date back to the Ancient Orient, where the oldest roots of archiving develop with the beginnings of the earliest libraries. In the Ancient Orient, there was no real difference between libraries and archives, just as there was no difference between a literary work and a record at that time.[3] For example, a significant part of the preserved clay tablets from the

[3] Posner, E. (1972). *Archives in the Ancient World*. Harvard University Press, p. 27.

> Library of Ashurbanipal established in one of the largest cities in the Assyrian Empire, the ancient city of Niniveh in the seventh century BC, contains records closely related to the actions of the Mesopotamian government and consistent in content to the content of today's archives.[4]

Archiving oscillates between the proverbial millstones of two in many respects opposing public interests and the usually constitutionally guaranteed rights it is supposed to defend and fulfil: On the one hand, archives are supposed to be a tool for opening access to information, enabling study and research, but also for creating a multi-layered memory, beginning with the memory of the individual, the memory of the family, going all the way to the memory of the whole society and civilisation. On the other hand, archives are one of the major actors in the field of reducing the enormous and permanently unpreservable amount of data and records created especially after 1945. In addition, they are an important element in the protection of an individual against various threats in the form of misuse of their personal and sensitive data, in the field of personality and privacy protection.

This tension is reflected in yet another paradox of archiving: The preservation of data and records, including long-term/permanent archiving, is always determined and driven in its deepest foundations by its counterpart—that is, by non-preservation and destruction. The vast majority of records and data must necessarily be destroyed in order to preserve the absolute minimum for a longer period of time—sometimes with the vision of permanent archiving. The main challenge of the existing records management and archiving is how to limit the quantity of records and data stored so that they can be preserved or archived in the long term, given the limited financial, staffing, and storage capacities.

In the future, however, records management and archiving face yet another and probably much more challenging issue in dealing with the significantly increasing risk of data misuse, which always comes hand in hand with data and records. This risk was already pointed out 20 years ago by Terry Cook in a methodological study prepared for UNESCO on the subject of archival appraisal and selection of records containing personal

[4] Ibid.

data.[5] It is not inconceivable and, in my opinion, it is extremely likely that this perspective will soon outweigh the very problem of the quantity of records.

In this respect, the following three chapters will present an argument for the main thesis and conclusion that records management and, for the purpose of our research, archives and archiving in particular should, among other forms of testing, also carry out public interest and proportionality testing to determine on the one hand the value (historical, social, archival, etc.) of the record for long-term or permanent archiving, and on the other hand, assess the sensitivity of the data contained in the records together with the risk of misuse of such data intended for transfer to permanent archiving.

This does not mean, however, that records management and archiving are always faced with a Sophie's Choice—having to choose between the "life" and "death" of a record or the personal data it contains, when, for example, a decision is made to irreversibly anonymise personal data. In addition to data destruction and anonymisation, there are other ways to preserve personal data, at least in some cases, that at the same time allow us to bridge the phase of their high sensitivity and substantial risk potentially endangering the data holder, by, for example, hermetically sealing them for a certain period of time. These methods and some other options will be discussed further below.

All these cases consider the means of data minimisation in one way or another. Not strictly in the sense of the European GDPR regulation that regards minimisation solely as the irreversible destruction of this data, but we see minimisation in a broad sense, which also includes restrictions on access to records and information, but also, for example, restrictions on the period of their preservation.

Archiving is currently undergoing a significant transformation: The basic and practically only motivation for legal archival destruction after 1945 was the necessity to reduce the dramatically increasing volume of records created since World War II. Archiving then understood that the pre-war idea of one of the classics of archival theory, Hilary Jenkinson, was

[5] "There are several major problems in appraising records containing personal information: […] increasing concerns about violating personal privacy by permitting the collection of such data in the first place or its later diffusion." Cook, T. (1991). *The archival appraisal of records containing personal information: A RAMP study with guidelines.* PGI-91/WS/3. Paris, April 1991. https://unesdoc.unesco.org/ark:/48223/pf0000090644

unsustainable; the theory claimed that an archivist should preserve the archives exactly as received from the creator without reducing any records of his own volition. According to Jenkinson, this was the only way for the archive to retain its character of being an impartial witness, a sole account of the activities of a particular institution. Archival appraisal of records in terms of their possible historical significance was something Jenkinson would prefer to omit altogether. Records should be preserved primarily for the value they had during their active use. If anyone at all should evaluate records and possibly designate some for discarding, it should be the creator, not the archivist at the archive where the records should eventually be transferred.[6]

The sharp increase in the volume of records created after 1945 thus anticipated a phenomenon that contemporary society has and will continue to face—big data. According to one statistic, the volume of data and information created, captured, copied, and consumed globally (most of it already digital) has increased more than tenfold in the last decade; in 2020 it is estimated at 59 zettabytes compared to 2011 when the estimate was 5 zettabytes.[7] The same statistics then projects a total volume of 149 zettabytes for 2024, that is, in four years the volume of these data would double again (for 2021 the volume of 74 zettabytes was estimated). Another fact shall also be taken into account—the ever-increasing percentage of replicated and non-unique data in relation to unique data. The cited research has arrived at a rough estimate of 1:9 (unique data: replicated data) for 2020, with the trend slowly moving towards less unique and more replicated data; in 2024 the estimate of this ratio is 1:10.

However, it is not only the current era of "big data" that understands the risks and impossibility of processing and longer-term storage of all or the majority of the created information. Document management and archiving saw soon after 1945 that for capacity reasons alone it was

[6] Jenkinson, H. (1922). *A Manual of Archival Administration*. Clarendon Press, passim, for example, pp. 106–108; 128–129.

[7] Cf. statistics produced by the International Data Corporation. Results published here: IDC's Global DataSphere Forecast Shows Continued Steady Growth in the Creation and Consumption of Data. (2020, 8 May). https://www.businesswire.com/news/home/20200508005025/en/IDCs-Global-DataSphere-Forecast-Shows-Continued-Steady-Growth-in-the-Creation-and-Consumption-of-Data. The summary statistics are also published on the Statista website: Volume of data/information created, captured, copied, and consumed worldwide from 2010 to 2024 (3 December 2020). https://www.statista.com/statistics/871513/worldwide-data-created/

impossible to archive everything or almost everything and that massive reductions in the created records were needed in order to reduce their unsustainable volume. This purpose persists to this day. However, alongside this—which brings us to the aforementioned basal transformation—there are some very clear indications that it will be joined by yet another purpose or motivation: Data minimisation and the destruction of records, and probably in some cases even the destruction (or irreversible anonymisation) of records already stored in the archives will henceforth be substantially motivated also by the protection of people, their personality rights, privacy, and data.

The following chapters will demonstrate the premise that archives will (be forced to) take a much more detailed look at the issue of personality and privacy protection in the future, not only from the perspective of what data already stored in archives should be anonymised/pseudonymised when and how, what data should be available to which researchers and in which situations, but also in terms of what data to transfer to the archives for archiving and what data to destroy. In this respect, archiving and archival science should in the near future develop a methodology of archival appraisal that takes into account this aspect of reducing and minimising the data stored in archives and limiting their storage in order to protect the personality and privacy of the persons concerned in the records and archives.

I will analyse the issue of data protection, especially personal data, protection of personality rights and privacy in the archival sector in view of the role played by the process of reduction and minimisation of data that are, should, or should not be preserved. In doing so, I will pinpoint some specific examples of misuse of personal data that were stored either in still living records management or already archived. In the analysis of the process of reduction and minimisation of data maintained in archives, I will also look at the anonymisation and pseudonymisation of data that are either already stored or aspire to be archived in the future.

6.1 Records Archiving as a Tool of Personal Data, Personality, and Privacy Protection

Even though any archiving of (personal) data can itself be interpreted eo ipso as a security risk and a threat of potential future misuse, archives and archiving also act as a protector of data and rights, including personality

rights and privacy. After all, since the earliest ancient archives, the motivation for the protection of rights and the possibility of their potential future claim, application, and enforcement has been at the heart of archives. In his classic work on archival history, Ernst Posner detected several basic groups that come into play when creating records from ancient times to the present day; he called them "constants in record creation".[8] In the vast majority of cases, the motivation for their creation lies in the very foundations of the exercise of rights and claims for which the archived records were intended to serve as evidence. Among these constants, Posner highlighted particularly those records serving as testimony and evidence of past administrative actions, financial and other accounting materials used by the ruler or another owner for the administration of their estates, tax records, records serving the civil registry for military purposes, forced labour, various payments and levies, and notarial records.

These intentions have persisted to a significant extent through the medieval period to the present day. Particularly in the twentieth century, the content of archives began to consist to a greater extent of other material serving also personality rights and their protection, although the original purpose of their creation was often different, sometimes even directly opposite. A prime example can be found in court records and records created by prosecutors, security services and other entities, especially public authorities, in countries that underwent a phase of totalitarianism and subsequent transition to democracy in their modern history. This is specifically the case of prosecution and court investigative files in which citizens were unjustly prosecuted and sentenced in politically motivated trials during the period of Nazi or Communist totalitarianism, in which their rights, including personality rights, were fundamentally damaged; these files usually became a direct part of and an essential piece of evidence in rehabilitation proceedings in which the damaged rights, including personality rights, were rectified as far as possible. At the same time, these rehabilitation files, as well as the original court files of courts where political

[8] Posner, E. (1972). *Archives in the Ancient World*, pp. 3–4.

trials took place, are determined for permanent archiving in their entirety[9]; on the other hand, the vast majority of other agendas of prosecution authorities and courts undergo archival selection and only a very small percentage is maintained and the absolute majority (about 90–95%) is designated for destruction.

The situation is similar for security forces materials, especially those created by the secret police and intelligence services of the totalitarian period. In this case again, records that represent one of the most significant violations of citizen's rights ever, after the fall of totalitarianism, become one of the key sources for the rehabilitation and satisfaction of victims of injustice. For example, in the case of the Stasi Records Archive, the former East German State Security (Stasi-Unterlagen-Archiv), from the beginning of its existence in 1990 to 31 December 2020, an astonishing 7,353,885 requests were addressed to the archive for consultation or access to its archival records and data, of which 3,349,609 were made by citizens.[10] This represents an average of approximately 240,000 applications per calendar year. Nearly half of them were requests from individual citizens, whose interest was usually motivated by the desire to find out whether and, if so, how the Stasi and the state were interested in them and collected information about them, and how their rights were violated by the public authorities. Official requests for consultation served to a large extent to correct and atone for injustices and violations of rights. Purely research- or education-oriented interest represents an absolute minimum

[9] For example, in the case of the Czech Republic, which went through the phase of Nazi occupation and the subsequent Communist totalitarianism, the rehabilitation files (marked Rt and Tr) as well as, for example, the files of the former State Court (Státní soud), where the largest political trials took place during the most rigid period of the Communist regime in the late 1940s and 1950s, are listed in the Records retention schedule issued by the Ministry of Justice as subject groups type 'A'. Cf. Instrukce Ministerstva spravedlnosti ze dne 19. prosince 2008, č. j. 94/2007-OIS-ST, kterou se vydává skartační řád pro okresní, krajské a vrchní soudy. Příloha č. 1 Spisový a skartační plán [Instruction of the Ministry of Justice of 19 December 2008, 94/2007-OIS-ST, issuing the retention schedule for district, regional, and high courts. Appendix 1 Records Retention Schedule]. The obligation to submit rehabilitation files for selection as archival material is also stipulated by the Czech Archives Act: Act No. 499/2004 Coll. on Archiving and Records Management amending certain other acts [Zákon o archivnictví a spisové službě a o změně některých zákonů] of 30 July 2004, Appendix 2: Records that shall always be submitted for selection as archives based on their content, item 15. Archivists could thus in theory decide not to keep all the rehabilitation files, but in the practice of Czech archives and as far as I am aware, this is not the case.

[10] Das Stasi-Unterlagen-Archiv in Zahlen. https://www.bstu.de/ueber-uns/bstu-in-zahlen/#c2391

of the total number of requests to the Stasi Records Archive (in recent years, with one exception, it has been below 1000 requests per year). It should also be taken into account that the archive manages a total of 111 linear kilometres of archival materials, of which 51 kilometres were archived and processed by the Stasi itself, another 60 kilometres were found disorganised in the Stasi offices after the fall of the East German totalitarian regime. To date, the Stasi Records Archive has managed to process and open 94% of these materials to research interest.

The fact that the preservation and archiving of records can serve to protect various rights has also been demonstrated in some specific cases. The year 1997 saw the flare-up of the case of the then Union Bank of Switzerland, now UBS, who deliberately destroyed records proving ownership of property stolen by the Nazis from Holocaust victims, lists of mortgaged buildings, general ledgers, personal bank accounts, including Swiss accounts of Holocaust victims.[11] The case was triggered by a security guard at the bank who happened to come across these materials in the bins in which records designated for destruction were collected. He secretly removed some of this material and made the case public. It was subsequently picked up by the world press. UBS later admitted that its employees had accidentally destroyed some materials from the Nazi period that could provide evidence regarding the affairs and property of Holocaust victims. The bank thus violated an express prohibition mandated by the Swiss government against the destruction of such material in light of the then ongoing investigation into the collaboration of Swiss banks with the Nazis, and their assistance in legalising the stolen wealth of Nazi victims. The employee in question, Christoph Meili, who brought the case of unauthorised destruction to the public, was fired from UBS and, in addition, criminally investigated for violating banking secrecy. Meili subsequently left Switzerland under pressure from threats made by neo-Nazi groups[12] and became the first-ever Swiss political asylum-seeker in the USA. As a result of public pressure, the bank suspended its chief archivist,

[11] The case is neatly summarised by Barry, R. (2005). Ethics issues for creators, managers, and users of records. In M. Procter, M. Cook, C. Williams (Eds.), *Political Pressure and the Archival Record* (pp. 131–149). Society of American Archivists, pp. 132–133.

[12] Swiss end bank guard investigation (1997, 2 October). *Washington Post*. https://www.washingtonpost.com/archive/politics/1997/10/02/swiss-end-bank-guard-investigation/5bc310f0-c2ba-4f99-a92f-bdab58240798/

Erwin Haggenmueller,[13] who had allegedly made the decision to shred the records in question and who was thus blamed in an internal UBS investigation.

Another notable example is the so-called fichiers juifs, a registration file of Jews living France at the time of the occupation, which I will discuss in more detail in Chap. 7, and which the French Minister of the Interior decided to destroy shortly after the liberation of France from Nazi rule, in order to protect people of Jewish origin and guarantee their rights; he then reversed his decision and decided to preserve the files for the same reason, especially for the purposes of compensation.

However, the preservation of records and archiving as a tool for the protection of personality rights is also demonstrated in a number of other cases. Chapter 4, discusses several cases related to child sexual abuse. In the case of the German Odenwaldschule, the archive consulted with the relevant prosecutor's office and decided on the premature transfer of the material for preservation and possibly permanent archiving of some of its parts, arguing that both the preservation of the records and the guarantee of proper management of the personal data in them, including restrictions on access, are crucial for the investigation of the entire case and the protection of the personal data and rights of those affected. The need was intensified by the fact that there had previously been unauthorised data leaks from these records.

Another form of protection of rights, including personality rights, is demonstrated in the same chapter that analyses the cases of some Roman Catholic diocesan "secret archives" relating to cases of child sexual abuse by clergy and church leaders. In this case, the crucial moment is the Church's deliberate and unauthorised destruction of the records testifying to secret internal investigation into the cases of sexual abuse, especially of children. Needless to say, the risk of illegal destruction of records resulting in violation of the rights of the victims is not solely limited to the Church. The Australian Heiner Case, also known as "Shreddergate", has become

[13] Stein, L. (1997, 5 June). ADL to Aid Swiss Bank Guard Who Turned over Documents. *Jewish Telegraphic Agency*. https://www.jta.org/1997/06/05/lifestyle/adl-to-aid-swiss-bank-guard-who-turned-over-documents

one of the most debated cases of illegal records destruction in Australia.[14] In 1989, a retired Queensland stipendiary magistrate, Noel Heiner, launched an investigation into allegations of sexual abuse at the government-run John Oxley Youth Detention Centre in Brisbane, Australia. Heiner did not complete the investigation and forwarded the file he had been working on to the Queensland Department of Family Services and Aboriginal and Islander Affairs. The Department was later questioned about this file by Kevin Lindeberg and attorney Ian Berry. It turned out the file had been destroyed, not at a point prior to Lindberg's request, but later, when it was apparent to the then Queensland government under Wayne Goss that Heiner's file was being sought as evidence for the anticipated trial in the matter.[15] The government approached the state archivist at the time to give an opinion on whether the incriminating Heiner file had historical value and should be archived, but deliberately withheld the fact that the file would probably be requested in future court proceedings. The archivist was given 24 hours to make a decision whether to destroy the record, which was eventually the case. Lindeberg subsequently initiated a series of legal actions to prove that the destruction of the file was illegal. In the following years, special Australian Senate committees were formed to investigate the case, including the issue of the illegal destruction of Heiner's file. In 2014, Attorney General Jarrod Bleijie finally decided to suspend the investigation into the case.[16]

Not only should documentation testifying to crimes of sexual violence not be destroyed prematurely, on the contrary, it should be preserved for as long as it can potentially serve as evidence. It is also necessary to point out that many countries have been gradually extending or even abolishing the statute of limitations for such criminal offences (they do not exist, for

[14] In 2002 Chris Hurley reported on the case in Hurley, Ch. (2002). Recordkeeping, Document Destruction, and the Law (Heiner, Enron and McCabe). *Archives & Manuscripts*, 30(2), 6–25. https://publications.archivists.org.au/index.php/asa/article/view/9597. On the case as of 2005 cf. Barry, R. (2005). Ethics issues for creators, managers, and users of records, pp. 134–137. Tony Moore provides up-to-date summary information on the case in Moore, T. (2021, 1 January). Goss cabinet knew it destroyed documents wanted for court case. *Brisbane Times*. https://www.brisbanetimes.com.au/politics/queensland/goss-cabinet-knew-it-destroyed-documents-wanted-for-court-case-20201230-p56qw9.html. A comprehensive overview of the case is available at: http://heineraffair.info/index.html

[15] Barry, R. (2005). Ethics issues for creators, managers, and users of records, p. 134.

[16] Moore, T. (2014, 2 July). No Heiner trial for Goss ministers: Bleijie. *Brisbane Times*. https://www.brisbanetimes.com.au/national/queensland/no-heiner-trial-for-goss-ministers-bleijie-20140702-zstrm.html

example, in the United Kingdom or in the Netherlands, where all statutes of limitations for serious sexual abuse offences were abolished in 2013 and the minimum prison sentence is eight years). If this trend continues, the material in question should be archived permanently, or the retention periods for such records should be extended (for more detail see Chap. 4).

The problem in these and similar cases lies in the detection of the relevant records, as information about the commission of these crimes often comes to light only after a long delay and the records can thus be destroyed in the meantime. However, this was not the case in the destruction of Heiner's investigation file, as the responsible authorities were well aware that the file concerned child sexual abuse and that it was to become an important piece of evidence in an anticipated trial.

Although archiving is one of the important tools for the protection of rights, including personality rights, data protection, and privacy, let us now concentrate on the main topic of the following chapters, which is quite the opposite; it concerns the risks associated with the preservation and archiving of personal data, their minimisation and storage limitation as a tool for the protection of personality rights and privacy and in relation to archives and archiving.

6.2 Archival Inflation and the Reduction of Records, Data, and Archives

It may sound like heresy, especially from the point of view of archiving, yet the only way to protect certain data (including personal data) is simply not to maintain them, that is, to destroy them. Traditionally, the primary interest of archives and archivists tends to go in the opposite direction that is towards records and data preservation. In the 1980s, the famous French historian, Pierre Nora, claimed that the contemporary climate was ruled by a "religion of preservation" ("réligion conservatrice") and "archival production" ("productivisme archivistique").[17] In his view, contemporary society suffered from an "obsession to preserve". However, today archivists—at least those who deal with modern records from the twentieth and twenty-first centuries—know that in addition to the art of preservation, the art of destruction is just as necessary for archival science.

[17] Nora, P. (1984). Entre Mémoire et Histoire. La problematique des lieux. In P. Nora (sous la dir.), *Les Lieux de mémoire, vol. 1 (La République)* (pp. XVII–XLII). Gallimard, cf. in particular pp. XXVI–XXVIII.

From a philosophical perspective, this phenomenon was aptly described by Jacques Derrida in the 1990s in his now classic work of archival theory; he distinguished two basic concepts that drive archiving, which he tried to elaborate using the categories of Freud's psychoanalysis. The first is the "destruction drive" or, as Derrida writes, "the aggressive and destructive drive" ("pulsion de destruction", "pulsion d'agression et de destruction"), the drive of "radical destruction" ("effacement radical") corresponding to the "death drive" ("pulsion de mort").[18] The second is the conservation drive ("désir d'archive"; "pulsion de conservation"; "pulsion d'archive") corresponding to the pleasure principle. Derrida characterises this drive as the archive desire or fever ("mal d'archive"), which also gave name to his entire book.[19]

The need to destroy the absolute majority of created records saw a radical increase especially after 1945, and this trend has obviously continued in recent decades and years. The development can also be clearly demonstrated by the statistical figures and the methodological recommendations based on them. In 1983, the United Nations noted that the central or national archives of countries from different parts of the world that participated in the empirical survey maintain between 5% and 40% of the total created documentation (Table 6.1).[20] For the past several years, the UN has recommended the archiving of approximately 5–10% of records (Table 6.1).[21] The British National Archives estimate the number of archived records to be only 5%[22] and this number—as illustrated—corresponds to the amount of material preserved in the State Regional Archives

[18] Derrida, J. (1995). *Mal d'archive. Une impression freudienne.* Galilée, pp. 25–27.

[19] Ibid., p. 38.

[20] Guptil, M. B. (1986). *Evaluation et tri des documents d'archives dans les organisations internationales: une étude RAMP accompagnée de principes directeurs.* Programme général d'information et UNISIST. UNESCO, p. 9. See also Franz, E. G. (1984). The archivist and the inflation of contemporary records. In *Conférence internationale de la table ronde des archives, 22ème, Bratislava, 17–20 October 1983.* Conseil international des archives, French version pp. 19–52, English version pp. 117–145, here pp. 121–122.

[21] United Nations. *Records and Information Management Guidance 5: When and how can I destroy records?* https://archives.un.org/sites/archives.un.org/files/5-guidance_destroying_records.pdf

[22] According to information in the British National Archives 2011 guide on disposal of records: The National Archives. (2011, 24 March, last updated). *Guide 8: Disposal of records.* http://www.nationalarchives.gov.uk/documents/information-management/rm-code-guide8.pdf, pp. 3 and 12.

Table 6.1 Percentage of archives preserved in relation to records destroyed

Archives	*Percentage of archives preserved in relation to records destroyed*	*Information as of*
UN Archives (selection)—UN Statistical Survey	5–40% (majority)	1983
UN—methodological recommendation	5–10%	Current recommendations
The National Archives (Great Britain)	ca. 5%	2011
State Regional Archives in Prague (Czech Rep.)	ca. 5%	2016
National Archives and Records Administration—NARA (USA)	1–3%	Current status

in Prague, one of the regional state archives in the Czech Republic.[23] However, the US National Archives—NARA, National Archives and Records Administration, preserves only 1–3% of the records created by the US federal government (Table 6.1).[24]

This growing need to destroy is mirrored by the rapidly increasing volume of archived records (Table 6.2). No other period had ever preserved so much official material. Let us now take a look at two striking examples. In 1985, the US National Archives and Records Administration (NARA) managed an impressive 416 linear kilometres of archival records (throughout this study, I will round up to the nearest linear kilometre).[25] Twenty-eight years later, at the end of 2013, the number had grown to a

[23] Státní oblastní archiv v Praze. (2017). *Zpráva o činnosti za rok 2016* [State Regional Archives in Prague, *Activity Report 2016*]. http://www.soapraha.cz/Files/vyrocni-zprava-soa-2016.pdf, pp. 84–85.

[24] See U.S. National Archives and Records Administration National Archives Frequently Asked Questions. http://www.archives.gov/faqs/

[25] In the USA, the volume of archival material is not measured in linear metres, but in cubic metres or feet. Conversion to linear metres is not an easy task. I based my calculations on an estimate made by UNESCO in the early 1980s. Their calculations resulted in this formula: 1 cubic meter corresponds to 35.315 cubic feet, and these in turn correspond to 10 linear metres of archival material. Cf. UNESCO (General Information Programme and UNISIST). (1982). *Survey of Archival and Records Management Systems and Services 1982.* PGI-82/WS/3. https://unesdoc.unesco.org/ark:/48223/pf0000048252, p. 3.

Table 6.2 Increase in the volume of archival material in selected archives in recent decades

Archive	*Average percentage increase in the volume of archival material in 1 calendar year*	*Period under review*
National Archives (National Archives and Records Administration—NARA), USA	7.7%	1985–2013
Federal Archives (original figure for West Germany only, final figure after German reunification)	11%	1977–2018
Federal Archives, Germany	5%	2012–2018
National Archives (Library and Archives Canada), Canada	4.2%	2005–2015
Czech archives (complete)	2%	2002–2014
Departmental archives (complete), France	2%	2006–2019
State Archives of Baden-Württemberg	1.68%	2006–2019
National Archives, France	1.25%	2014–2019
National Archives, France	0.7%	2019
National Archives, United Kingdom	0.5%	2011–2020
(Regional archives, France)	30%	2006–2015

breath-taking 1308 linear kilometres.[26] In just under 30 years, its volume had more than tripled. Even more incredible is the increase in the volume of a specific part of French "regional archives" (i.e., the archives of French regions constituting a special level of French public administration established during the second half of the twentieth century), which will be further discussed below, and which had quadrupled (sic!) in volume in just 10 years between 2006 and 2015, growing cumulatively by nearly 300% (in this review, I will always compare the increase in archival volume to its increase in the first year of the period under review and will do so in the case of multi-annual cumulative calculations as well). Their volume then increased from 32 linear kilometres to 127 kilometres (Table 6.2)!

[26] Cf. National Archives and Records Administration. (2013). *Annual Report 2013: Preserving the Past to Protect the Future. Summary. National Archives and Records Administration. Performance and Accountability Report.* https://www.archives.gov/files/about/plans-reports/performance-accountability/2013/par-summary.pdf. Cf. also: United States Government Accountability Office. (October 2010). *GAO-11-15. Report to the Ranking Member, Committee on Finance, U.S. Senate. National Archives and Records Administration. Oversight and Management Improvements Initiated, but More Action Needed.* https://www.gao.gov/assets/gao-11-15.pdf

If Daniel Doležal was really seriously taken aback by the increase in the linear metres of archival materials stored in archives in the Czech Republic—between 2002 and the beginning of 2015 the increase was an alarming 27.6%, and this without taking into account digital archives,[27]—then the three times faster rate of growth in the volume of archival material in the US National Archives would take his breath away, not to mention the specific situation of French regional archives, where the rate of growth is ten times greater than the summary figures for Czech archives. The approximate annual increase of less than 2% in the volume of archival records in Czech archives is more than overshadowed by the almost 8% (7.7% to be exact—all percentages in this text are rounded to the nearest tenth) average annual increase in the volume of archives in the US National Archives and falls massively behind the almost 30% average annual increase in the volume of French regional archives.

The rate of increase in the volume of archives in the US National Archives, but also in Czech archives, is indeed—to put it very mildly—striking and calls for a deeper reflection. The figures prompted me to research what the situation is in other archives in some of the countries with the most advanced archival systems when it comes to these parameters. The results are quite remarkable.

My statistical survey included selected archives from the USA, Canada, France, the United Kingdom, Germany, and the Czech Republic. The differences between the individual archives and countries are considerable. Unfortunately, publicly available sources do not always provide exactly comparable data for the same time period. I am therefore compelled to refer to the increases in the volume of archival material over the last 10 or 15 years or so, with slight variations.

By far the largest increase in the volume of archives has been recorded by a very specific type of French public archives, the so-called regional archives *(archives régionales*), that is, archives preserving materials created by the relatively recently established new level of local government in

[27] Cf. Doležal, D. (2016). Malé zamyšlení nejen nad jedním výsledkem generální inventury 2012–13. K situaci českých archivů na příkladu SOA Praha [A brief reflection not only on the result of one stocktaking 2012–2013. On the situation of Czech archives using the example of SOA in Prague]. *Archivní časopis* [Journal on Archives], 66(3), p. 262. Statistical data according to Hora, J., Wanner, M. (2015). Národní dědictví v roce 2015 [National Archival Heritage in 2015]. *Archivní časopis* [Journal on Archives], 65(3), 252–271, p. 255.

France—the regions. The French regions, however, date their administrative origins in the modern era back to 1963 or 1964, but it was not until 1982 that they acquired the status of a genuine local authority with their own powers, which happened in the context of the then radical process of the decentralisation of public administration in France. French regional archives are therefore very young institutions with a relatively recent "birth date", and that is also one of the reasons for the high increase in their volume.

The French regional archives are followed—apart from the specific situation of the German Federal Archives, which will be discussed later—by the US National Archives, with an average annual increase of 7.7% in the period 1985–2013. The third position on my list of selected archives is held by the German Federal Archives (Bundesarchiv). First, it is worth noting the increase in the volume of the archive over the long time horizon of 41 years between 1977 and 2018. It should not go unnoticed that West and East Germany unified during this time and the figure is thus slightly distorted. While in 1977 the West German Bundesarchiv held 72 kilometres of archival material,[28] in 2018 it was already 420 kilometres for the whole of Germany.[29] In 41 years the archive grew by 348 kilometres of records, a cumulative increase of 483%! This means an average annual growth rate of 11%! What is more, this figure does not include the increase in digital records. Recent acquisitions of archival material in the German Bundesarchiv show an average annual increase of 5% between 2012 and 2018. While in 2012 the Federal Archives held 323 kilometres of archival records,[30] in 2018 it was, as mentioned, 420 kilometres, 97 kilometres, that is 30% more!

The National Archives of Canada (Library and Archives Canada) increased its archival holdings by 42.2% (!) between 2005 and 2015, an

[28] Andrea Hänger takes the figure from Hans Booms. Hänger, A. (2019). Die Geschichte des Bundesarchivs. *Forum 2019. 100 Jahre Reichsarchiv*. Bundesarchiv, 107–116. https://www.bundesarchiv.de/DE/Content/Publikationen/Forum/forum-2019.pdf?__blob=publicationFile, p. 109.

[29] Grütters, M. (2019). Grußwort anlässlich des Festaktes "100 Jahre Reichsarchiv" am 22. Oktober 2019 im Deutschen Historischen Museum in Berlin. *Forum 2019. 100 Jahre Reichsarchiv*. Bundesarchiv. https://www.bundesarchiv.de/DE/Content/Publikationen/Forum/forum-2019.pdf?__blob=publicationFile, 7–10, p. 7.

[30] Herrmann, T. (2013). Das Bundesarchiv in Zahlen. *Forum 2013*, I–IV. https://www.bundesarchiv.de/DE/Content/Publikationen/Forum/forum-2013.pdf?__blob=publicationFile, p. I.

average of 4.2% per calendar year (Table 6.2).[31] Just as a matter of interest, I would like to add that in 2005 this archive (not including the library holdings of the part of this archive connected with the library) managed 169 kilometres of archival material, of which 46 kilometres were of private-law provenance. In 2015, the total was already 241 kilometres of archives, an increase of 72 linear kilometres in just 10 years!

Lower figures can be seen, for example, in the case of summary data for the whole of archives in the Czech Republic, where, the average increase in the volume of archives in recent years has been approximately 2% per year (Table 6.2), and a similar figure applies to the French departmental archives responsible for the management of archives of departmental provenance as one of the levels of public administration in France (Table 6.2). Between 2006 and 2019, the French departmental archives saw a 2% annual increase in total average volume.[32] To use specific numbers, this represents an increase of 602 kilometres in the total volume of French departmental archives over 14 years, with a total of 2713 kilometres of archives stored at the end of 2019.[33] The 2% growth also applies to the last five years (2014–2019).

However, we also come across archives that are not afraid to close the floodgates on the stream of new archival material for permanent storage in a more significant way. For example, one of Germany's archives, Landesarchiv Baden-Württemberg (State Archives of Baden-Württemberg), which increased its volume by an average of 1.68% between 2006 and 2019 and grew by 31.5 kilometres to a total of 165 kilometres (Table 6.2), is below

[31] The statistical survey was based on: Library and Archives Canada. (2006–2007). *Report on Plans and Priorities.* http://www.tbs-sct.gc.ca/rpp/2006-2007/lac-bac/lac-bac-eng.pdf. Cf. also: http://www.bac-lac.gc.ca/eng/about-us/about-collection/Pages/about.aspx

[32] Comprehensive statistics for the period 2010–2019 published online: https://francearchives.fr/article/37978. The situation at the end of 2005 shows: *Des Archives en France – 2005. L'activité de la direction des Archives de France et des services publics d'archives.* (2006). https://francearchives.fr/file/b742bae0d42bc0accdefb6c7905ec591fb5c6f5a/static_1176.pdf, p. 5.

[33] On the 2019 data not only for departmental archives cf. *Des Archives en France. L'activité des services d'archives 2019.* (2019). https://francearchives.fr/file/6d139a81db2d82b09aedc3ed2828c6cbb57f7a53/BD-rapport-2019-2020-ArchivesenFrance.pdf. Cf. also https://francearchives.fr/file/107c185e375831ac752cef7b834d80b5a74958e9/AD_2019_DonneesCles.xls

the annual growth rate of 2%.[34] But the French National Archives goes much further; in the five-year period of 2015–2019, the increase was only 1.25% per year (Table 6.2). The total number went from an initial 349 kilometres[35] of archival records at the beginning of 2015 to 370 kilometres at the end of 2019.[36] However, concentrating on the increase in the volume of archival material purely in 2019, the number gets even lower. The new addition (not including digital archives) amounted to 2.6 kilometres,[37] an increase of only 0.7% of paper records in relation to the total volume of the maintained archives (Table 6.2)!

Finally, the archive growing at the slowest pace in the sample I selected, is the British National Archives. In the decade between 2011 and 2020, its

[34] For statistical figures regarding the Landesarchiv Baden-Württemberg in 2019, see Friesen, I. (2020). Rückblick auf das Jahr 2019. Jahresbericht des Landesarchivs Baden-Württemberg. *Archivnachrichten*, 60, 36–42, https://www.la-bw.de/media/full/69705, p. 42. For statistical figures regarding the Landesarchiv Baden-Württemberg in 2005, see the annual report published as Kretzschmar, R. (2006). Das Landesarchiv Baden-Württemberg im ersten Jahr seines Bestehens. Jahresbericht für 2005. *Archivnachrichten*, 32, 12–15. https://www.landesarchiv-bw.de/media/full/44485, p. 14. Cf. also *Landesarchiv Baden-Württemberg – Eröffnungsbilanz und Betriebsergebnisse*. (2005). http://www.landesarchiv-bw.de/sixcms/media.php/120/Eroeffnungsbilanz_und_Betriebsergebnisse_2005.pdfhttp://www.landesarchiv-bw.de/sixcms/media.php/120/Eroeffnungsbilanz_und_Betriebsergebnisse_2005.pdf

[35] *Archives nationales – Chiffres clés 2014*. https://francearchives.fr/file/30899b279470069db52a09955802ae2991c6d828/static_8619.pdf. However, looking at the subsequent annual records, it is highly likely that the figure given in the 2014 annual report of the National Archives (Archives nationales. *Rapport d'activité 2014*. http://www.archives-nationales.culture.gouv.fr/documents/10157/11405/Rapport_d'activit%C3%A9_2014_des_Archives_nationales_%28France%29.pdf/9a5ea923-ac06-4c67-a983-fd0e2aceac60, p. 4) is provided by mistake. The 2015 annual report indicates the volume of 356 kilometres and an increase of 7 kilometres during the single year. Archives nationales. *Rapport d'activité 2015*. http://www.archives-nationales.culture.gouv.fr/documents/10157/11405/Rapport-d-activite-2015.pdf/1c9cf41e-7094-4f90-b257-4211023eecdb, p. 12.

[36] Archives nationales. *Rapport d'activité 2019*. http://www.archives-nationales.culture.gouv.fr/documents/10157/11405/Rapport+d%27activit%C3%A9%20des+AN+-+2019/652514a1-a16f-4852-91f0-118fc2dec805, p. 4.

[37] Archives nationales, Rapport d'activité 2019, p. 20.

volume grew by an average of only 0.5% (Table 6.2)![38] The total volume of the UK National Archives is also relatively small relative to the size of the country and its population (since 2011, Scotland has had its own central archive, the National Records of Scotland), amounting to about 200 kilometres of archival records. It should be added, however, that the volume of archival acquisitions at the British National Archives has increased significantly in recent years. From 2011 to 2020, the transfer in terms of linear metres was respectively: 373, 612, 882, 799, 898, 1492, 1663, 1343, and finally 2018. It needs to be added that electronic records are not included (Table 6.2).

However, any future increase in the volume and percentage of records destroyed within the archival appraisal procedures in relation to preserved material should not occur only due to the long-term unsustainable increase in the volume of archival material, but also, to no lesser extent, due to the protection of the personality, privacy, and personal data of those concerned in such material. I shall defend this argument in the text below.

[38] I base my data on the British National Archives annual reports. See: The National Archives. (2020). *Annual Report and Accounts of The National Archives 2019–20.* https://www.nationalarchives.gov.uk/documents/annual-report-accounts-2019-2020.pdf, p. 88. The National Archives. (2019). *Annual Report and Accounts of The National Archives 2018–19.* https://www.nationalarchives.gov.uk/documents/the-national-archives-annual-report-and-accounts-2018-19.pdf, p. 96. The National Archives. (2018). *Annual Report and Accounts of The National Archives 2017–18.* https://www.nationalarchives.gov.uk/documents/the-national-archives-annual-report-and-accounts-2017-18.pdf, p. 88. The National Archives. (2016). *Annual Report and Accounts of The National Archives 2015–16.* https://www.nationalarchives.gov.uk/documents/annual-report-and-accounts-2015-2016.pdf, p. 94. The National Archives. (2015). *Annual Report and Accounts of The National Archives 2014–15.* https://www.nationalarchives.gov.uk/documents/annual-report-2014-15.pdf, p. 88. The National Archives. (2014). *Annual Report and Accounts of The National Archives 2013–14.* https://www.nationalarchives.gov.uk/documents/annual-report-13-14.pdf, p. 80. The National Archives. (2013). *Annual Report and Accounts of The National Archives 2012–13.* https://www.nationalarchives.gov.uk/documents/annual-report-12-13.pdf, p. 70. The National Archives. (2012). *Annual Report and Accounts of The National Archives 2011–12.* https://www.nationalarchives.gov.uk/documents/annualreport-11-12.pdf, p. 66.

CHAPTER 7

Archiving as Security Risk to Protection of Persons and Their Personality Rights

The preservation of any data, including their subsequent permanent archiving, always carries the risk that this data may be subject to unauthorised access, may be extracted and misused. This potential misuse takes on various forms and has different consequences. In this chapter I will take a closer look at some specific record categories which also become, either fully or partly, archival records in the final phase of their life cycle, usually stored in public archives. In doing so, I will present several actual cases illustrating how and in what form data misuse may occur.

The key point here is that the potential risks of data misuse apply both to the management of so-called live records, that is, those that are still held by their creators, whether in registries, actively used databases, and so on, as well as to the archival care of those records that have already been transferred to the archive. At the same time, many archives are still not sufficiently aware of the risks that are transferred to them along with the records, especially those that carry sensitive information about people and which are therefore also valuable in terms of monetisation, most often in the form of blackmail by hackers and data thieves.

The risks of misuse as well as the impact of such misuse have increased dramatically with digital data. I will demonstrate this theory in the following text and illustrate it using the examples of medical records and personal data leaks in the US National Archives and Records Administration (NARA). There are already many estimates of the number of leaks and misuses of digital data, including calculations of the costs involved and

M. Čtvrtník, *Archives and Records*,
https://doi.org/10.1007/978-3-031-18667-7_7

some other remarkable parameters. A 2020 report by IBM Security seeks to quantify these financial costs.[1] In their summary report, the authors used data from 524 organisations in 17 countries and based on these they abstracted global average figures. The very ratio of the individual data categories is well worth noting. By far the absolute largest share of 80% of total data leaks concerned data containing customers' personal data. Figures related to intellectual property come second (32%) with a large margin.[2] The estimated costs associated with the leak or loss of a single record containing customers' personal information was $150.[3] The volume of data leaks as such reaches alarming figures.[4] The ones that stand out are the AOL data leaks (leak of 92 million client names and email addresses in 2005), TJX (leak of VisaCard and MasterCard payment details of 94 million customers in 2007), Sony PlayStation Network (names, addresses, and apparently credit card data of 77 million customers leaked in 2010), but also Deep Root Analytics, which leaked a database containing data on 198 million voters in the USA, which was then used for Donald Trump's presidential campaign in 2016. The absolute winner, however, is Yahoo leaking the data on 1 billion user accounts. The quantity and quality of the leaked data would however be exceeded by the so far only partially verified data leak, in which a hacker stole personal and sensitive data from the Shanghai police database on approximately 1 billion Chinese citizens including the name, address, birthplace, national ID number, mobile number, as well as data on the criminal activities and police investigations of these persons, ranging from petty theft and cyber fraud to, for example, reports of domestic violence.[5]

With this perspective, it is all the more important that in their acquisition of records archives also consider the risks involved in the management of the category or group of records concerned and assess whether it is

[1] IBM Security. *Cost of a Data Breach Report 2020*. https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/pdf

[2] IBM Security. *Cost of a Data Breach Report 2020*, p. 18.

[3] IBM Security, Cost of a Data Breach Report 2020, p. 19.

[4] Some of the biggest data leaks in recent years are summarised in de Groot, J. (2020, 1 December). The History of Data Breaches. *Digital Guardian*. https://digitalguardian.com/blog/history-data-breaches

[5] Hao, K., Liang, R. (2022, 4 July). Vast Cache of Chinese Police Files Offered for Sale in Alleged Hack. *The Wall Street Journal*. https://www.wsj.com/articles/vast-cache-of-chinese-police-files-offered-for-sale-in-alleged-hack-11656940488; Hacker claims to have stolen 1 billion records of Chinese citizens from police. (2022, July 6). *Reuters*. https://www.reuters.com/world/china/hacker-claims-have-stolen-1-bln-records-chinese-citizens-police-2022-07-04/

really necessary to archive those records permanently. It is in this context that this study presents one of its main theses: Archives should carry out proportionality testing and measure, on the one hand, the value of a record for permanent archiving and its importance for future use for various purposes, and, on the other hand, the sensitivity of the data contained in the transferred record and the risk of their (future) misuse.

7.1 Medical Records and Data Security

Medical records represent a typical and very illustrative example of a records category that is, first, very vulnerable to misuse and, second, the consequences of any misuse, given that these records contain some of the most sensitive personal data that can be kept, are fatal. This is by no means just about the risk of an unauthorised person finding out about an individual's medical condition.

Sharona Hoffman and Andy Podgurski have systematised several forms of risk specifically in the area of biomedical data and databases, where medical records are also often found.[6] According to their systematisation, the first risk lies in the very fact that the data are not necessarily always correct. The second risk is bias, that is, misinterpretation and distortion of results based on both the nature of the information and the biases of the scientists mining the data. The third risk is the deliberate misinterpretation of the data by some individuals, for example from the fields of politics or economics, who can seemingly scientifically yet deliberately formulate wrong research results and conclusions and manipulate public opinion accordingly.

However, from the perspective of data archiving and archives, the greatest risk is unauthorised access to medical records or other records related to the health status of citizens and the misuse of such data. This risk can also take several forms. In 2013, the German weekly, *Die Zeit*, revealed that German doctors and pharmacists were massively abusing patients' personal data by reselling it without the patients' knowledge for market research purposes for the pharmaceutical industry.[7] Yet, the most

[6] Hoffman, S., Podgurski, A. (2013). The use and misuse of biomedical data: is bigger really better? *American Journal of Law & Medicine*, 39(4), 497–538.

[7] Kunze, A. (2013, 31 October). Behandelt und verkauft. Ärzte und Apotheker geben die Kranken- und Rezeptdaten von Millionen Patienten weiter – ohne deren Wissen. Es ist ein dickes Geschäft. *Die Zeit*. https://www.zeit.de/2013/45/patientendaten-marktforschung-pharmaindustrie

common risk in recent years has been hacker attacks consisting in data theft, or blocking access to them followed by blackmail (ransomware), threatening not to return the access or to publish the stolen data. In recent years, data breaches for illegal financial gain have been on the rise. According to some reports, the number is now nearly 90%[8] and the increase in health data breaches in the decade between 2009 and 2019 in the USA is estimated to be as high as 2733%, with an average of at least 500 records being compromised every day.[9] Moreover, some figures suggest a trend of increasing financial costs associated with a single healthcare data breach. An IBM Security study identified a 10% increase in costs between the years 2019 and 2020.[10]

Worldwide, hospitals and medical facilities with their medical records and patient data have become one of the main hacker targets in recent years (perhaps even the most attractive target ever). This is confirmed by reports that provide statistical surveys of data breaches and misuse. Verizon Communications, one of the largest telecommunications companies in the world, has listed healthcare as the most common target of hacker attacks in its annual data breach reports in recent years.[11] In 2019, the company recorded 798 incidents as part of their investigations of data provided by their customers (not nearly the total number of incidents), and of those, 521 were confirmed data leaks.[12] These attacks most often take the form of ransomware, that is, extortion software.

Although it is virtually impossible to determine the exact number of people worldwide who have been affected by leaks of personal data from medical records, some studies have attempted to at least bring an estimate. Data based on security incident reports primarily coming from the USA and collected by the Privacy Rights Clearinghouse, a non-profit organisation based in the USA are of great interest. The resulting statistics based on these data speak of nearly 250 million people who were affected by data leaks between 2005 and 2019, including 157 million people in the period

[8] *2020 Data Breach Investigations Report.* (2020). Verizon. https://enterprise.verizon.com/resources/reports/2020/2020-data-breach-investigations-report.pdf, p. 7.

[9] Robinson, J. (2020, 9 September). US Healthcare Data Breach Statistics. Privacy Affairs. https://www.privacyaffairs.com/healthcare-data-breach-statistics/

[10] IBM Security, *Cost of a Data Breach Report 2020*, p. 14.

[11] *2018 Data Breach Investigations Report.* (2018). 11th edition. Verizon. https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf, p. 25. *2020 Data Breach Investigations Report.* (2020). Verizon, p. 40.

[12] *2020 Data Breach Investigations Report.* (2020). Verizon, pp. 40, 54–56.

2015–2019 alone.[13] The statistics for the period 2005–2019 conclude that the absolute majority of attacks and leaks are aimed at the healthcare sector, with 61.55%, that is 3912 cases of confirmed data leaks. There is a recent trend that is even more indicative. Over the five-year period 2015–2019 within the same statistical data set, the percentage of healthcare attacks and leaks rose to 76.59% of the total volume of attacks/leaks. According to other surveys, as of February 2017, a total of 26% of Americans were affected by medical data theft.[14]

One specific feature of healthcare data leaks and thefts is that each incident typically represents a leak concerning an extremely high number of people, often in the millions. These data breaches and leaks include, among many other cases, the Excellus BlueCross BlueShield breach of September 2015 (medical data leak of more than 10 million people), the Premera Blue Cross breach of January 2015 (medical data leak of more than 11 million people), and the Anthem Blue Cross case of January 2015, arguably the largest in history to date, when highly sensitive data on nearly 79 million patients were leaked; the data included names, home addresses, dates of birth, and social security numbers.[15] Of course, the financial, operational, and other impacts on the medical establishments resulting from the attacks on personal data managed by them are enormous and pose a very serious risk.

Naturally, the risks of data breaches are not solely limited to medical establishments. This segment in the text serves only as an illustrative example of why the management of already archived data should in the future also seriously consider the risks of a breach of the data maintained in archives, including all the potential consequences, both in terms of misuse of sensitive personal data resulting in breaches of privacy, personality

[13] Based on data from the Data Breaches database compiled by the Privacy Rights Clearinghouse, statistical summaries were conducted by Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R., Khan, R. A. (2020). Healthcare Data Breaches: Insights and Implications. *Healthcare* (Basel), 133 June 8(2). https://www.mdpi.com/2227-9032/8/2/133

[14] One in Four US Consumers Have Had Their Healthcare Data Breached, Accenture Survey Reveals (2017, 20 February). *Accenture*. https://newsroom.accenture.com/subjects/technology/one-in-four-us-consumers-have-had-their-healthcare-data-breached-accenture-survey-reveals.htm

[15] Descriptions of these and other cases of massive medical data breaches in the USA are summarised in, for example, Lord, N. (2020, 28 September). Top 10 Biggest Healthcare Data Breaches of All Time. *Digital Guardian*. https://digitalguardian.com/blog/top-10-biggest-healthcare-data-breaches-all-time

rights and, ultimately, potential financial and property damage to citizens, as well as the financial risks for archives as the administrators of these data. Data administrators can also be sanctioned for data leaks if it is proven that they have neglected to take sufficient care to keep data, particularly personal data, secure. At the European level, the form of the sanctions is determined by the General Data Protection Regulation (GDPR).[16] Naturally, there are risks of litigation and civil lawsuits by the affected individuals.

Above, I have considered medical records only in the context of the security risks of digital data leaks. But that is far from the only risk. Medical records are among a group of records and archives that carry highly sensitive information about individuals, and represent a typical case in which data protection continues long after a person has died. This is when the so-called post-mortem personality and privacy protection comes into play; this protection is analysed in detail in Chaps. 2, 3 and 4 of this book. The disclosure of the psychiatric history of the famous actor, Klaus Kinsky, was a prime example. Although the file was made available by the Landesarchiv Berlin a long 58 years after its creation, and 17 years after the actor's death, the survivors sued for violation to privacy under the German Criminal Code,[17] and even though the commission of a crime was not established, the violation of post-mortem protection of privacy was recognised and a conciliation agreement between the survivors and the Landesarchiv Berlin was concluded in court.

The question of whether to transfer medical records from healthcare institutions and doctors to archives, even if only in the form of a small illustrative sample, and whether to perform the irreversible process of anonymisation, is very pressing in international comparison and the approach of individual countries to this issue can differ greatly. On the one hand, some countries designate medical records for destruction after the administrative need expires; currently, for example, the Czech Republic as one of the EU member countries, initiated a legislative process at the end of which medical records are to be exempt from the scope of the Archives

[16] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). https://eur-lex.europa.eu/eli/reg/2016/679/oj

[17] Strafgesetzbuch, § 203 (Verletzung von Privatgeheimnissen).

Act and from the obligations of records management.[18] Medical records would thus not be subject to the obligation to preserve records and to archival selection, as imposed by the Czech Archives Act. This would lead to the not unlikely scenario that this obligation would in the future be removed from medical records by other legal regulations coordinating the management and preservation of medical records.[19]

On the other hand, there are countries that have recently began including medical records in long-term or permanent archiving programmes, including digital archiving. On the European continent, Norway is the most recent representative of this approach. In 2010, the Norwegian Health Archives project was launched as one part of the National Archives Services of Norway.[20] Its aim is to permanently archive patients' medical records in digital form, additionally digitising the hardcopies of such records and making health data available for research and to surviving relatives. The global goal is then to use the data to "understand national health".[21]

Currently, the European Commission is developing an eHealth project to provide European citizens with secure access to digital health services.[22]

[18] Návrh zákona, kterým se mění některé zákony v souvislosti s přijetím zákona o elektronizaci zdravotnictví. Vládou schváleno jako Usnesení Vlády České republiky ze dne 15. února 2021 čj. 102/21 k návrhu zákona, kterým se mění některé zákony v souvislosti s přijetím zákona o elektronizaci zdravotnictví. Sněmovní tisk 1164/0, Vládní návrh zákona, kterým se mění některé zákony v souvislosti s přijetím zákona o elektronizaci zdravotnictví [Bill amending certain acts in connection with the adoption of the Act on Electronic Healthcare. Approved by the Government as Resolution of the Government of the Czech Republic of 15 February 2021 No. 102/21 on the bill amending certain acts in connection with the adoption of the Act on Electronic Healthcare. Parliamentary Print 1164/0, Government Bill amending certain acts in connection with the adoption of the Act on Electronic Healthcare].

[19] Zákon č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách), ve znění pozdějších předpisů [Act No. 372/2011 Coll., on Health Services and Conditions of their Provision (Act on Health Services), as amended]; Vyhláška č. 98/2012 Sb., o zdravotnické dokumentaci, ve znění pozdějších předpisů [Decree No. 98/2012 Coll., on Medical Documentation, as amended].

[20] Briefly on the project Ahlquist, K. R. Norwegian health archives. A new type of archive in The National Archives of Norway. https://www.nordiskarkivportal.org/wp-content/uploads/2017/10/24.05_4.3-3_Kurt-Ahlquist_Norway_Norsk-helsearkiv-en-ny-type-virksomhet-....pdf

[21] Norwegians' digital health data to be preserved for future generations (2019, 30 January). https://www.piql.com/news/norwegians-digital-health-data-to-be-preserved-for-future-generations/. The digital archive will use the Archivematica system.

[22] European Commission. Shaping Europe's digital future. eHealth. https://digital-strategy.ec.europa.eu/en/policies/ehealth

The EU then models the process of transferring electronic health records from their creators to archives on the SIP package of the aforementioned Norwegian Health Archives.[23]

It will be interesting to see how individual countries approach long-term or permanent archiving of medical records in the future. On the one hand, this may be significant for public healthcare also in the perspective of long-time intervals and long-term archiving—and the COVID-19 epidemic will probably reinforce this view. On the other hand, however, hacker attacks on medical records in particular have increased massively in recent years, targeting huge volumes of sensitive personal data. The financial costs associated with securing these data, and often paying ransoms to blackmailers, have been rising proportionately.

7.2 Census

On the one hand, the census has been an extremely important tool for state and public administration for centuries. At the same time, however, such a complex collection of data, including highly sensitive data on virtually all residents of a country compiled in a single data set, carries great risks. This tension is then palpable for all public administrations, including archives. Should census records be permanently archived? And if so, should the records be archived with "full data" or should they undergo anonymisation? Is there any risk of misuse and does history provide examples of such?

In 2009 in France, census archives were opened under general derogation up to and including the 1974 census. That means that the census was opened very young in the context of current practice in international comparison, with a time gap of only 35 years. However, access to these archives was limited to the purpose of consultation solely for the purposes of public statistics and scientific or historical research (echoing thus the same exemptions that appear in the European GDPR in relation to specific regimes for the processing of personal data), and not for the purpose of "data reuse" ("réutilisation des données"), in particular that with commercial

[23] *Guideline for the E-ARK Content Information Type Specification for eHealth1 (CITS eHealth1)*. (2021, 1 February). https://dilcis.eu/images/2020review/18_Draft_Guideline_CITS_eHealth1.pdf

motivations.[24] If this general derogation were not approved, a period of 75 years would apply, that is, as of 2020 the 1936 census would be the "youngest" accessible (in the twentieth century, censuses in France took place in 1901, 1906, 1911, 1921, 1926, 1931, 1936, 1946, 1954, 1962, 1968, 1975, 1982, 1990, 1999).

The purpose limitation was not the only level on which the protection of those in the census was implemented. Another one was the restriction of access on the census of 1946, 1954, 1962, 1968, 1975 (that were subject to the general derogation) to individual consultation only in the archives research rooms, and not remotely via the web. But is this sufficient protection? As shown above, even an individual consultation does not entirely exclude the possibility of using the researcher's own reproduction devices. Even though the law prohibits the "reuse" of census archives, is that sufficient to prevent the risks of their misuse?

7.2.1 Misuse of Personal Census Data in the USA

Recognition of the risk of misuse of personal data collected in a census goes back deep into history. The USA has been aware of this danger since the very first formalised census in 1790.[25] Decades later, it turned out that these fears were not in vain. During the American Civil War (1861–1865), census data were used in a de facto intelligence way by a Northern Union general and later by the commander-in-chief of American troops, William T. Sherman.

As the American historian Susan Schulten details, Sherman approached Joseph Kennedy, the superintendent of the census, to see if he could create a map that would not just cover landscape features, but would include a range of data on the population, food sources, and so on based on information collected in the 1860 census.[26] Since the time to create such a map was very short, Kennedy used what was available and added the requested data on the existing maps of the states of Georgia and Alabama. This

[24] Arrêté du 4 décembre 2009 portant dérogation générale pour la consultation des listes nominatives du recensement général de la population. JORF n°0288 du 12 décembre 2009 page 21505 texte n° 48.

[25] Mayer, T. S. (2002). *Privacy and Confidentiality Research and the US Census Bureau. Recommendations Based on a Review of the Literature*. Research Report Series (Survey Methodology #2002–01). https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.8.3379&rep=rep1&type=pdf, p. 4.

[26] Schulten, S. (2014, 20 November). Sherman's Maps. *The New York Times*.

resulted in extremely remarkable maps created not long after 1862. They contain data not only on the composition of the population, the number of conscripts (then 18–45 years old), the number of slaves, but also on the cultivated areas, the harvest volumes of grain, hay, rice, corn, tobacco, and cotton, as well as information on the number of horses, pigs, or cattle.

The data Sherman and his troops gathered were subsequently used during his famous 1864 campaign against part of the Confederate States armies, which became known as the "March to the Sea". It is well known that Sherman followed a "scorched earth" policy; he himself referred to these debilitating tactics, as "hard war". He destroyed not only the territory and economy of Georgia in particular, but also the morale of the inhabitants as a result. Of course, he also used the data for logistical purposes, such as when his armies had to break away from the standard supply lines and use local resources in order to march through the territory as quickly as possible. Sherman's well-known tactics would never have been so effective had it not used the comprehensive data collected in the census. Given the dire impact on the lives of the residents of the areas through which Sherman's troops marched, serious questions can be asked as to whether it was a simple use of census information and data, or a difficult-to-define and unwritten boundary was crossed and the data were misused.

Although to this day there is no consensus among the experts and authorities involved on this matter, it is very likely that data from other US censuses, this time the ones conducted in 1930 and 1940, were misused to some extent during the unconstitutional internment of some Americans of Japanese ancestry on US soil during World War II.[27] As of this day, it is still unclear whether a spectacular data breach happened even before the

[27] For most detail cf. Anderson, M., Seltzer, W. (2007). Census Confidentiality under the Second War Powers Act (1942–1947). Paper prepared for presentation at the session on "Confidentiality, Privacy, and Ethical Issues in Demographic Data". Population Association of America Annual Meeting, 29–31 March 2007, New York, NY. More detailed links to further literature. Most recently Anderson, M. (2015). Public Management of Big Data: Historical Lessons from the 1940s. *Federal History*, 15, 17–34. Cf. also the printed edition Anderson, M. (2015). *The American Census. A Social History*. Yale University Press. See also Anderson, M., Seltzer, W. (2000). After Pearl Harbor. The proper role of population data systems in time of war. Material prepared for the meeting, entitled "Human Rights, Population Statistics, and Demography: Threats and Opportunities" and organised by the Population Association of America, 23–25 March 2000, Los Angeles. Cf. also Anderson, M., Seltzer, W. (2009). Federal Statistical Confidentiality and Business Data: Twentieth Century Challenges and Continuing Issues. *The Journal of Privacy and Confidentiality*, 1(1), 7–52. https://doi.org/10.29012/jpc.v1i1.563, p. 18.

Japanese attack on Pearl Harbor and the USA entry into World War II; it is only certain, that as early as 1939, there was pressure especially from the FBI and military intelligence.[28] However, the director of the United States Census Bureau at that time, William Lane Austin (1871–1949), prevented the security and intelligence services from getting to information about individuals from the census records. After he was forced to retire in 1941, his successor James Clyde Capt (1888–1949) was much more open to handing over census data to the security and military services. Then, a few years ago, American historian Margo Anderson and statistician William Seltzer, long-time researchers in this subject, proved that the United States Census Bureau provided other institutions (intelligence agencies, the FBI, and military authorities) not only with general information about the population density of a significant number of Japanese Americans in the USA, but also with microdata, that is, names and other data on specific identified individuals, at least for those living in the Washington D.C. area.[29] Needless to say, this entails a fundamental violation of civil rights and the principle of the protection of personal data collected in a census.

7.2.2 Totalitarian Regimes and Personal Data: Misuse of Personal Census Data in Nazi Germany

One of the most massive (based on the available documented data; it can be assumed, without the possibility to verify the assumption from public sources, that totalitarian regimes, including countries with populations of many hundreds of millions of people, routinely misuse census data also for the purposes of mass persecution of individuals and entire ethnic groups) and extreme cases of census data misuse occurred in Nazi Germany. The Nazi regime needed to obtain as much information on its population as possible, a typical feature of any dictatorship. Special attention was of

[28] Anderson, M., Seltzer, W. (2007). Census Confidentiality under the Second War Powers Act (1942–1947), p. 5. Claims that the Census Bureau was instructed to collect personal data on Japanese Americans of US origin or foreign-born by President Franklin D. Roosevelt prior to the Japanese attack on Pearl Harbor, are made by Daniel J. Solove and Paul M. Schwartz, but without any evidence. Cf. Solove, D. J., Schwartz, P. M. (2018). *Information Privacy Law*. Wolters Kluwer, p. 733.

[29] Anderson, M., Seltzer, W. (2007). Census Confidentiality under the Second War Powers Act (1942–1947). This text also reprints a sample of lists of citizens of Japanese ancestry in the Washington area that were turned over to the Secret Service by the US Census Bureau (pp. 67–68). Cf. also Anderson, M. (2015). Public Management of Big Data, pp. 31–32.

course paid to those of Jewish origin. Religion was a common information provided in censuses. However, it was more of an expression of religious affiliation. This was still true for the census carried out in Germany on 16 June 1933,[30] soon after the Nazis took power, after it had been postponed several times from the originally planned date of 1930 due to the very poor economic condition of the municipalities, states, and the whole country as a consequence of the outbreak of The Great Depression.[31]

Six years later, however, the optics changed radically. The Nazi census of 17 May 1939—postponed from the one originally planned for 1938 so that it could also include Austria, which had in the meantime been annexed into the German Reich—focused primarily on racial affiliation rather than religious beliefs. The census included a special questionnaire, the so-called *Ergänzungskarten* (the full title was *Ergänzungskarte für Angaben über Abstammung und Vorbildung*), supplementary cards on origin and education. On the back of the form, among the compulsory items, was the question whether the grandparents of the respective household member were Jewish ("Volljude") according to their race affiliation ("der Rasse nach") or not. These *Ergänzungskarten* were then to be handed in separately from the remaining census records in a sealed envelope, a measure which was intended to increase the citizens' trust in the confidentiality with which the data would be treated.

The extent to which the data contained on these *Ergänzungskarten* were actually used in the process of exterminating the Jews is still widely debated in Germany and Austria.[32] In her recent research, Jutta Wietog tried to show that the data from the 1939 census and these *Ergänzungskarten* were very probably not directly used to prepare deportations and create the Jews register, the *Judenkartei*.[33] Yet, Götz Aly and Karl Heinz Roth were inclined to the opposite conclusion as early as the 1980s.[34] On the

[30] The results of the 1933 census for the citizens of Jewish origin were published at the time as: *Die Bevölkerung des Deutschen Reichs nach den Ergebnissen der Volkszählung 1933. Heft 5: Die Glaubensjuden im Deutschen Reich.* (1936). Verlag für Sozialpolitik, Wirtschaft und Statistik.

[31] Cf. Volkszählungen in Berlin seit Bestehen des Statistischen Amtes der Stadt Berlin. (2012). *Zeitschrift für amtliche Statistik Berlin Brandenburg*, 1+2, 36–57, p. 42.

[32] Cf. Wietog, J. (2001). *Volkszählungen unter dem Nationalsozialismus.* Duncker und Humblot, p. 166ff. Cf. also Aly, G., Roth, K. H. (2000). *Die Restlose Erfassung. Volkszählen, Identifizieren, Aussondern im Nationalsozialismus.* Fischer E-Books.

[33] J. Wietog, J. (2001). *Volkszählungen unter dem Nationalsozialismus*, p. 193.

[34] Aly, G., Roth, K. H. (2000). *Die Restlose Erfassung. Volkszählen, Identifizieren, Aussondern im Nationalsozialismus.* Fischer E-Books, pp. 93–95.

other hand, however, it has been indisputably proven that the *Ergänzungskarten*, after their statistical evaluation by the Reich Statistical Office (Statistisches Reichsamt), were handed over first to the statistical offices of the Länder and the police reporting offices, and then in August 1942 to the Reich Kinship Office (Reichssippenamt).[35] The data they contained were compared with the existing data kept on individual citizens on the so-called *Volkskarteien* maintained in the basic register at the local police districts.[36] In conclusion, the data from the 1939 census were used at least in a complementary manner by the Nazi administration for the purpose of exterminating citizens of Jewish origin.[37]

Both the 1933 and 1939 censuses in Nazi Germany violated the most fundamental principles on which statistical surveys need to be based—and this is especially true for the census; it is the respect for the protection of the data collected in the course of the survey, discretion in handling the data, and the complete elimination of any future misuse of these data for non-statistical purposes. As late as 1933, the otherwise very brief Census Act issued after the Nazis had taken power, explicitly prohibited—as was the tradition up to that time—the use of personality data obtained in the census for other than statistical purposes.[38] At the same time, however, it was stipulated that the material resulting from the census could only be destroyed with the consent of the Reich Statistical Office, as it can be

[35] Zimmermann, N. M. Die Ergänzungskarten für Angaben über Abstammung und Vorbildung der Volkszählung vom 17. Mai 1939. Vortrag auf dem Workshop "Datenbanken zu Opfern der nationalsozialistischen Gewaltherrschaft in Deutschland 1933–1945". https://www.bundesarchiv.de/DE/Content/Publikationen/Aufsaetze/aufsatz-zimmermann-ergaenzungskarten.pdf?__blob=publicationFile, p. 1.

[36] Wietog, J. (2001). Volkszählungen unter dem Nationalsozialismus, p. 161. So-called Volkskarteien were introduced by a decree of the Reich Minister of the Interior in April 1941, it was the Verordnung über die Errichtung einer Volkskartei of 21 April 1939. Reichsgesetzblatt 1939, Teil I, Nr. 78, Berlin 1939, p. 823.

[37] Cf., for example, *200 Jahre amtliche Statistik in Bayern 1808 bis 2008.* (2008). Bayerisches Landesamt für Statistik und Datenverarbeitung, p. 39. The situation in Austria was mapped by Exner, G. (2002). Die Volkszählung von 1939 in Deutschland und Österreich – ein Beitrag zum Holocaust? *Austrian Journal of Statistics*, 31(4), 249–256.

[38] "Jedes Eindringen in die Vermögens- und Einkommensverhältnisse ist ausgeschlossen. Über die bei der Zählung über die Persönlichkeit des Einzelnen sowie über die Verhältnisse der einzelnen Grundstücke und Vertriebe gewonnenen Nachrichten ist das Amtsgeheimnis zu wahren; sie dürfen nur zu statistischen Arbeiten, nicht zu anderen Zwecken benutzt werden." Gesetz über die Durchführung einer Volks-, Berufs- und Betriebszählung of 12 April 1933, § 4.

assumed that they already anticipated the use of the data for purposes beyond mere statistics.[39]

Only four years later, in 1937, the Nazis had blatantly deleted the provision declaring the protection of official secrecy from the Census Act, which had until then guaranteed the de jure inviolability of personal data obtained in the census and expressly prohibited their use for other than statistical purposes.[40] Strictly speaking, the fact that the data obtained from the 1939 census were subsequently used mainly to obtain information on citizens of Jewish origin as part of Nazi policy did not violate the legislation that was in force at the time. In the same breath, however, it needs to be added that German legislation at the time was already fully in service of the machinery of an absolutely monstrous regime that stood against everything human.

Another example worthy of our attention also comes from the time of the Nazi dictatorship, this time from the occupied Netherlands. The fact that population registers or census data represent extremely risky information in certain circumstances was understood by the Dutch resistance soon after the German invasion. The population register data were misused by the Nazi occupying power for various purposes. One of those purposes was the identification of those suitable for forced labour in Germany and another was the better identification of residents of Jewish origin with the aim of carrying out their systematic extermination. In the Netherlands, the Nazi occupying power made it compulsory for every citizen over the age of 15 to carry a personal identification card ("persoonsbewijs"), marked with a capital "J" for those of Jewish origin. One of the tools of Dutch resistance against the Nazi occupation was thus a highly diverse system of expertly faking identification cards.[41]

In addition to forging identity cards, however, the Dutch resistance also sought to destroy some population registers, an effort shared among various resistance groups. Still, these were rather low-impact events, with one exception. On 27 March 1943, Willem Arondeus and his associates attacked the Amsterdam civil registry office located at 36–38 Plantage

[39] *200 Jahre amtliche Statistik in Bayern 1808 bis 2008*. (2008), p. 37.

[40] Gesetz über die Durchführung einer Volks-, Berufs- und Betriebszählung of 4 October 1937. The relevant § 4 that in 1933 still provided for the protection of official secrets, was reduced by this provision.

[41] Schlebaum, P. (2019, 1 September). Raid on the Population Registry of Amsterdam. https://www.tracesofwar.com/articles/5329/Raid-on-the-Population-Registry-of-Amsterdam.htm

Kerklaan.[42] The result of the bombing, however, was not as significant as the resistance had hoped for. The fire did not have such a devastating impact, among other things, due to the fact that the identity cards were kept in catalogue cabinets and the fire did not cause any significant damage. Some of the files were then damaged by water. Nevertheless, the estimations are that the fire managed to destroy tens of thousands of identification cards (the Yad Vashem memorial claims the number of completely burned cards reached a total of 800,000, which is probably a slight overstatement). Soon after the attack, the civil registry office was largely restored, except for the approximately completely destroyed 15% of records stored in the Amsterdam population register.[43] It might seem so but this is not a marginal figure. Most of those who helped develop the plan of attack were eventually arrested, 12 resistance fighters were executed, others sent to concentration camps.[44]

One might argue that the provided examples taken from both democratic and totalitarian regimes, primarily relate to the management of records before they were stored in archives. However, these examples prove that personal census data can be misused, sometimes many decades later. In this context, the experience of countries that underwent a totalitarian period, often imposed from the outside, leads to legitimate concerns that one cannot rely on the fact that society currently exists within a democratic legal order with a very sophisticated system that guarantees the protection of personal data, such as the European Union. This order may not last forever and it is therefore impossible to accurately predict the form of future personal data management and the risk of its potential future

[42] The attack is described in detail in *Het Koninkrijk der Nederlanden in de Tweede Wereldoorlog*. (1969). Deel 6. Tweede helft Juli '42 - mei '43. Rijksinstituut voor oorlogsdocumentatie, 712–736, p. 733.

Ketelaar, E. (2005). Records and Societal Power. In S. McKemmish, M. Piggott, B. Reed, F. Upward (Eds.), *Archives: Recordkeeping in Society* (277–298). Centre for Information Studies, Charles Sturt University, p. 286. Cf. also Schlebaum, P. (2019, 1 September). Raid on the Population Registry of Amsterdam.

[43] *Het Koninkrijk der Nederlanden in de Tweede Wereldoorlog*, pp. 734–735. Data from the Yad Washem memorial, including a detailed description of the bombing of the office building, see The Righteous Among the Nations Database, Willem Arondeus (Johannes Arondeus), 1894–1943. https://righteous.yadvashem.org/?searchType=righteous_only&language=en&itemId=4043044&ind=NaN

[44] *Het Koninkrijk der Nederlanden in de Tweede Wereldoorlog*, p. 733.

misuse. And as Christian Keitel succinctly puts it: "Every totalitarianism loves personal data".[45]

It is for this reason that some countries—no wonder that they include countries that experienced a period of totalitarianism in the twentieth century—protect their citizens by anonymising certain census data or completely removing the link to a specific person from them. The Czech Republic is a prime example; the country experienced a period of Nazi oppression followed by long communist rule. Intense debates arose after the 2011 census, when the authorities themselves could not agree on whether to preserve or destroy the census records filled with personal data. The Czech National Archives asked for complete preservation, while the Czech Statistical Office and the Office for Personal Data Protection sought for the materials containing the data of each citizen to be destroyed, or at least completely anonymised, before being transferred to the National Archives. In the end, the records were archived, but only after complete anonymisation that also included the names of the census subjects.

7.2.3 Germany: "Census Ruling" and the Principle of Timely Anonymisation of Personal Data

Germany, a country with rich experience of totalitarian regimes, also struggles with a continuing concern about the possible misuse of personal data collected in the census. Already in the early 1980s, the West German Federal Constitutional Court commented on the question of whether and in what form data obtained in a census could be maintained. It warned of the risks of misuse and explicitly declared in a judgement known as the 1983 "Judgment on the Census" ("Volkszählungsurteil") that it was necessary to ensure that, during the collection and subsequent storage of data, sufficient rules were in place that allow data redaction and their subsequent "deanonymisation" (in particular names of persons, addresses, numbers of census officers), that is, the possibility to re-assign the data to specific individuals.[46]

[45] Keitel, Ch. (2019). Archivcamp "Volkszählung 2021 und Rolle der digitalen Archive". In *23. Tagung des Arbeitskreises Archivierung von Unterlagen aus digitalen Systemen*. National Archives (Prague). https://www.nacr.cz/wp-content/uploads/2019/12/KnihaAUDS_e-kniha_DEF.pdf, p. 167.

[46] Urteil des Ersten Senats vom 15. Dezember 1983 auf die mündliche Verhandlung vom 18. und 19. Oktober 1983. BVerfGE 65, 1, 49

Applied to the specific case of the 1987 census in West Germany,[47] the census questionnaire consisted of two parts: The first part consisted of individual data, the so-called Einzelangaben, data subject to statistical evaluation and not related to a specific individual or household. The second part consisted of auxiliary characteristics, the so-called Hilfsmerkmale containing data on the household or the person completing the questionnaire. These "Hilfsmerkmale" had to be separated from the "Einzelangaben" part and destroyed as soon as possible.

In the abovementioned decision restricting the handling and storage of personal data, the Federal Constitutional Court defined a new fundamental right to informational self-determination, which is derived from the German Constitution and the right to the free development of personality it guarantees. This also foreshadowed the future practice in the implementation of statistical surveys, which had to comply, inter alia, with the principle of timely anonymisation of personal data ("Gebot der frühzeitigen Anonymisierung"), the purpose of which, according to the decision of the Constitutional Court, is not only to protect the right to informational self-determination, but is constitutive for statistics itself.[48] Subsequent interpretations derived from this judgement point out that data erasure takes precedence over the obligation to offer the records for archiving in public archives.[49] Over time, the German Federal Court further strengthened the protection of the private sphere and corrected the legislator in this respect. In 2008, it formulated a new fundamental right to guarantee the confidentiality and integrity of information technology systems, which was

[47] Not only on population censuses, but on the archiving of statistical data in general, see an older but very concise article by Buchmann, W., Wettengel, M. (1996). Auslegung des Bundesstatistikgesetzes bei der Archivierung von Statistikunterlagen. *Der Archivar* 49(1), 67–74, p. 71 in particular.

[48] "ist das Prinzip der Geheimhaltung und möglichst frühzeitigen Anonymisierung der Daten nicht nur zum Schutz des Rechts auf informationelle Selbstbestimmung des Einzelnen vom Grundgesetz gefordert, sondern auch für die Statistik selbst konstitutiv." "Urteil des Ersten Senats vom 15. Dezember 1983 auf die mündliche Verhandlung vom 18. und 19. Oktober 1983. BVerfGE 65, 1, 51.

[49] Cf. Schäfer U. (1997). Die Pflicht zur Anbietung und Übergabe von Unterlagen in der archivarischen Praxis. In R. Kretzschmar (Ed.), *Historische Überlieferung aus Verwaltungsunterlagen. Zur Praxis der archivischen Bewertung in Baden-Württemberg* (pp. 35–46). Kohlhammer, p. 46 (in his citation of the judgement of the Federal Court, Schäfer made a typo; the correct version is BVerfGE 65, 1).

derived from the general right to protection of personality guaranteed by the German Constitution.[50]

Indeed, even after the 1983 Census ruling, the practice of protecting personal census data had not been established permanently and invariably. Already during the 1987 census in West Germany, critical voices pointed out that, among other things, no fixed periods were determined for the deletion of auxiliary characteristics allowing the identification of individuals, and the law was very vague on the "as soon as possible" destruction.[51] For the subsequent census, which only occurred in 2011, German law had already explicitly stipulated a maximum period of four years (after the census report had been produced) for which the auxiliary characteristics allowing the reidentification and thus the re-personalisation of data in the census records could be retained by the statistical office. The data had to be destroyed during this period, which was also the case.[52] Germany also has a separate law imposing the deletion of auxiliary characteristics allowing identification of persons as soon as possible applying to the production of federal statistics.[53]

As for the very question of archiving census records and other statistics,[54] it was only from the 1990s onwards that the German Federal Archives began to put pressure on the Federal Statistical Office to start transferring

[50] Urteil des Ersten Senats vom 27. Februar 2008–1 BvR 370/07–1 BvR 595/07, BVerfGE 120, 274–350.

[51] Gesetz über eine Volks-, Berufs-, Gebäude-, Wohnungs- und Arbeitsstättenzählung (Volkszählungsgesetz 1987) vom 08.11.1985, § 15. The above criticism came, for example, from Rottmann, V. S. (1987). Volkszählung 1987 – wieder verfassungswidrig? *Kritische Justiz*, 20(1), 77–87, p. 82–83.

[52] Gesetz über den registergestützten Zensus im Jahre 2011 vom 8. Juli 2009 (BGBl. I S. 1781), § 19. For information on the deletion of auxiliary characteristics, see Bundesbeauftragte für den Datenschutz und die Informationsfreiheit. Volkszählung 2011. https://www.bfdi.bund.de/DE/Datenschutz/Themen/Melderecht_Statistiken/VolkszaehlungArtikel/Volkszaehlung.html

[53] Bundesstatistikgesetz in der Fassung der Bekanntmachung vom 20. Oktober 2016 (BGBl. I S. 2394), § 12.

[54] For a comprehensive discussion of the archiving of statistics in German archives, see the reports of several working groups; mainly: KLA-Arbeitsgruppe. (June 2016). Bewertung von Statistikunterlagen. Abschlussbericht. https://www.bundesarchiv.de/DE/Content/Downloads/KLA/abschlussbericht-bewertung-statistikunterlagen.pdf?__blob=publicationFile; ARK-Arbeitsgruppe. (Mai 2008). Bewertung von Statistikunterlagen. Abschlussbericht. https://www.bundesarchiv.de/DE/Content/Downloads/KLA/abschlussbericht-statistikunterlagen.pdf?__blob=publicationFile

statistical material to the archives for archiving.[55] Not only the federal but also some of the regional statistical offices were initially reluctant to hand over statistical materials to the archives, including those subject to confidentiality rules. The tension between the Federal Statistics Act and the Archives Act was alleviated by the general principle applied in Germany stating that in the event of a conflict between two legislative regulations of equal weight, the younger, that is, later enacted piece takes precedence, which in this case was the Archives Act.[56] The dispute over the transfer of statistical materials to the Federal Archives was finally resolved by a decree of the Federal Ministry of the Interior in 1994, by which the Ministry confirmed the obligation to offer statistical material to the archives for permanent archiving.[57] The fact that the archives would not get the auxiliary characteristics allowing the identification of persons included in the statistical survey as these had already been redacted or deleted by the statistical office, naturally remained unchanged. This also applies to censuses, which are thus transferred to the German archives in a form that does not allow the identification of specific persons.[58] The development of this issue in Germany in the 1990s has been concisely described by Wolf Buchmann and Michael Wettengel.[59]

The sensitive nature of census personal data management persists in Germany to this day. The census originally planned for 2021 and postponed to 2022 due to the COVID-19 pandemic is a matter of lively debate, especially the issue of transferring and storing non-anonymised data collected in the ongoing pilot testing. The 2022 census is a combination of obtaining data from public administration registers, cleaning them,

[55] Keitel, Ch. (2019). Statistik im Archiv – Eine schwierige Beziehung. In *23. Tagung des Arbeitskreises Archivierung von Unterlagen aus digitalen Systemen* (pp. 169–176). National Archives (Prag), p. 175.

[56] For a comprehensive overview see Buchmann, W., Wettengel, M. (1996). Auslegung des Bundesstatistikgesetzes bei der Archivierung von Statistikunterlagen, p. 70.

[57] Bundesministerium des Innern, Erlaß vom 3. August 1994 – O II 3–142,002/16. Cf. Buchmann, W., Wettengel, M. (1996). Auslegung des Bundesstatistikgesetzes bei der Archivierung von Statistikunterlagen, p. 70.

[58] Šimůnková, K., Šisler, M. (2019). Zur Problematik der elektronischen Archivierung von Volkszählungen 2011 und 2021 in der Tschechischen Republik. In *23. Tagung des Arbeitskreises Archivierung von Unterlagen aus digitalen Systemen* (pp. 177–183). National Archives. Prague 2019. https://www.nacr.cz/wp-content/uploads/2019/12/KnihaAUDS_e-kniha_DEF.pdf

[59] Buchmann, W., Wettengel, M. (1996). Auslegung des Bundesstatistikgesetzes bei der Archivierung von Statistikunterlagen.

and finally supplementing them with a representative sample of a selected part of the population in the traditional form of basic household interviews. As part of the testing, non-anonymised data from the residence permits of all residents were transferred to the Federal Statistical Office, a step that was challenged before the German Federal Constitutional Court by the Gesellschaft für Freiheitsrechte. However, the Federal Constitutional Court denied the request to reject such a procedure in 2019.[60]

The development of German society's attitude to the preservation of data from statistical surveys is a crystalline example of how the experience of the horrific consequences of totalitarian regimes significantly increases the sensitivity and need for the protection of human rights even in an advanced democracy.

7.2.4 Time Capsule Versus Archiving: Census Time Capsules in Australia and Ireland

Finally, I will mention the specific approach Australia and Ireland have implemented in handling census data; the use of the time capsule.

In the last two decades Australia has represented in a sense the opposite tendency to what we have witnessed in, for example, Germany or the Czech Republic. Until 2001, Australia destroyed all the identifiable personal data, starting with the very first census conducted in 1911.[61] However, in 2001, the hundredth anniversary of the Australian Federation, the country made a substantial change and came up with a new and interesting solution abandoning the previous strict policy of unambiguous privacy protection.

In 1998, the Standing Committee on Legal and Constitutional Affairs of the Australian House of Representatives produced a report entitled "Saving our census and preserving our history". The Advisory Council on Australian Archives, as an advisory body to the Minister responsible for archives, recommended the preservation of census records, including non-anonymised personal data, with the proviso of applying a 100-year closure

[60] Bundesverfassungsgericht, Beschluss vom 06.02.2019, Az.: 1 BvQ 4/19.

[61] Census and Statistics Act 1905, No. 15, 1905. Cf. Iacovino, L., Todd, M. (2007). The long-term preservation of identifiable personal data: a comparative archival perspective on privacy regulatory models in the European Union, Australia, Canada, and the USA. *Archival Science*, 7, 107–127. https://doi.org/10.1007/s10502-007-9055-5, p. 119; Australian Bureau of Statistics. (2011, 28 April). *2903.0 – How Australia Takes a Census, 2011*. https://www.abs.gov.au/ausstats/abs@.nsf/lookup/2903.0Main%20Features52011

period. At the same time, the then-chairman of the Council, Rodney Cavalier, argued that for genealogical and historical purposes, it was not necessary to preserve every single census (Australia conducts censuses in a five-year cycle), but that it would be sufficient to preserve the data every 20 or 25 years to capture a "portrait of each generation" and for future historical research.[62]

The final decision gave each citizen the opportunity to choose whether or not they wanted to keep their personal data from the census.[63] The personal census data shall be thus preserved in the National Archives of Australia only provided that the individual has given their explicit consent. The data will then be stored in a "time capsule", where they will be sealed for 99 years, during which time no one will see the data stored inside. The capsule will not be opened and access to the data will only be possible after the given period. That means that the 2001 census data will only be available in 2100. Perhaps even more remarkable is the number of the nearly 10 million, or 52.6% of the population who participated in the Australian census, and consented to their personal data being stored in a "time capsule" in the National Archives of Australia.[64] The same principle was then applied to subsequent censuses conducted in five-year intervals in 2006, 2011, 2016 and will be applied to the 2021 census as well. In 2006, over 56% of the population agreed to maintain their data in a "time capsule".[65]

[62] House of Representatives Committees. Standing Committee on Legal and Constitutional Affairs. (May 1998). *Saving our census and preserving our history*. https://www.aph.gov.au/parliamentary_business/committees/house_of_representatives_committees?url=/laca/inquiryincensus.htm, Sec. 5.7, p. 87. Commentary on this report by Smith, C. (1998). Review commentary. Saving our census and preserving our history: Report of the House of Representatives Standing Committee on Legal and Constitutional Affairs. *Archives and Manuscripts*, 26(2), 410–417.

[63] Census information Legislation Amendment Act 2000, No. 30, 2000, Sec. 8A a Sec. 19A.

[64] Mutch, S. (2001). Public Policy Revolt: Saving the 2001 Australian Census. *Archives and Manuscripts*, 30(2), 26–44, p. 41. Cf. also Australian Bureau of Statistics. (July 2006). *2902.0 - Census Update* (Newsletter). https://www.abs.gov.au/ausstats/abs@.nsf/7d12b0f6763c78caca257061001cc588/ea2223b65f7787aaca2573210017ede3!OpenDocument

[65] Australian Bureau of Statistics (2011, 4 August). Census Time Capsule – it's time!. https://www.abs.gov.au/websitedbs/censushome.nsf/home/CO-42. See also Census Time Capsule delivered to the National Archives vaults today. (2007, 13 September). Joint media release from Australian Bureau of Statistics and National Archives of Australia. https://www.abs.gov.au/AUSSTATS/abs@.nsf/mediareleasesbyReleaseDate/FE3AE1DF58707778CA257354007FC7D9?OpenDocument

The time capsule stores the census records of those who agreed to archive their data in the form of microfilm.

A quick look at Europe shows that Ireland keeps non-anonymised census records, including personal data, by default. Access to them is granted after 100 years.[66] Censuses in Ireland after its separation from the United Kingdom were conducted in 1926, 1936, 1946, 1951, 1956, 1961, 1966, 1971, 1979, 1981, 1986, 1991, 1996, 2002, and 2006.[67] The records are preserved in an astonishingly complete condition, unlike the nineteenth century Irish census forms as the censuses of 1881 and 1891 were deliberately destroyed during World War I, presumably due to lack of paper. The 1821, 1831, 1841, and 1851 census records were then, with minor exceptions, destroyed in 1922 in a fire at the Public Record Office at the outbreak of the Irish Civil War.

What is remarkable is how the data are stored. Census records dating back to 1946 and partly to 1951 are maintained in the National Archives of Ireland. Younger census forms remain in the care of the Central Statistical Office. On the one hand, the census records are non-anonymised, but on the other, access to records less than 100 years old is strictly prohibited and this ban also includes the staff of the National Archives of Ireland as well as any official consultation purposes.

The 2021 census, postponed to 2022 due to the COVID-19 pandemic, was the first time the Irish introduced the option of using a time capsule. Any citizen can write a handwritten message for future generations on the back of the census form. This message will be removed from the time capsule and revealed together with the entire census after 100 years.[68] In addition, the 2021 census contains an additional eight questions concerning renewable energy sources, internet access, smoke alarms, smoking, working from home, volunteering, childcare, and travelling home from work, school, or college.

On one side, Ireland significantly widens the range of information about a person, their existence, everyday life and privacy, and opens up space for self-expression in the form of a personal message which allows an individual to express their own personality. And as the Central Statistics

[66] Statistics Act 1993. Nr. 21 of 1993, Sec. 35.

[67] The National Archives of Ireland. History of Irish census records. http://www.census.nationalarchives.ie/help/history.html

[68] Central Statistics Office. (2019, 10 July). Press Statement Census 2021 date and questions approved by Government. Press Statement.

Office rightly pointed out, the opportunity to self-express into a time capsule adds "a fun element, you can see it as a small reward for filling in the form and making your own mark. Whatever you want can go in there."[69]

On the other side, it is somewhat of a paradox that just before the latest census planned for 2021 and postponed to a year later, a case of archived census personal data misuse has emerged. In 2020, the data from the 1926 census, which were supposed to be absolutely inaccessible until 2027, appeared on social media.[70] The records are physically maintained in the National Archives of Ireland but remain under the control of the Central Statistics Office.[71] The case ended with the Central Statistics Office contacting the person responsible for illegally publishing the data who then removed them from social media.

At the very heart of the issue of managing and archiving personal data is the fundamental tension between the need to obtain and store certain data about citizens and the gradually increasing risk of their misuse. It may seem ironic, but one way to address this tension is by public archives deviating from standard procedures of archiving in the public interest. What does this mean?

It is necessary to start by comparing the time capsule with the principles of standard archiving. Both the time capsule and archiving share the intention of long-term and secure information preservation, but there are fundamental differences. Data archiving and the archival sector intend to preserve data permanently and at the same time want to gradually allow access to the public, while applying all standard closure periods and other legal measures regulating access to the data. On the contrary, time capsules are based on maximum to absolute restriction of access to their contents. Motivations for restricted access have varied throughout history. The reasons usually included security measures protecting the creator and depositor of information whose disclosure would put them at risk. It

[69] Aodha, G. N. (2019, 10 July). For the first time, you can write a message for future generations on the Census. *The Journal.* https://www.thejournal.ie/censuscensus-2021-time-capsule-4718938-Jul2019/

[70] Murray, S. (2020, 20 October). The CSO has alerted the gardaí after extracts from the 1926 Census were published on social media. *The Journal.* https://www.thejournal.ie/cso-1926-censuscensus-5238786-Oct2020/

[71] For background information on the census in Ireland and the preservation of census records, see Central Statistics Office. Census through History. https://www.cso.ie/en/census/censusthroughhistory/; The National Archives of Ireland. History of Irish census records. http://www.census.nationalarchives.ie/help/history.html

might also have been simple preservation of information for future generations. In a sense, we might see early examples of time capsules in the preservation of documents and other artefacts in church domes or inside statues, as shown by the recent discovery of a secret box containing a document dated 1777 inside a statue of Christ called Cristo del Miserere inside the church of Santa Águeda in Sotillo de la Ribera, Spain,[72] and so on.

In the twentieth century, the time capsule began to add a second essential feature; it can be used to determine the exact period for which the information is made absolutely inaccessible and, at the same time, it can pinpoint a specific point in time when the time capsule is to be opened and its contents made available. This feature in its embryonic form was also present in the early stages of time capsules, but was tied to a specific act such as—bearing in mind the above examples—the moment of necessary repair or reconstruction. Naturally, in cases like these it was impossible to determine the exact point in time when the capsule would be opened. This began to change significantly in the twentieth century. A typical early example was a time capsule known as the "Detroit Century Box" created on 31 December 1900 and intended to be opened 100 years later, as actually happened at the end of the year 2000. The similarly famous "Crypt of Civilization" built in 1936 at Oglethorpe University intends to preserve records of period life; it is meant to be unsealed in 8113.[73] However, the inability to determine an exact moment in time when a capsule will be opened is not solely a thing of the past, just think of the examples of capsules located in space probes Pioneer 10, Pioneer 11, Voyager 1, or Voyager 2.

Nevertheless, traditional archiving and preservation of data is more similar to time capsules with a clearly defined period before they can be opened, a period that is "observable", and it is much less similar to, for example, the KEO satellite, whose departure has been postponed several times, that is intended to carry various information about humanity and civilisation in their current state for future inhabitants of the Earth and that should return to Earth in approximately 50,000 years.

[72] EFE. (28 November 2017). Encuentran una cápsula del tiempo oculta dentro del trasero de un Cristo del XVIII. *El Mundo*. https://www.elmundo.es/f5/comparte/2017/11/28/5a1d5fd7468aebc0358b4599.html

[73] Hudson, P. S. The "Archaeological Duty" Of Thornwell Jacobs: The Oglethorpe Atlanta Crypt of Civilization Time Capsule. https://crypt.oglethorpe.edu/history/detailed-history/

The principle of preserving certain information, usually for a specific, well-defined period of time, and at the same time the principle of absolutely restricting access to it until the expiration of a specified period of time, eventually became the reason that attracted archives and data archivists to the phenomenon of time capsules. At certain moments, however, the two otherwise substantially different phenomena, the time capsule on one side and archiving on the other, meet and are applied simultaneously. That is the case, for example, of the preservation of census records currently used in Australia and Ireland; based on the proposed four categories of the right to be forgotten presented in Chap. 5, under Sect. 5.3, this case would call for the application of the "temporary absolute" right to be forgotten.

This may actually be the way to balance the tension between the need to collect and store personal data on citizens and the increasing risk of misuse of these data.

Almost without exception, public archives and archiving in standard democracies base their access policies on the principle that there is a fundamental difference in access to archives for official and for private purposes. While closure periods are usually introduced for private access to archives, they do not apply by default in the case of official purposes and the records may thus be accessed immediately. The time capsule, on the other hand, works or can work quite differently, which also applies to it being used in archiving. One of the examples analysed above makes this crystal clear; it is the example of the 2011 archival census records held at the National Archives of Australia. The census records of citizens who gave consent to their non-anonymised preservation are kept in the National Archives sealed in a time capsule for 99 years, and unlike other archival records, access to them is restricted for official purposes and it is explicitly prohibited for court needs.[74] Still, as is the case in other countries, the Australian Bureau of Statistics will destroy all the original records after statistical evaluation and data extraction is performed.[75] The only preserved microfilm copies of the records of those who volunteered are archived precisely and only in the time capsule. If this is not opened, no personal data from the census should leak to the public.

[74] Census and Statistics Act 1905, No. 15, 1905, as amended and in force on 1 October 2020, Sec. 19A.

[75] Australian Bureau of Statistics. 2903.0 – How Australia Takes a Census, 2011.

The time capsule thus represents an instrument which—legally—increases the protection of personal data contained in the records stored inside. This certainly does not mean that it automatically eliminates the risk of misuse in the case that the democratic state and the rule of law get replaced by a totalitarian, lawless, strongly populist regime, and so on. The seal, honoured by a person, society, or a country just and honest, will wilfully and without hesitation be broken by injustice, malice, and oppression.

7.3 The Case of Jewish Files ("Fichiers Juifs") in France: Archiving of Materials Intended for Destruction and Their Concealed Existence

In November 1991, Nazi hunter Serge Klarsfeld, a French lawyer specialising in cases of persecution of Jews in France during the Holocaust, discovered files known as "fichiers juifs" that were believed to no longer exist as they should not have existed. No search function in the archive that maintained these records recognised their existence; the only information leading to the files was in an internal function.[76] The case caused quite a stir throughout the French archival and historical community and became one of the important drivers of change in French archives, which eventually led, years later, to a complete revision of the entire French archives legislation when the Code du patrimoine replaced the original 1979 Archives Act in 2004.[77] Vincent Duclert considers the outbreak of the case to be one of the important starting points marking the period of the so-called archive crisis ("crise des archives") of French archiving at the time and consisting essentially, according to Duclert, in the absence of a

[76] Cf. Combe, S. (1994). *Archives interdites. Les peurs françaises face à l'histoire contemporaine*. Albin Michel, p. 200. The same author presents only very brief information on the case of the Jewish files in English in Combe, S. (2013). Confiscated Histories. Access to Sensitive Government Records and Archives in France. *Zeithistorische Forschungen/Studies in Contemporary History*, 10(1), 123–130, https://zeithistorische-forschungen.de/1-2013/id=4435, p. 126. The case of the Jewish files was the topic of serious discussion in France at the time. It is the subject of Gasnault, F. (2013). L'affaire du "fichier juif", ou l'éveil d'une nouvelle sensibilité documentaire. In D. Fabre (sous la dir.), *Émotions patrimoniales* (pp. 237–258). Éditions de la Maison des sciences de l'homme, Ministère de la Culture.

[77] The development up to just before the publication of the Code du patrimoine (2004) is followed by Duclert, V. (2003). La politique actuelle des archives. In S. Laurent (sous la dir.), *Archives „secrètes", secrets d'archives. L'historien et l'archiviste face aux archives sensibles* (pp. 21–56). CNRS Éditions, p. 25ff.

scientific policy of archival institutions and therefore in the inability to respond when archival work was challenged.[78]

These files were among those created at the behest of the German Nazi occupying power on French territory, but similar ones were also created in Vichy France. Serge Klarsfeld came across some records in the fonds of the Ministère des Anciens combattants (Department of Veterans Affairs) that were at first interpreted as purely a register created by the Préfecture de police de la Région parisienne (Paris Police Prefecture).[79] Subsequently, by means of a thorough analysis, an independent committee of historians presided by René Rémond concluded that these so-called fichier juif files consist of three categories of archival records.[80] Firstly, it is a second copy of the Drancy camp register containing the names of deported persons, which was kept and hidden by prisoners detained there. Second, there are files from the Beaune-la-Rolande and Pithiviers camps, which were handed over to the Department of Veterans Affairs by the social assistants at these camps. And finally, there are files of individuals and families of diverse character, which may have included, among other things, information from the Prefecture of Police registers created in 1940, a source whose existence was presumed but that has not survived to this day. And this is the heart of the problem.

During the occupation, police prefectures created file registers of Jewish people, which became an important tool for the Holocaust in the country during World War II. Immediately after the end of the war, the then Minister of the Interior, Édouard Depreux, in a circular dated 6 December 1946, ordered the destruction of "all records based on racial distinctions between Frenchmen" ("tous les documents fondés sur des distinctions

[78] Duclert, V. (2001). Les historiens et la crise des archives. *Revue d'histoire moderne & contemporaine*, 5(48-4bis), 16–43, p. 34. The crisis of French archives was also addressed by Duclert in other texts in a broader context, including, for example, the question of the relationship between historical science and archives. Among others Duclert, V. (1999). Les historiens et les archives. Introduction à la publication du rapport de Philippe Bélaval sur les Archives nationales. *Genèses. Sciences sociales et histoire*, *36. Amateurs et professionnels*, 132–146.

[79] Kahn, A. (1993). *Le fichier*. Robert Laffont; Combe, S. (1994). *Archives interdites*, pp. 194–232.

[80] *Le "Fichier Juif". Rapport de la Commission présidée par René Rémond au Premier ministre*. (1996). Plon.

d'ordre racial entre Français").[81] The Jewish files were also subject to this regulation. In the chaotic times just after the end of the war, however, soon afterwards the same Minister Depreux, albeit in a different government, issued yet another circular dated 31 January 1947, reversing his original decision and calling for the preservation of the records as they might help the Jews affected by the Holocaust, the search for missing and displaced persons, the provision of certificates of deportation or imprisonment, the reparations, the needs of the judicial system, and so on. They were to be kept only as long as they could benefit the affected persons of Jewish origin.[82] Soon afterwards, there was a massive destruction of records and it was generally believed that these files compiled at the time of World War II were completely destroyed as well.[83]

This obligation was also later sealed at the level of legislation by the Information and Freedoms Act in 1978. This Act imposed an obligation not to preserve any data relating to the names of persons that would directly or indirectly reveal, inter alia, racial origin (as well as other data, nowadays generally referred to as sensitive personal data, such as political or philosophical beliefs, religion, or trade union affiliation).[84]

The first echoes of the Jewish files issue had already appeared in the early 1980s. In the spring of 1980, the investigative magazine, *Le Canard enchaîné*, drew attention to the fact that there was a Jewish register in one

[81] According to Poznanski, R. (1997). Le fichage des juifs de France pendant la Seconde Guerre mondiale et l'affaire du fichier des juifs. *Gazette des archives*, 177–178. *Transparence et secret. L'accès aux archives contemporaines*, 250–270, pp. 264–265. Cf. also Chabin, M.-A. (2017, 17 September). Détruire ou conserver les données sensibles… il y a 70 ans. Petit éclairage historique pour la mise en œuvre du Règlement général pour la protection des données personnelles (RGPD). https://www.marieannechabin.fr/2017/09/detruire-ou-conserver-les-donnees-sensibles-il-y-a-70-ans/

[82] "Je vous invite, en conséquence, à maintenir, le cas échéant dans vos archives, les documents relatifs aux enquêtes, sévices et arrestations dont les personnes considérées comme juives ont été victimes, lorsque ces documents peuvent présenter des avantages pour de telles personnes, par exemple en permettant la recherche et le regroupement d'individus disparus ou dispersés, ou la délivrance de certificats de déportation ou d'arrestation." According to Chabin, M.-A. (2017, 17 September). Détruire ou conserver les données sensibles… il y a 70 ans.

[83] The destruction took place at the end of 1948. See L'affaire du "fichier juif". (2020, 5 October). *France Culture*. https://www.franceculture.fr/emissions/lsd-la-serie-documentaire/politique-et-race-en-france-un-mariage-dangereux-14-episode-1-laffaire-du-fichier-juif

[84] Loi n° 78–17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés of 7 January 1978, Art. 31. In the current version it is Art. 6.

of the National Gendarmerie centres in Rosny-sous-Bois.[85] The National Commission on Informatics and Liberty (Commission nationale de l'informatique et des libertés) conducted a cross-ministerial survey at the time and concluded that there was no trace of any Jewish files anywhere, but it was equally strange that there was no evidence of their proper destruction except in the Marseille area.[86] The case was subsequently revived by the above Serge Klarsfeld who discovered parts of the files in the records maintained by the Department of Veterans Affairs.

The case of the French Jewish files provoked a great deal of controversy, especially with regard to the issue of public access to archival material; the subsequent legislative developments confirmed that society demands liberalisation of access to archival records and calls for the introduction of equal access in particular. At the time, the Jewish files were an unfortunate example of creating privileged access to records and archives only for certain individuals; they became one of the indicators of restricted access to newer records to the public. This situation was also reflected in Guy Braibant's comprehensive report to the French Prime Minister on the state of French archiving, in which he touched on, among other things, the excessively long closure periods.[87]

Yet, in view of the question this text wants to answer, the case of the Jewish files is more important regarding the topic of the preservation of data and archival records in particular. It is remarkable on several levels. First, it demonstrates how the experience of massive crimes against humanity—perpetrated not only by the German occupying power but also by the French themselves—has shown society the risks of collecting personal data. This was one of the reasons why the French Minister of the Interior, Depreux, ordered the destruction of records containing information about individuals of Jewish origins soon after the liberation of France. However, the same minister realised soon after his decision that the very same records could in turn help the Jewish victims of the Holocaust. And

[85] Cf. Combe, S. (1994). *Archives interdites*, p. 198.

[86] Combe, S. (1994). *Archives interdites*, p. 199.

[87] Braibant, G. (Ed.). (1996). *Les Archives en France: rapport au Premier ministre*. La Documentation française (Collection des rapports officiels). https://www.vie-publique.fr/sites/default/files/rapport/pdf/964093000.pdf, drafts no. 16, 18 and 19, p. 124. For a detailed discussion of closure periods, see Čtvrtník, M. (2021). Closure periods for access to public records and archives. Comparative-historical analysis. *Archival Science*, 21(4), 317–351. https://doi.org/10.1007/s10502-021-09361-4

so he decided to preserve these materials until they could be used to serve the victims.

The whole case then climaxed half a century later when Klarsfeld discovered the remains of the Jewish files and no longer called for their destruction but rather for their permanent archiving. He and the National Commission on Informatics and Liberty suggested the preservation of the original files, meanwhile transferred to the French National Archives, in what was then the Memorial of the Unknown Jewish Martyr (Mémorial du Martyr juif inconnu), now part of the Memorial of the Shoah (Mémorial de la Shoah).[88]

On the contrary, the Rémond Commission pleaded for the preservation of the records in the National Archives.[89] In the end, an original compromise was agreed upon, that had the direct support of then President Jacques Chirac. The archival records remained in the official custody of the National Archives in order to fulfil the legal requirements for the maintenance of public records in a public archive, and at the same time they were actually stored in a new depot, located next to the crypt that represents the symbolic tomb of the six million murdered Jews who do not have a grave and which is administered by the Shoah Memorial in France.[90] The Memorial has no control over the Jewish file, which falls exclusively within the purview of the National Archives.

A significant role in exposing the entire context was played by the intention of the Jewish community that wished to be able to manage material that was once used for its persecution (similarly, Indigenous peoples in Canada are now demanding that public and private organisations in Canada hand over records testifying to the cultural genocide of Indigenous peoples in Indian residential schools to the National Centre for Truth and Reconciliation, as I briefly mentioned in Chap. 4) and which, unfortunately, can never be excluded from being used for persecution in the

[88] Klarsfeld, S. (1996, 6 July). L'embarras de la commission Rémond. *Le Monde*. Serge Klarsfeld, along with some other experts, commented on the case of the Jewish files at a round table; this commentary was published as Peschanski, D. (1997). Le fichier juif. Table ronde. *La Gazette des archives*, 177–178. *Transparence et secret. L'accès aux archives contemporaines*, 241–249.

[89] *Le "Fichier Juif". Rapport de la Commission présidée par René Rémond au Premier ministre*. (1996), p. 231.

[90] Cf. Shoah Memorial website, Les espaces du musée-mémorial. http://www.memorialdelashoah.org/le-memorial/les-espaces-du-musee-memorial/la-crypte-et-le-fichier-juif.html

future. Although this intention was only partially fulfilled in the form of a compromise solution and agreement with the French state, it was in a way accepted. What is remarkable and significant is that half a century after the Holocaust, concerns about the misuse of personal data, and in this case especially data on racial origin, have diminished, and the Jewish community is no longer opposed to their preservation. It is possible that were the files of French Jews to survive in their entirety, they would have been preserved as such. This ultimately shows a process I call "disappearing sensitivity"; data sensitivity fades in proportion to their ageing or to the transformation of the character of the sensitivity. This is a process that I will mention again in the following chapter, and that is central to the whole field of post-mortem protection, which is one of the topics of the preceding chapters.

7.4 Personal Data Breaches: National Archives and Records Administration (NARA) Cases

In 2009, the US National Archives and Records Administration (NARA) discovered that an external hard drive containing a copy of data from the Bill Clinton Administration Executive Office had disappeared.[91] The hard disk was used as a part of routine copying operations of data intended for long-term archiving. It contained files with the personal information of approximately 250,000 individuals, including the names and social security numbers of, first, the employees of the Executive Office of the President of the USA at that time, and second, the individuals who either contacted, for example, as job applicants, or visited the White House complex. One of the daughters of former Vice President Al Gore was reportedly among the individuals concerned.[92] The impact of either the lost or stolen hard drive was not that the data was irretrievably lost (they were only backups), but that the protection of the said personal data had been breached and, as a consequence, it was possible for those concerned to fall victim to identity theft.

[91] National Archives and Records Administration, Fact Sheet Regarding the National Archives and Records Administration Breach of a Hard Drive Containing Personally Identifiable Information (PII). https://www.archives.gov/files/press/press-releases/2010/pdf/nara-breach-notification-faq-2010-01-12.pdf

[92] National Archives Warns Former Clinton Staff, Visitors of Major Data Breach. (2015, December 23). *Fox News*. https://www.foxnews.com/politics/national-archives-warns-former-clinton-staff-visitors-of-major-data-breach

At the time, NARA initiated a mailing list first of 26,000 letters to those individuals whose data might have been leaked, which was then followed by another 150,000 letters.[93] NARA offered those affected the option to use credit monitoring, identity theft insurance, and fraud resolution assistance free of charge for one year. In addition, NARA posted a $50,000 reward for providing information that would lead to the recovery of the missing hard drive. According to the information I have available, the disk was never found.

There was yet another case that came to the fore in connection with the US NARA. In that same year, 2009, NARA turned over a damaged hard drive containing personal information (in part presumably including sensitive personal information) of approximately 76 million veterans (including millions of social security numbers dating back to 1972) to a contractor for repair without deleting the personal information on the drive. The contractor found the disc beyond repair and handed it over to yet another company for recycling. Some of the well-known media outlets rushed to conclude that this meant one of the biggest leaks of personal data by a government agency in history.[94] NARA countered these conclusions arguing that the protection was not breached as all the contractors and subcontractors who came into contact with the incriminated hard drive were contractually bound to NARA and committed to the privacy principles regarding the data with which they came into contact.[95] At the same time, NARA pointed out that there was no evidence that the companies in question had tampered with the disc. There was even a hearing before the Subcommittee on Information Policy, Census, and National Archives of the House of Representatives Committee on Oversight and Government

[93] National Archives and Records Administration. (2010, 4 January). Statement on Notification Letters relating to PII Information from Clinton Hard Drive. Press Release. https://www.archives.gov/press/press-releases/2010/nr10-41.html?_ga=2.116140486.152971816.1604912356-605976007.1604912356

[94] Singel, R. (2009, 10 January). Probe Targets Archives' Handling of Data on 70 Million Vets. *Wired*. https://www.wired.com/2009/10/probe-targets-archives-handling-of-data-on-70-million-vets/. Forbes also came to a similar conclusion, cf. Greenberg, A. (2009, 24 November). The Year Of The Mega Data Breach. *Forbes*.

[95] See NARA Statement Regarding Defective CMRS Disk Drive. (2009, 13 October). Press Release. https://www.archives.gov/press/press-releases/2010/nr10-05.html

Reform.[96] The fact that NARA's credibility specifically on military veterans affairs had not been undermined was finally confirmed by the latest cooperative agreement with the United States Department of Veterans Affairs to digitise certain archival materials from the Veterans Benefits Administration under the jurisdiction of that Department.[97] The agreement explicitly declares that the digitised materials also contain sensitive personal information, including, but not limited to, social security numbers, especially when linked to dates of birth, birth names, and other identifiers, and that NARA is responsible for not disclosing such materials that are less than 75 years old.

7.5 Totalitarian Abuse of Totalitarianism: The East German State Security Service and Personal Data Misuse in the "Archive of National Socialism" ("NS-Archiv")

Paradoxically, there may be cases when personal data of the representatives of a totalitarian regime are misused by yet another dictatorship. After the fall of totalitarian regimes, the documentation may be used by the successor democracy to legally seek and achieve justice. A typical example is the post-war Nuremberg Trials of 1945–1946 held against the top Nazi representatives. But history has also seen other cases. For example, a similar group of materials surviving from the period of Nazi Germany began to be systematically misused by the Ministry for State Security (Stasi) in the newly constituted East Germany (DDR). This process was finally formalised in 1967 when the so-called NS-Archiv was established within the Stasi.[98]

The NS-Archiv, which is now quite well mapped, was created in no small part as a reaction to the activities of the Dokumentationsstelle zur

[96] *The National Archives' ability to safeguard the nation's electronic records. Hearing before the Subcommittee in information policy, census, and National Archives of the Committee on oversight and Government reform.* (2009). House of Representatives. 111 Congress. First Session. November 5, 2009. Serial No. 111–63.

[97] Letter of agreement between Department of Veterans Affairs: veterans benefits administration (VBA) and National Archives and Records Administration (NARA). (2019, 9 August). https://www.archives.gov/files/digitization/pdf/va-letterofagreement-final-signed.pdf

[98] For a monograph on the Archive of National Socialism cf. Unverhau, D. (Ed.). (2004). *Das „NS-Archiv" des Ministeriums für Staatssicherheit. Stationen einer Entwicklung.* Lit.

zentralen Erfassung allen Materials der NS-Zeit (1933–1945), which had been formed in 1964 as part of the Staatliche Archivverwaltung (State Archive Administration) of the East German Ministry of the Interior. In this way, the Stasi intended to maintain control and power over all files from the Nazi period. However, the origins of the NS-Archiv date back to the turn of 1953–1954, as reconstructed by the current president of the German Federal Archives, Michael Hollmann.[99] The resulting NS-Archiv was created by artificially combining materials left over from the activities of a number of offices and party apparatuses of the Third Reich. It is basically built on the principle of pertinence and in this sense stands in opposition to the principle of provenance, the fundamental constituent of modern archiving. For the most part, it consists of materials related to specific persons.[100]

The Stasi systematically collected materials maintained in the NS-Archiv in order to "fulfill so-called 'political-operational' tasks: to prosecute Nazi and war criminals or to 'move' them to cooperate, which was understood to be an offer to rectify the crimes committed".[101] The very motivation for the creation of the NS-Archiv collection was the intention to gather information about people and their Nazi burdens and not an attempt to create an archival collection based on the principle of provenance. In its NS-Archiv collection, the Stasi thus accumulated records such as ordinary personal files, court files, medical records, party membership files, and many other categories of records; these were then processed and used to compile and create "personal files" of persons of interest.[102]

As Michael Hollmann points out, a significant amount of the records have little meaning and testimonial value as such and would not be

[99] On the topic of NS-Archiv, cf. in particular Hollmann, M. (2001). Das "NS-Archiv" des Ministeriums für Staatssicherheit der DDR und seine archivische Bewältigung durch das Bundesarchiv. *Mitteilungen aus dem Bundesarchiv*, 9(3), 53–62; Dumschat, S. (2007). Archiv oder "Mülleimer"? Das "NS-Archiv" des MfS der DDR und seine Aufarbeitung im Bundesarchiv. *Archivalische Zeitschrift*, 89, 119–146. https://doi.org/10.7788/az-2007-jg05. https://www.bundesarchiv.de/DE/Content/Downloads/Aus-unserer-Arbeit/ns-archiv-des-mfs1.pdf?__blob=publicationFile (Cited from this issue).

[100] Michael Hollmann estimates the number to be as high as 95% of the total material. Hollmann, M. (2001). Das "NS-Archiv" des Ministeriums für Staatssicherheit der DDR und seine archivische Bewältigung durch das Bundesarchiv.

[101] Dumschat, S. (2007). Archiv oder "Mülleimer"?, p. 2.

[102] For information on this process, cf. Hollmann, M. (2001). Das "NS-Archiv" des Ministeriums für Staatssicherheit der DDR und seine archivische Bewältigung durch das Bundesarchiv.

archivable; what is valuable from today's point of view is the body of material in the NS-Archiv, which, Hollmann believes, could in a way be described as the "Document Center of the East" ("Document Center des Ostens").

The misuse of personal data itself not only took place in a massive way within the NS-Archiv, the NS-Archiv was directly built on the misuse of personal data. The data collected on citizens was misused by the Stasi for various purposes, in particular by obtaining compromising material by no means limited only to the citizens of the then DDR. One of their main interests was the citizens of the Federal Republic of Germany. The Main Department IX/11 (Hauptabteilung IX/11) established by the Stasi used the NS-Archiv as a tool particularly for collecting and acquiring data on the Nazi past of key figures in the West German economy, military, politics, and other public authorities.[103] In some cases, sensitive data were also used for massive political campaigns against Western democracies and their representatives, such as Kurt Georg Kiesinger, Hans Globke, Heinrich Lübke, Theodor Oberländer, and others.

The sheer volume of the NS-Archiv was extraordinary. Towards the end of its operation, it maintained approximately 1 million units.[104] The amount was estimated between 7–10 linear kilometres.[105] The NS-Archiv was also, with certain exceptions, the only one of the Stasi archives not to remain under the authority of the Federal Commissioner for the Records of the Stasi (Der Bundesbeauftragte für die Unterlagen des Staatssicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik), but was transferred to the German Federal Archives.

Although it was a special archive artificially created for the purposes of the intelligence service and secret police of the East German dictatorship and not a standard public archive, with the perspective from which we view the minimisation, preservation, and protection of data in archives, the difference does not matter in the end; the data created and preserved during the period of one totalitarianism were used and misused by the next. Although in many cases the intention was to punish the crimes of the Nazi period, this motivation evolved into the determination to use the materials as compromising data on people and their behaviour during the

[103] S. Dumschat, Archiv oder "Mülleimer"?, pp. 2–3.

[104] Hollmann, M. (2001). Das "NS-Archiv" des Ministeriums für Staatssicherheit der DDR und seine archivische Bewältigung durch das Bundesarchiv.

[105] Dumschat, S. (2007). Archiv oder "Mülleimer"?, p. 7.

Nazi Third Reich and to exploit them for the purposes of the new East German communist dictatorship. A dictatorship that did not respect the fundamental rights of democratic regimes, including the right to a fair trial or the principle of "ne bis in idem", which we know as one of the pillars of democratic criminal proceedings. To conclude, the NS-Archiv demonstrates very well how dangerous it is to combine the two elements: 1. the violation of the fundamental principles of the democratic rule of law in totalitarian non-democratic regimes, and 2. the existence and preservation of sensitive data about citizens that are potentially damaging and compromising. Along with this, it is necessary to take very seriously the constant and ever-present risk that at some point in the future a democratic regime may fundamentally change towards a non-democratic one, and the permanence of the rule of law cannot thus be relied upon absolutely. In geopolitical terms, the risks increase especially in countries that do not have a tradition of long-lasting and continuous democracy, or that are threatened by the proximity of non-democratic states with great power ambitions. This is true for the vast majority of existing countries, including many European states.

CHAPTER 8

Data Minimisation—Storage Limitation—Archiving

Any preservation of data or records automatically entails the potential risk of misuse. The digital world, including the sector of electronic archiving, has accentuated this phenomenon even further. On the one hand, it has facilitated unauthorised remote access to electronic data, on the other, it has enabled the unauthorised extraction of digital data from which—although primary access is open or permitted by the citizen—using certain tools and algorithms it is possible to indirectly extract other information without the consent or even knowledge of the citizen. In a way, this is analogous to typical intelligence work, which is increasingly being used in the private sphere for various purposes.

This is also true for the risks of deanonymisation of personal data, that is, reidentification of individuals. Although together with data destruction, anonymisation belongs among the important tools of data minimisation, it is becoming increasingly apparent that anonymisation is not a panacea. Not only can it be opted for in certain situations and not in all circumstances, given the need to preserve (personal) data, but the increasing capabilities of information technology and artificial intelligence are bringing more effective tools enabling the reidentification of individuals and the deanonymisation of anonymised and pseudonymised data. In this respect, one could apply the observation of the Working Party on the Protection of Individuals with regard to the Processing of Personal Data

M. Čtvrtník, *Archives and Records*,
https://doi.org/10.1007/978-3-031-18667-7_8

as an independent European data protection and privacy advisory body: "Thus, anonymisation should not be regarded as a one-off exercise and the attending risks should be reassessed regularly by data controllers".[1]

8.1 Data Retention as a Specific Form of Data Minimisation, and Data Storage Limitation

One of the specific levels on which the problem of minimising personal data and limiting their preservation demonstrates, is the phenomenon of "data retention" as the process of retaining traffic and location data, that is, a broad set of data relating to the use of public telephone networks, public mobile telephone networks, and electronic communications networks.[2] In the legal systems of European countries, it is common to find data retention obligations imposed on entities providing public communications networks or providers of publicly available electronic communications services for a certain period of time.[3] In October 2020, the most recent (but not the first) judgement of the Court of Justice of the European Union was delivered, which demanded that the governments of the Member States of the European Union may require operators to store and access aggregated and non-targeted data only in the case of fighting serious crime or in a situation of serious threat to national security.[4] The court went on to state that national legislation imposing an obligation to make traffic and location data available to security and intelligence services "exceeds the limits of what is strictly necessary and cannot be considered to be justified, within a democratic society".[5] In this respect, the Court did not find legitimate such legislation which allows public authorities to impose on providers of electronic communications services an obligation

[1] Article 29 data protection working party. (2014). Opinion 05/2014 on Anonymisation Techniques. 0829/14/EN. WP216. Adopted on 10 April 2014. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf, p. 4.

[2] In the Czech legal system, the rules and scope of the preservation of traffic and location data are set out in a decree of 17 of October 2012, Decree No. 357/2012 Coll. on preservation, transfer, and deletion of traffic and location data.

[3] In the Czech legal system, the data retention period is 6 months according to Act No. 127/2005 Coll. on Electronic Communications and on Amendment to Certain Related Acts (Electronic Communications Act), as subsequently amended, Section 97(3).

[4] Judgment of the Court of Justice of the European Union (Grand Chamber) of 6 October 2020 in Case C-623/17.

[5] Ibid., par. 81.

to transmit traffic and location data to security and intelligence services on a general and indiscriminate basis.[6]

However, in some European countries, including the European Union itself, the issue of data retention has been a matter of concern for some time. In 2006, the European Union passed a controversial directive that required EU Member States to ensure that their legislations preserve traffic and location data of public telephone, mobile, and electronic communications networks for a minimum of six months and a maximum of two years from the date of communication.[7] Subsequently, individual member states started to implement the directive in their national law. In Germany, the directive was enforced at the end of 2007,[8] after which a number of constitutional complaints were filed alleging violation of telecommunications secrecy and the right to informational self-determination as fundamental rights guaranteed by the German constitution.[9] In 2010, the German Federal Constitutional Court ruled the law unconstitutional and abolished it. It declared the six-month general retention of traffic and location data to be contrary to the German constitution as it contravened postal and telecommunications secrecy.[10] General retention and provision

[6] Ibid., par. 82.

[7] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, Art. 6.

[8] Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG vom 21.12.2007, BGBl I S. 3198.

[9] On the right to informational self-determination as a fundamental right in Germany, see Chap. 2.

[10] Urteil des Ersten Senats vom 02. März 2010 - 1 BvR 256/08 -, Rn. 1-345. BVerfG. Reference to the German Constitution: Grundgesetz für die Bundesrepublik Deutschland (Grundgesetz für die Bundesrepublik Deutschland in der im Bundesgesetzblatt Teil III, Gliederungsnummer 100-1, veröffentlichten bereinigten Fassung, das zuletzt durch Artikel 1 des Gesetzes vom 15. November 2019 (BGBl. I S. 1546) geändert worden ist), par. 10 [Basic Law for the Federal Republic of Germany in the revised version published in the Federal Law Gazette Part III, classification number 100-1, as last amended by Article 1 of the Act of 28 March 2019 (Federal Law Gazette I p. 404), Art. 10]. On the abovementioned judgement of the Federal Constitutional Court, cf. also de Vries, K., Bellanova, R., Hert, P. D., Gutwirth, S. (2011). The German Constitutional Court Judgment on Data Retention: Proportionality Overrides Unlimited Surveillance (Doesn't It?). In *Computers, Privacy and Data Protection: an Element of Choice* (pp. 3–23). https://doi.org/10.1007/978-94-007-0641-5_1

of data violates the principle of proportionality when the interference with fundamental freedoms is not proportionate to the need to protect the rights. For example, in the field of criminal proceedings, the balance would lie in the use of such data in the case of suspected serious offences.

Meanwhile, the European Directive continued to apply in Germany. However, this changed by a 2014 judgement of the Court of Justice of the European Union, which retroactively annulled the controversial 2006 directive.[11] The Court considered the relationship of the Directive to the rights guaranteed by the Charter of Fundamental Rights of the European Union, in particular the "right to respect for private and family life, home and communications" and the right to the protection of personal data.[12] In particular, the Court took into account that "the data which providers of publicly available electronic communications services or of public communications networks must retain, pursuant to Articles 3 and 5 of Directive 2006/24, include data necessary to trace and identify the source of a communication and its destination, to identify the date, time, duration and type of a communication, to identify users' communication equipment, and to identify the location of mobile communication equipment, data which consist, inter alia, of the name and address of the subscriber or registered user, the calling telephone number, the number called and an IP address for Internet services. Those data make it possible, in particular, to know the identity of the person with whom a subscriber or registered user has communicated and by what means, and to identify the time of the communication as well as the place from which that communication took place. They also make it possible to know the frequency of the communications of the subscriber or registered user with certain persons during a given period."[13]

Based on this, the Court concluded that: "Those data, taken as a whole, may allow very precise conclusions to be drawn concerning the private

[11] Judgment of the Court of Justice of the European Union (Grand Chamber) of 8 April 2014. "Electronic communications—Directive 2006/24/EC—Publicly available electronic communications services or public communications networks services—Retention of data generated or processed in connection with the provision of such services—Validity—Articles 7, 8 and 11 of the Charter of Fundamental Rights of the European Union". In Joined Cases C-293/12 and C-594/12.

[12] Charter of Fundamental Rights of the European Union of 26 October 2012. 2012/C 326/02, Art. 7 and 8.

[13] Judgment of the Court of Justice of the European Union (Grand Chamber) of 8 April 2014, par. 26.

lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them".[14] As a result, the very storage of such data for the purpose of their eventual further disclosure to the public authorities "directly and specifically affects private life",[15] and therefore the right to respect for one's private and family life, home, and communications, as well as the right to the protection of personal data guaranteed by the Charter of Fundamental Rights of the European Union.

In its judgement, the Court then summarised that the phenomenon of the retention of traffic and location data and their subsequent use by the public authorities without informing the person concerned constitutes an extensive and particularly serious interference with the abovementioned fundamental rights, highlighting the fact that if the persons concerned are not informed of the retention and use of such data, it may "generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance".[16]

In 2016, the Court of Justice of the European Union issued another judgement reiterating that the limitation of personal data protection in the context of the storage and provision of electronic communications must be reduced to the absolute minimum necessary.[17]

Going back to Germany, the development in the area of data retention had been completed for the time being by the 2015 law, which, although it stipulated the obligation to retain traffic and location data, reduced the retention period from 6 months to 10 weeks.[18] In addition, at the end of

[14] Ibid., par. 27.

[15] Ibid., par. 29.

[16] Ibid., par. 37.

[17] Judgment of the Court of Justice of the European Union (Grand Chamber) of 21 December 2016. Reference for a preliminary ruling—Electronic communications—Processing of personal data—Confidentiality of electronic communications—Protection—Directive 2002/58/EC—Articles 5, 6 and 9 and Article 15(1)—Charter of Fundamental Rights of the European Union—Articles 7, 8 and 11 and Article 52(1)—National legislation—Providers of electronic communications services—Obligation relating to the general and indiscriminate retention of traffic and location data—National authorities—Access to data—No prior review by a court or independent administrative authority—Compatibility with EU law). In Joined Cases C-203/15 and C-698/15.

[18] Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten vom 10. Dezember 2015, § 113b, sentence 1.

2015, an amendment was added to the German Code of Criminal Procedure[19] imposing significantly stricter rules and limitations on access to traffic and location data. These are provided only for the investigations of a selected group of particularly serious crimes, such as high treason, sexual abuse, child pornography, murder, and certain other crimes.

The issue of data retention is also undergoing significant development in the Czech Republic. A 2005 Act imposed an obligation on those providing a public communications network or a publicly available electronic communications service to retain traffic and location data for a maximum period of 12 months, while an implementing decree specified this period to be 6 or, in the case of some data, 3 months.[20] Several years later, however, following an initiative of 51 Czech MPs, the Czech Constitutional Court assessed this provision and annulled it.[21] Subsequently, an amendment was approved which made it mandatory to keep these data for 6 months.[22]

[19] Strafprozeßordnung in der Fassung der Bekanntmachung vom 7. April 1987 (BGBl. I S. 1074, 1319), die zuletzt durch Artikel 49 des Gesetzes vom 21. Dezember 2020 (BGBl. I S. 3096) geändert worden ist, § 100 g [Code of Criminal Procedure as published on 7 April 1987 (Federal Law Gazette I, p. 1074, 1319), as last amended by Article 3 of the Act of 11 July 2019 (Federal Law Gazette I, p. 1066). Amendment Act § 100 g of 18 December 2015].

[20] Zákon č. 127/2005 Sb. ze dne 22. února 2005, o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích [Act No. 127/2005 Coll. on Electronic Communications and on Amendment to Certain Related Acts (Electronic Communications Act)], as subsequently amended, § 97 (3); Vyhláška č. 485/2005 Sb. ze dne 7. prosince 2005, o rozsahu provozních a lokalizačních údajů, době jejich uchovávání a formě a způsobu jejich předávání orgánům oprávněným k jejich využívání [Decree No. 485/2005 Coll., of 7 December 2005, on the Extent of Traffic and Location Data, Period of Time for which such Data are Retained and Manner in which they are Submitted to Bodies Authorised to Use the Data], § 4.

[21] Nález Ústavního soudu, Pl.ÚS 24/10 ze dne 22. 3. 2011. 94/2011 Sb., N 52/60 SbNU 625. Data retention I (shromažďování a využívání provozních a lokalizačních údajů o telekomunikačním provozu) [Constitutional Court judgement PI.ÚS 24/10 of 22 March 2011, 94/2011 Coll., N 52/60 SbNU 625. Data retention I (collection and use of traffic and location data on telecommunications traffic)].

[22] Zákon č. 127/2005 Sb. ze dne 22. února 2005, o elektronických komunikacích a o změně některých souvisejících zákonů, § 97. [Act No. 127/2005 Coll. of 22 February 2005, on Electronic Communications and on Amendment to Certain Related Acts, § 97]. Pursuant Amendment No. 273/2012 Coll. of 18 July 2012, amending Act No. 127/2005 Coll., on Electronic Communications and on Amendment to Certain Related Acts (Electronic Communications Act), as subsequently amended.

In 2012, the Czech Constitutional Court[23] repealed Section 88(a) of the Code of Criminal Procedure, which was subsequently revised and the above amendment was added. The Czech legal system thus anticipated the development in Germany by several years and narrowly specified the categories of offences for which law enforcement authorities may request data on telecommunications traffic (including intentional offences with a maximum penalty of at least three years).[24]

The development in the Czech Republic finally concluded in 2019 by a ruling of the Czech Constitutional Court, which confirmed the obligation of those providing a public communications network or a publicly available electronic communications service to retain traffic and location data for a period of 6 months.[25]

Data retention represents a specific situation in which data minimisation becomes the underlying question, both in terms of the scope of the data to be retained and the time limit determined for their retention. It is thus a special case as the ability to tip the imaginary scales lies with the minimisation of the data that the state is entitled to keep on its citizens in order to ensure their security on the one hand, their freedom on the other, and at the same time a democratic open society; the other side of the scales is totalitarian practices, Big-Brother-like surveillance, and discipline of the citizens.

Data minimisation in archives and archiving asks a similar key question as data retention, that is, what data on their citizens do public authorities have the right to maintain. Yet, another specific focus moves in a different direction: What citizen data the state and public authorities can keep permanently or for long periods of time. In the following part, I will take a closer look at how the principles of data minimisation and storage

[23] Nález Ústavního soudu, Pl.ÚS 24/11 ze dne 20. 12. 2011. 43/2012 Sb. N 217/63 SbNU 483 Data retention II (přístup orgánů činných v trestním řízení k údajům o telekomunikačním provozu) [Constitutional Court judgement PI.ÚS 24/11 of 22 December 2011, 43/2012 Coll., N 217/63 SbNU 483 Data retention II (access of law enforcement authorities to data on telecommunications traffic)].

[24] Zákon č. 141/1961 Sb. ze dne 29. listopadu 1961, o trestním řízení soudním (trestní řád), § 88a [Act No. 141/1961 Coll. of 29 November 1961 on Criminal Procedure (Code of Criminal Procedure), § 88(a)].

[25] Nález Ústavního soudu, Pl.ÚS 45/17 ze dne 14. 5. 2019. 161/2019 Sb. Data retention III (shromažďování a využívání provozních a lokalizačních údajů o telekomunikačním provozu) [Constitutional Court judgement PI.ÚS 45/17 of 14 May 2019, 161/2019 Coll. Data retention III (collection and use of traffic and location data on telecommunications traffic)].

limitation shape the field of archives and archiving, including archival theory and methodology, and what are the main tools archives and archiving use to apply them. I will briefly introduce this issue with a specific concept of data minimisation in relation to archiving in the public interest using the diction of the European GDPR.

8.2 Data Minimisation and Storage Limitation in Relation to Archives and Archiving

In the European Union, the General Data Protection Regulation (GDPR)[26] has assigned archiving in the public interest—similar to scientific and historical research or statistical purposes—a privileged status. Archiving in the public interest has been exempt from the generally formulated and applied principles of personal data processing, including an exemption from the very broadly formulated right to be forgotten, in which case the purpose of archiving in the public interest is itself the reason for not applying the right to be forgotten. However, this privileged position also has significant limitations. Any privileges reserved for archiving in the public interest are conditional on guaranteeing the main principles of personal data processing as defined by the GDPR in Article 5, two of which are key: the "data minimisation" principle and the "storage limitation" principle. These safeguards are then further specified in GDPR Article 89 under the somewhat convoluted wording that the relevant measures "may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner."

The core of the regulation, which is crucial for archival and historical science, is based on conditionality: If it is possible to erase the specific identity of a person, the obligation to de-identify a specific person applies, provided that the public interest of archiving and the scientific and historical research objectives or statistical purposes are not compromised. At this point, the European Regulation opens a very large room for

[26] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). https://eur-lex.europa.eu/eli/reg/2016/679/oj

interpretation: Who shall assess, in what way and according to what criteria, whether the purpose pursued—in the case of archiving, it is the purpose of archiving in the public interest—can be fulfilled, even when the identification of persons concerned in the records and archives is erased? Typically, this may be the case of census records, which, for example, Germany has been anonymising for several decades, and the Czech Republic did so most recently in 2021 before transferring the records to an archive for permanent preservation.

Yet, regardless of the European GDPR, it is extremely important that archives and entire archival systems are able to view the protection of personality and privacy from the perspective of the actual permanent or—if we are more realistic—long-term preservation of data in archives. Here, archiving comes into contact with what can be aptly described—and not only according to the GDPR—as data minimisation and data storage limitation. In the vast majority of developed archival systems, archives are the places that both implement and are responsible for the absolute largest share of the total reduction of public records created. In the context of archival appraisal and selection of records for permanent preservation, archives perform by far the largest, completely legal destruction of public records that occurs today; it is usually around 95% of the total of public records created. This is then proportionate to the responsibility not only for the adequate and professional selection of records valuable from an archival-historical perspective, but also for the irreversible destruction of such records and data which, on the one hand, pose a serious risk of potential future misuse and on the other, do not have such a high historical-archival value that they should be preserved in an archive permanently or for a long term.

Archival theory, methodology, and practice, however, have so far neglected the potential risks of misuse of sensitive personal data contained in permanently (or long-term) stored records, and have focused almost exclusively on the records information content and their future usability by various research projects and private research interest. This is what archiving should change in the future. In the following part, I will take a closer look at some models of archival appraisal as they took shape in the post-1945 period. I will conclude by analysing another form of minimisation and data storage limitation, which is the process of anonymisation or pseudonymisation, proposing a concept of linking anonymisation and pseudonymisation to the four categories of the right to be forgotten as

presented in Chap. 5. I will pay particular attention to the risks of deanonymisation and reidentification.

8.2.1 Records Destruction and Archival Appraisal as Basic Tool for Minimising Personal Data in Records and Archives

General awareness views archives primarily as institutions serving the purpose of preserving and archiving data and records. However, their equally important function is to reduce records created by a wide range of entities ranging from public to private institutions and natural persons. However, the purpose of this reduction should not only be the necessary reduction of the volume of permanently or long-term archived material, but also the protection of the personality, privacy, and personal data of those concerned in the records. This purpose will play an increasingly important role in the future, due to the significantly higher risk of data misuse in the case of electronic data and records compared to paper documents.

Common developed archival systems across countries establish more or less similar models to implement a process by which a very small part of records is designated for permanent or long-term preservation and the absolute majority for legal destruction. This process occurs even before the actual archiving and preservation and processing of archival records in archives. Although the legislations of some countries do implement an obligation even for private entities to submit their records to archives for retention procedures and archival appraisal, this is a rather minor phenomenon. This is due to the common assumption that private entities, including individuals, should have the right to dispose of their records as they see fit (provided, of course, that other rights are not infringed, including the most closely watched protection of personality, privacy, and personal data). For this reason, and in the context of the whole text, I will therefore consider archival appraisal primarily using the example of public records.

In the English-speaking world this process is most often referred to as "archival appraisal", in German terminology it is called "archivische Bewertung", in French the terms "évaluation" or "tri" are used, in Italian it is "selezione". In terms of meaning, the professional archival terminology reflects that it is a certain "selection" of records, a process that goes hand in hand with their "evaluation" based on certain content criteria. The International Council on Archives, in its draft methodology for records appraisal, provides a fairly adequate definition: "Appraisal is the process of evaluating records to determine how long to keep them,

including to decide if the records have sufficient long term value to warrant the expense of preservation in an archives. Appraisal is fundamental to the archival endeavor, because appraisal determines what records will be kept and what records can be disposed."[27]

Especially after 1945, in the context of a massive increase in the volume of records created, the archival industry began to develop some models of archival appraisal, which sought to systematically reduce the volume of records before the moment they are archived. At the very core of the different models is the search for and reconnaissance of certain values or, in more recent terms, meanings that a record or archival material can carry and, if applicable, also the determination of who do they carry them for. The now classic concept of primary and secondary values by the American archivist and thinker Theodore R. Schellenberg achieved a great international resonance and has had a significant impact on contemporary archives. "Primary value" according the Schellenberg's mid-1950s reasoning represents the meaning of the record for which it was originally created.[28] It is therefore the meaning primarily determined by the needs of the record creator. "Secondary value" is then determined by the interests of other institutions or private researchers, it expresses a secondary meaning, in the classical Schellenberg sense, the scientific, research, or historical meaning. Schellenberg then divides secondary value into two categories. First, there is the "evidential value", which consists in the information the record provides on the activity of the record creator. Second, it is the "informational value" or "research value", which expresses what information for research in various sciences the particular record contains.[29] In both cases, however, it is of value for research purposes.

However, Schellenberg's concept introduced one crucial point: It marked a sharp departure from the opposing approach, the most prominent representative of which was already before World War II, another distinguished classic of archival theory, Hilary Jenkinson. The key was the departure from Jenkinson's idea that archives should preserve the exact

[27] Mills, T. (May 2005). *Strategic approaches to appraisal. In International Council on Archives. Guidelines on Appraisal.* https://www.ica.org/sites/default/files/CAP_2005_guidelines_appraisal_EN.pdf

[28] Schellenberg, T. R. (2003). *Modern Archives. Principles and Techniques.* Society of American Archivists, p. 133. Cf. also Schellenberg, T. R. (1956, October). The Appraisal of Modern Records. *Bulletins of the National Archives*, 8.

[29] Schellenberg, T. R. (2003). *Modern Archives*, p. 140ff. Cf. above all Schellenberg, T. R. (1956). The Appraisal of Modern Records.

arrangement of the collection of records as it was constituted by the creator, without discarding any of the records.[30] Jenkinson would have preferred to leave out appraising records in terms of their possible historical significance, and Schellenberg in this respect represented the post-war awakening to the absurdity of Jenkinson's idea.

Then, at the beginning of the twenty-first century, Canadian archival thinkers (Yvon Lemay, Sabine Mas, Louise Gagnon-Arguin) came up with the idea of expanding and complementing the classical concept of primary and secondary value of the record and they proposed the concept of a tertiary value at the sixth symposium of the Interdisciplinary Group for Research in Archival Science (Groupe interdisciplinaire de recherche en archivistique, GIRA) "Archives, from information to emotion" ("Les archives, de l'information à l'émotion"), held in Montréal in 2010.[31] The Canadian concept uses several not yet fully unified terms: the "emotional value" ("valeur émotive"),[32] the "sentimental value" ("valeur sentimentale"),[33] and also the "artistic-emotional-affective" nature of the value thus defined.[34] The common denominator of this idea is the hypothesis that archival records have, in addition to the abovementioned primary and secondary value, or in addition to the testimonial and informational value, also an emotional value. Yvon Lemay and Marie-Pierre Boucher provide a condensed definition: "Imagine for a moment that on the desk in your office is a framed photograph of your mother, taken in hospital just before she passed. Needless to say, whenever you look at that photo, you feel devastated. Even though a very banal photograph, it has immense

[30] Jenkinson, H. (1922). *A Manual of Archival Administration*. Clarendon Press, passim, for example, pp. 106–108, 128–129.

[31] 6e symposium du Groupe interdisciplinaire de recherche en archivistique (GIRA). (2010). Les archives, de l'information à l'émotion. Congrès des milieux documentaires, 3 November 2010. Symposium programme and main theses: http://gira-archives.org/activites/6e-symposium-2010/

[32] Mas, S., Gagnon-Arguin, L. (2010–2011). Considérations sur la dimension émotive des documents d'archives dans la pratique archivistique. La perception des archivistes. 6e symposium du Groupe interdisciplinaire de recherche en archivistique (GIRA). *Archives*, 42(2), 53–64, passim.

[33] Lemay, Y., Boucher, M.-P. (2010–2011). L'émotion ou la face cachée de l'archive. 6e symposium du Groupe interdisciplinaire de recherche en archivistique (GIRA). *Archives*, 42(2), 39–52, p. 45.

[34] Cf. Mas, S., Klein, A. (2010–2011). L'émotion: une nouvelle dimension des archives. Contexte et résumé des exposés du 6e symposium du GIRA tenu le mercredi 3 novembre 2010 au Palais des Congrès de Montréal. *Archives*, 42(2), 5–8, p. 7.

value."[35] Usually it is the authenticity of the (archival) record with a direct link to its source, origin, or author that creates a strong "emotional charge". Lemay and Boucher eventually systematised three basic functions of archival records and, with them, of archives as their controllers: (1) to inform ("informer"), (2) to bear witness ("témoigner"), and (3) to revive the past, to evoke, to "recall the past" ("évoquer").[36] Not only Lemay and Boucher, but also other members of the GIRA group appeal to archives and archivists to take this third value, dimension, and function of the archival record seriously enough to start noticing it and implementing it in their activities, especially in the field of various forms of access to and use of archives, including exhibitions.

Eric Ketelaar, one of the most influential and formative figures in contemporary archival studies, looked at the layers of meaning in records from a slightly different direction. Ketelaar has significantly reversed the perspective when he asked how users (researchers, historians, etc.) create meaning for the record and the historical source. He began with the claim that records have a whole range of "meanings", in a way, they are a "repository of meanings".[37] A few years ago, with the help of psychology, Ketelaar specified and systematised the various ways of the emergence or constitution of record meanings.[38] He based his distinction on one of the basic systematisations used in psychology, distinguishing in principle three kinds of mental processes: cognitive (knowledge), affective (emotions), and conative (volition). This is a division that psychology uses in other contexts as well, in the teaching of propositional attitudes, and so on. Ketelaar transferred this division into archival theory and methodology and applied it when considering the constitution of the meanings of records. He distinguished three ways of forming the meanings: (1) cognitive mode, (2) affective mode, and (3) conative mode. The cognitive mode of constructing

[35] "Imaginez un instant qu'il y a dans votre bureau un cadre qui contient une photographie de votre mère prise à l'hôpital peu de temps avant son décès. Inutile de dire qu'à chaque fois où vous regardez cette image, elle vous bouleverse. Elle vous remémore son absence. Peut-être entendez-vous sa voix. Des bribes de sa vie, tout comme de la vôtre, vous reviennent à l'esprit6. Bien que cette image soit des plus banales, elle possède à vos yeux une valeur inestimable." Lemay, Y., Boucher, M.-P. (2010–2011). L'émotion ou la face cachée de l'archive, pp. 45–46.

[36] Lemay, Y., Boucher, M.-P. (2010–2011). L'émotion ou la face cachée de l'archive, p. 47.

[37] Ketelaar, E. (2001). Tacit Narratives: The Meanings of Archives. *Archival Science*, 1, 131–141. https://doi.org/10.1007/BF02435644

[38] Ketelaar, E. (2012). Cultivating Archives: Meanings and Identities. *Archival Science*, 12, 19–33. https://doi.org/10.1007/s10502-011-9142-5, pp. 24–26.

the meaning of a record, or the cognitive mode of the user's attitude towards the record, represents a purely cognitive way, and cognitive motivation of the record user. The conative mode of constructing the meaning is based on the specific motivations and intentions with which the user approaches the historical source. The motivation is different for a person looking for employment records to calculate his pension, different for a historian writing an expert study, and different for a thief looking to gain profit from selling archival records or valuable parts of archival material. Ultimately, the affective mode embodies the emotional level of the user's attitude to the record/archive/historical source, corresponding to the tertiary value of the record according to Canadian archival theory.

The above concepts focus on what layers of meaning shape records. One step "down" from the actual practice of appraisal of records are the models of archival appraisal, which began to take shape gradually from the 1950s onwards. Already in the early discussions of the 1950s, the West German archivists, Georg Wilhelm Sante and Wilhelm Rohr, called for the assessment of records not to be based on the records themselves, but rather use the entire files and groups of creators as the starting point for such assessment. Hans Booms later referred to the findings of the archivists as the Sante-Rohr model.[39] Hans Booms himself, President of the German Federal Archives from 1972 to 1989 and one of the most important German archival theorists and thinkers, built a different model in the 1970s, based on a different premise: Archival appraisal is intended to create a society-wide documentation of public life in all its complexity and diverse facets. For this purpose, Booms proposed to create models for the creation of historical documentation ("Überlieferungsmodelle"), which he called the "documentation plan" ("Dokumentationsplan").[40] In younger debates in Germany, the term "documentation profile"

[39] Sante, G. W. (1957). Archive und Verwaltung – historische Provenienz und Probleme der Gegenwart. *Der Archivar*, 10, 7–16, p. 7ff.; Sante, G. W. (1958). Behörden – Akten – Archive. Alte Taktik – neue Strategie. *Archivalische Zeitschrift*, 54, 90–96; Rohr, W. (1958). Zur Problematik des modernen Aktenwesens. *Archivalische Zeitschrift*, 54, 74–89. On the Sante-Rohr model cf. also Uhl, B. (1994). Die Geschichte der Bewertungsdiskussion. In A. Wettmann (Ed.), *Bilanz und Perspektiven archivischer Bewertung. Beiträge eines Archivwissenschaftlichen Kolloquiums.* (pp. 11–36). Archivschule Marburg, p. 23.

[40] Booms, H. (1972). Gesellschaftsordnung und Überlieferungsbildung – Zur Problematik archivarischer Quellenbewertung. *Archivalische Zeitschrift*, 68, 3–40, pp. 37–40. Published in English as: Booms, H. (1991–92). Uberlieferungsbildung: Keeping Archives as a Social and Political Activity. *Archivaria*, 33(Winter), 25–33. https://archivaria.ca/index.php/archivaria/article/view/11796, pp. 28–30.

("Dokumentationsprofil") became more common. One of the results was a methodological aid for creating documentation profiles in municipal archives, approved by the German Federal Conference of Municipal Archives ("Bundeskonferenz der Kommunalarchive") in 2008.[41]

Boom's concept of a documentation plan and the effort to mirror the whole of society in archives and archival collections corresponds with the direction of archival methodology in the USA and Canada, which have been and still are greatly influenced by social history, including the so-called new social history.[42] Social history was absorbed into one of the world's most influential archival appraisal models, called macro-appraisal developed by Terry Cook (1947–2014) in Canada in the early 1990s (the origins date back to the late 1980s). It has been put into practice at the National Archives of Canada (now Library and Archives Canada), further developed until recently and is gradually applied in archival systems in various parts of the world.[43] In the macro-appraisal model, Cook calls for a shift away from concentration on the substantive content of a particular individual record and a focus on the functions, activities, programmes, and so on of the record creator.[44] The functions and activities of the creator must be understood in the context of their origin and within a broader

[41] Arbeitshilfe. Erstellung eines Dokumentationsprofils für Kommunalarchive. Beschluss der BKK von 2008-09-15/16 in Erfurt. (2009). *Der Archivar* 62, 122–132. https://www.bundeskonferenz-kommunalarchive.de/empfehlungen/Arbeitshilfe_Dokumentationsprofil Dokumentationsprofil.pdf

[42] Cf. Lockwood, E. (1990). "Imponderable Matters": The Influence of New Trends in History on Appraisal at the National Archives. *The American Archivist*, 53 (Summer), 394–405. https://doi.org/10.17723/aarc.53.3.w66t31032j7528t4, p. 395. On the influence of social history on archiving, see also Mayer, D. (1985). The New Social History: Implications for Archivists. *The American Archivist*, 48 (Fall), 388–399. https://doi.org/10.17723/aarc.48.4.l107660916858k13; Miller, F. (1981). Social History and Archival Practice. *The American Archivist*, 44 (Spring), 113–124. https://doi.org/10.17723/aarc.44.2.r5x54qq0r71275w4; Miller, F. (1986). Use, Appraisal, and Research: A Case Study of Social History. *The American Archivist*, 49 (Fall), 371–392. https://doi.org/10.17723/aarc.49.4.e1251j7r1125525n

[43] On Cook's theory of macroappraisal including further bibliographical references cf. Čtvrtník, M. (2011). Die Theorie von der "macroappraisal" im Sinne Terry Cooks und die Frage der archivischen Bewertung. *Archivalische Zeitschrift*, 92, 73–98. https://doi.org/10.7788/az.2011.92.1.73. Cf. also Čtvrtník, M. (2011). Terry Cook. *Archivní časopis* [*Journal on Archives*], 61(1), 79–87.

[44] Cook, T. (1996). Building an Archives: Appraisal Theory for Architectural Records. *The American Archivist*, 59 (Spring), 136–143, p. 139. https://doi.org/10.17723/aarc.59.2.9016827w6t4271wl

context (political, social, cultural, etc.) and based on this context, the value of these functions, activities, and institutions, as well as the value of the creators themselves, needs to be determined. The theory of macro-appraisal consists in the transition from "content-based information" to "context-centred knowledge". Cook then interprets the aforementioned shift from the question "what information does the record contain" to the question "how and why was the record created" as a recovery of a sense of provenance or as a "rediscovery of a sense of provenance".[45] The reason why we can speak of a change in the meaning of the most important and default classical principle of provenance is the fact that in Cook's work provenance is no longer primarily the office and its organisational structure, but in short, it is the functional context of the record creation. Similar tendencies in contemporary archiving can be found in the aforementioned Eric Ketelaar, who also claims to have found inspiration in Terry Cook.[46] While Cook uses macro-appraisal theory as a means of defining himself in relation to traditional archiving, Ketelaar, in a very similar vein, introduces the dichotomy of "descriptive archivistics" and "functional archivistics".[47] Compared to Cook, however, Ketelaar's approach is characterised by a greater focus on the person of the record creator.

However, archival methodology is also developing some other models of archival appraisal. One of the thoroughly elaborated models, including a step-by-step application in public records, was created in Germany by the State Archives of Baden-Württemberg, one of the German Landesarchives. The method of "vertical and horizontal evaluation" is based on a comparison of the roles and functions of organisations and their components in their vertical (superordinate and subordinate units) and horizontal structure (division of competences between units at the

[45] Cook, T. (2005). Macroappraisal in Theory and Practice: Origins, Characteristics, and Implementation in Canada, 1950–2000. *Archival Science*, 5, 101–161. https://doi.org/10.1007/s10502-005-9010-2, p. 124. Cf. also Cook, T. (1997). What is Past is Prologue: A History of Archival Ideas Since 1898, and the Future Paradigm Shift. *Archivaria*, 43 (Spring), 17–63. https://archivaria.ca/index.php/archivaria/article/view/12175, pp. 35ff. Terry Cook mentions Tom Nesmith, who used the term "rediscovery of provenance".

[46] Ketelaar, E. (2000). Archivistics Research Saving the Profession. *The American Archivist*, 63 (Fall/Winter), 322–340. https://doi.org/10.17723/aarc.63.2.0238574511vmv576, p. 326. For a more detailed interpretation cf. Čtvrtník, M. (2012). Eric Ketelaar. *Archiwista Polski*, 67(3), XVII, 129–137, p. 132.

[47] Ketelaar, E. Archivistics Research Saving the Profession, p. 327ff.

same level, their cooperation, etc.).[48] By finding out the tasks, activities, competences of a given subject in the context of competences, activities, and cooperation with other subjects (their superiors, subordinates, or those standing on the same level), the archivist then uses this method to excavate the records with the greatest relevance and informative value.[49]

The perspective of not only evaluating records but also the offices, organisations, that is, the creators of the records, and evaluating "their" records according to their "value", was already being pursued by the East Germans in the 1960s. Basically, they tried to establish classes or categories of creators (registry officers) according to their social importance.[50] A more significant shift away from the emphasis on the record alone towards evaluation of the creators occurred in West Germany around the 1970s. The creators were evaluated in the government system. However, it remained in principle in the context of the state administration; no broader or other context was considered. Current debate in Germany, known as the "horizontale und vertikale Bewertung", can trace its predecessor to the German debates in the 1970s that discussed "horizontally/vertically integrated appraisal" ("horizontal/vertikal integrierte Bewertung";

[48] Cf., for example, Treffeisen, J. Archivübergreifende Überlieferungsbildung in Deutschland. Die vertikale und horizontale Bewertung. http://www.forum-bewertung.de/beitraege/1022.pdf. Published in English as Treffeisen, J. (2003). The Development in Germany of Archival Processing—The Vertical and Horizontal Appraisal. *Archival Science*, 3(4), 345–366. https://doi.org/10.1007/s10502-004-2273-1; Schäfer, U. Vertikale und horizontale Bewertung der Unterlagen der Wasserwirtschaftsvervaltung in Baden-Württemberg. https://www.landesarchiv-bw.de/media/full/46752. Cf. also Kretzschmar, R. (Ed.). (2002). *Methoden und Ergebnisse archivübergreifender Bewertung.* Verband deutscher Archivarinnen und Archivare e. V. Frankfurt a.M.: Selbstverlag. Cf. also other contributions on the "Forum Bewertung" website, dedicated to archival appraisal (selection): http://www.forum-bewertung.de/. Specific applications of the method of vertical and horizontal appraisal in Baden-Württemberg: https://www.landesarchiv-bw.de/de/landesarchiv/informationen-fuer-behoerden/bewertungsmodelle/70776. The method has been thoroughly developed, for example, for the police, cf. https://www.landesarchiv-bw.de/media/full/47158.

[49] Treffeisen, J. Archivübergreifende Überlieferungsbildung in Deutschland, pp. 6–7.

[50] Cf. especially *Grundsätze der Wertermittlung für die Aufbewahrung und Kassation von Schriftgut der sozialistischen Epoche in der DDR* (1965). Staatliche Archivverwaltung, especially p. 32ff, § 64ff.

"horizontale/vertikale Intergration der Bewertung").[51] Since the 1990s, in addition to German archivists, Swiss archivists have also started to evaluate records based on the position of the creator (within the state administration; within the functions they perform, etc.).[52] At that time, the Swiss Federal Archives began to introduce the procedure of "Priorisierung" ("Prioritisation"). This procedure determines three priority classes ("Prioritätsklassen") A, B, or C on two levels. Registry officers (Registraturbildner) are prioritised first, followed by the groups of records, defined in the filing plans. The shift consists in the fact that the archival-historical significance of records depends on the significance of their creators, classified into individual priority classes.

It might seem that the theories and models of archival appraisal applied later during retention periods and record selection procedures are not primarily related to the protection of personal data, personality, and privacy. But that would be a false impression. The connection exists on two basic levels:

1. At a general level, it is the basic link between archival appraisal, retention periods, and data minimisation, including personal data. The best way to protect these data is to destroy them. In this sense, the most powerful form of data minimisation and storage limitation is the very data reduction in the process of records selection and appraisal. If we stick to using the narrow terminology of the European GDPR, it is true that it views pseudonymisation as primarily a reversible process, in which personal data are recoverable. But the GDPR also introduces the "hard" data minimisation that takes place before the data are transferred to the archive, that is, the data, including personal data, are destroyed.

[51] Cf., for example, Kahlenberg, F. P. (1972). Aufgaben und Probleme der Zusammenarbeit von Archiven verschiedener Verwaltungsstufen und Dokumentationsbereichen in Bewertungsfragen. *Der Archivar*, 25(1), 57–70, p. 59. In Czechia it was Jaroslav Vrbata who emphasised that the basis of the theory of archival appraisal is "the most precise formulation of the social position of the record creator". Vrbata, J. (1979). K některým obecným otázkám výběru archiválií [On some general issues of archival selection]. *Zpravodaj Pobočky ČSVTS SÚA*, 14, 12–67, p. 29.

[52] Cf. the workshop of the Verein Schweizerischer Archivarinnen und Archivare Arbeitstagung of 31 March 1995 and the resulting article: Bütikofer, N. (1995). Bewertung als Priorisierung. *Arbido*, 10(11), 14–16.

2. On a concrete level, it is the individual models of appraisal and selection of records implying the question of which specific groups of records to destroy and which groups to preserve. It is at this point that the potential for assuming a significantly different optic of looking at archival appraisal and records selection opens up: The initial perspective is no longer the question of what informative, and testimonial value the materials may have for current and future research, which ultimately corresponds to the classic Schellenbergian "secondary value" of records. Instead of this approach, which focuses on the information content and usability of records for various research purposes, and which so far still prevails in most archival theory and practice, a perspective opens up that puts the protection of personal data and the security risks of breaching this protection during long-term or permanent archiving at the starting point. This is a perspective that archival methodology has so far overlooked and has not taken in into account in a more fundamental and comprehensive way. It is an approach that primarily asks whether, and if so how, and with what consequences, the data that are hypothetically transferred to the archive could be misused.

Archival science can thus open a new and broad field of research into the crucial implications for archival practice. This raises questions as to which specific groups of records are to be irreversibly destroyed and which are to be preserved in the perspective of protection of personal data, personality, and privacy considering the risks of their possible misuse. Chapter 7, has already provided some specific examples of the misuse of certain groups of records and archives in the twentieth and twenty-first centuries, that included, among others, census and medical records.

I see several points crucial to the relationship of archiving and the process of data minimisation and storage limitation; they are:

1. In the future, archival appraisal and retention management will become key tools for applying the principle of data minimisation and storage limitation within records management even before transferring the data for archiving, as well as in the case of archives and data already archived.
2. Archival appraisal and disposal of records will henceforth acquire a new important function: They will serve as a fundamental pillar of justification for why personal data were preserved and passed on to

the archiving phase and not destroyed during their existence in the records management before being archived. For the vast majority of the first few decades of the records' existence, they will contain the personal data of living persons who will only pass away over time. At the beginning of their existence, archives are only on the starting line of a process that could, with a certain degree of exaggeration be described as the "disappearance of personal data". This is a process that is driven by the living actors concerned in the archives gradually dying and personal data are by definition in most legislative systems tied only to living individuals. The process is similar to post-mortem personality protection, in which the sensitivity of certain data related to personal data and privacy disappears as the period since the death of the individual concerned gets longer. The German Federal Court of Justice (Bundesgerichtshof) put it very precisely when at the end of the 1960s it stated that post-mortem personality protection is limited in time; it is not infinite.[53] In its judgement, the Court also emphasised that the need to protect the rights of the deceased "disappears as the memory of the deceased fades".

In any case, archiving, including archiving in the public interest, begins long before the persons concerned in the archival material die. Thus, archives will always have to deal with the fact that they are managing the personal data of living persons and are therefore subject to all the obligations imposed by the relevant legislation on the processing and protection of such data.

3. Retention periods will become a much more important and multifaceted function. These have so far fulfilled two main functions in the management of public records: For the creators, they serve as a tool for the timely and continuous release of capacity in their registries. But they serve a much more important function for an open democratic society: They compel the creators to propose public records for retention in a timely manner and without delay and to submit some of their records for archiving. In this respect, they are one of the key means for the exercise of transparent and controllable records management, archiving, and all government and public administration processes in general. However, in the new context we are looking at, they will acquire another at least as important

[53] Bundesgerichtshof, Urteil vom 20. März 1968, I ZR 44/66. On this judgement, see in more detail Chap. 2.

crucial role: They will become an essential lever for the application of the data storage limitation principle, if we follow the terminology of the European GDPR, which considers the data storage limitation principle to be one of the fundamental pillars of personal data protection and understands it as the principle that personal data cannot be retained for longer than is strictly necessary for their original purposes. If we stay in the European Union, the GDPR has indeed approved some form of exemption from this principle, inter alia for archival purposes, but even this exemption has its limits and it is not at all clear how its application will be interpreted in the future in individual countries and at the level of the Union (cf. Chap. 5).

In any case, retention periods will become more important in the future for both records management and archiving.

4. In the context of the archival appraisal of public records, in some situations archiving in the public interest is beginning to open up possibilities for the free consent/disconsent of those whose personal data are being considered for archiving. Until now, archiving in the public interest has not taken into account the consent of persons to archiving and has used the standard legal authority for the preservation of records, including personal data.

8.2.2 Anonymisation, Pseudonymisation, and the Link to the Model of Four Categories of the Right to Be Forgotten

Destruction is not the only possible way in which data, including personal data contained in archival records, can be reduced. The second main tool for such reduction, are processes that are mostly summarised under the term data "anonymisation".

Terminologically, the situation is somewhat complicated by the European GDPR, which in 2016 introduced (but not for the first time in the European Union) the concept of "pseudonymisation". Let me thus open the following topic with a terminological analysis.

GDPR distinguishes between two fundamentally different processes—anonymisation and pseudonymisation of data. Pseudonymisation, as defined by the GDPR, means replacing a piece of personal data (e.g., a name) with another identifier so that the personal data cannot be further associated with a specific data subject. However, the possibility of

re-establishing this link between the personal data and their subject is preserved.[54] This re-established link must once again comply—if we remain in the EU area—with all the requirements set out in the GDPR.

Anonymisation, on the other hand, is a process whereby the link between personal data and their bearer is irreversibly broken. The German legislation is a little more specific, defining anonymisation as "the alteration of personal data in such a way that individual data on personal or factual circumstances cannot—or can only be attributed to a specific or identifiable natural person by means of disproportionate demands on time, cost and manpower".[55] In a similar way, it explicitly defines the process of pseudonymisation, namely in the sense of replacing the name and other identifiers with another character in order to exclude or make it substantially more difficult to identify the person concerned, that is, in the form understood and defined by the GDPR.[56]

The question is whether the term "pseudonymisation" will gradually make its way into general archival terminology. Even though the GDPR and its pan-European validity will have a formative influence, it should be mentioned that Germany in particular knew and used this concept much earlier than the so far short-lived GDPR.[57]

Terminologically, it is possible to consider what category is the blacking out personal data, or such data that could lead to their being linked to a specific identifiable person, in copies of records or copies of archival material.

[54] General Data Protection Regulation (GDPR), Art. 4 (5). In connection with other provisions in relation to pseudonymisation set out in the GDPR.

[55] "Anonymisieren ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können." Bundesdatenschutzgesetz vom 30. Juni 2017. BGBl. I S. 2097, § 3 (6).

[56] "Pseudonymisieren ist das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren." Bundesdatenschutzgesetz, § 3 (6)(a).

[57] Amending Act of the German Bundesdatenschutzgesetz of 23 May 2001, adding item 6a under Section 3 and introduced the term "pseudonymisation". Although this amendment was intended to implement Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, the predecessor of today's GDPR, into German legal system, this original European Directive does not yet use the term "pseudonymisation".

In case of presenting "anonymised" ("pseudonymised"?) archival records in the research rooms (but similarly in other situations, typically when publishing a court judgement with blacked-out personal data) it cannot be considered anonymisation in the proper sense of the word. The possibility of re-establishing the link between personal data and their subject remains, for a simple reason: The data redaction (blacking out) only concerns copies of archival records, while the originals—containing all the original data—remain intact in archival depots. Strictly speaking, however, we cannot even talk about pseudonymisation as defined by the GDPR, because the personal data is not replaced by any other identifier and it is not a redaction of the original record but again, only its copies.[58]

However, abstracting from the limited narrow legal framework of this terminology, we could place data redaction (blacking-out) or any other process of "depersonalisation" of archival copies on the imaginary borderline between anonymisation and pseudonymisation. It combines features of both of them. On the one hand, considering the copy of the record/archive and the researcher who consults this record, it could be deemed anonymisation, as it is or should not be possible to recover the eliminated personal data from the copy itself. On the other hand, in the Kantian sense of "an sich", it is possible to restore the eliminated personal data by comparing the "depersonalised" copy of the record/archive with the original and complete the relevant data based on this comparison. And this is the most important feature of pseudonymisation, that is, the possibility of reconnecting the data to a specific person.

On the other hand, in cases when the records are transferred to the archive already anonymised by the creator themselves, so that no one else—not even the archive—will be able to "deanonymise" or "depersonalize" them again, we are dealing with the anonymisation of the original documents, or archival materials in the true sense of the word.

[58] On the concepts of pseudonymisation and anonymisation in the context of GDPR implementation, cf. Chap. 5. They are also mentioned in a paper prepared by the European Archives Group as an official expert group of the European Commission: European Archives Group. (October 2018). *Guidance on data protection for archive services. EAG guidelines on the implementation of the General Data Protection Regulation in the archive sector*. https://ec.europa.eu/info/sites/info/files/eag_draft_guidelines_1_11_0.pdf, cf. in particular pp. 12–13, 23, 34. On the relationship between pseudonymisation and anonymisation in the context of the GDPR cf. Mourby, M., et al. (2018). Are 'pseudonymised' data always personal data? Implications of the GDPR for administrative data research in the UK. *Computer Law & Security Review*, 34(2), 222–233. https://doi.org/10.1016/j.clsr.2018.01.002

It is, among other things, this very fragile relationship between anonymisation and pseudonymisation that will probably play a more important role in the field of archives and records management in the future than it does today, and will also become—at least in some cases, as I have demonstrated in detail using the example of census records—an important social issue. The discussion will be conducted in particular in the direction of the extent to which it will be possible to make do with mere pseudonymisation and to what extent it will be necessary to use "hard", irreversible anonymisation. The debates will undoubtedly include the economic dimension of the issue; data, as they say, is the "black gold" of the twenty-first century. And the irreversible and massive destruction of data will bring about considerable economic losses.[59]

In view of the terminological analysis performed above, the procedure of pseudonymisation is practically without exception applied to records that have already been handed over for permanent archiving and have undergone the process of archival appraisal; the links between the data and their carriers are broken on copies and not on the original records, and the possibility to restore the link between the data and their carriers thus remains.

The process of making archival materials available to researchers consists most often in blacking out the relevant parts that could lead to the identification of their bearer prior to offering them to the researcher for consultation. In the case of analogue pseudonymisation of paper records, usually, however, it is not enough to only redact one copy, most times it is necessary to make a second copy and black out the specific data a second time. Some archives even manually cut out the relevant areas from copies of archival records, which is of course possible only in the case of paper documents and for pseudonymisation of analogue data. This very demanding process is eventually crowned by providing a dissatisfied applicant access to the archival material in a research room, the applicant is unhappy as they have received the eagerly awaited material usually after a not too short period of time, which in the "age of access" they gradually cease to be willing to tolerate, or they lose interest in the data made available with such a delay.

[59] In the context of reflection on the GDPR, see, for example, Kafsack, H. (2015, 18 December). Im Tausch gegen Daten. *Frankfurter Allgemeine*. http://www.faz.net/aktuell/wirtschaft/netzwirtschaft/was-taugt-die-eu-datenschutz-verordnung-13972055.html

This point was already pinpointed in the 2005 Report on Archives in the enlarged European Union. "Changing societal expectations of the roles of the archivist in the twenty-first century are activated by the increasing irrelevance of constraints of place, time, and medium in 'the age of access', made possible by modern information and communication technologies. These facts increase citizens' expectations of free access to authentic information 24 hours a day, seven days a week, wherever they happen to be."[60]

The anonymisation/pseudonymisation of personal data in archival material is not in itself very problematic. Yet there are at least two levels on which it leaves fundamental question marks:

1. Process level: The process of analogue anonymisation/pseudonymisation of personal data on archival copies seems to be a more or less trivial matter. This is probably the reason why it is not given closer consideration. However, this assumption is wrong. Even at this procedural level, one basic difficulty stands out: It is the time-consuming and laborious nature of the whole process of personal data anonymisation/pseudonymisation, in its analogous as well as digital form. To support this thesis, we conducted an empirical survey with colleagues from two archives to quantify the labour and time needed for anonymising/pseudonymising personal data in archival records. The research was conducted in two public state archives in the Czech Republic as one of the member states of the European Union, namely the State Regional Archives in Prague and the National Archives of the Czech Republic. Although this was a form of analogue pseudonymisation, many of the steps, and the overall time and effort involved are similar for digital pseudonymisation as well. This will be the case at least until artificial intelligence tools are applied to a more substantial extent for digital pseudonymisation, which is not yet happening to any significant extent in the archival environment.

The following calculation and list of the individual steps necessary for the processing of personal data in archives thus represents an insight into

[60] *Report on Archives in the enlarged European Union. Increased archival cooperation in Europe: action plan*. (2005). Office for Official Publications of the European Communities. https://ec.europa.eu/transparency/regdoc/rep/1/2005/EN/1-2005-52-EN-F1-2.Pdf

the archival practice of one of the EU Member States, but the calculations concerning some of the actions, especially the process of data pseudonymisation by means of blackening out copies of archival records, are more or less universally valid.

The first step is simply to copy the archival record including the arrangement and preparation of the copies for the research room. The State Regional Archives in Prague performed their calculation on a sample of two boxes. The first box contained material on the Regional Committee of the Communist Party of Czechoslovakia (minutes of the Board), which took a total of 4 hours. The second box contained records from the Extraordinary People's Court in Prague fonds and represented a full 10 hours of work. This step of preparation of judicial materials is considerably more time consuming.

What is the time required for the actual redaction of the copies (blacking out)? The State Regional Archives in Prague based their calculation on a sample of two boxes from the same fonds. Pseudonymisation of materials from the Regional Committee of the Communist Party of Czechoslovakia (minutes of the Board) took 3.25 hours per box of records, while pseudonymisation of archival materials from the Extraordinary People's Court in Prague involved 9.75 hours of work per box of records. Pseudonymisation of judicial material is significantly more time consuming due to the enormous amount of (sensitive) personal data.

The cumulative time devoted to anonymisation/pseudonymisation (not including time for research and other activities related to the preparation of the records for researchers), including the preparation of copies, ranges from 7.25 to 19.75 hours of work on a single box.

A similar empirical survey was carried out in parallel in the Czech National Archives.[61] The results are almost identical. It took 6.2 hours to make copies of one box containing records from the Central Committee of the Communist Party of Czechoslovakia, and another 8.2 hours to pseudonymise them. It then took much longer for the same tasks in the case of the fonds belonging to the State Court, which in the early days of the communist regime in Czechoslovakia in 1948–1953 conducted political trials with opponents of the regime and handed out death sentences in these politicised trials. In the case of these fonds, the copying and preparation for pseudonymisation took 13.2 hours, while the pseudonymisation

[61] The information is based on internal unpublished documents prepared by the archivist and chief methodologist of the National Archives of the Czech Republic, Karolina Šimůnková.

itself took 15 hours. The time required for pseudonymisation thus ranged from 14.4 to 28.2 hours of time per one box of records.

These figures, however, by no means cover the entirety of the work that must be devoted to preparing archival material to be "stripped" of personal data. This is a specific situation of the Czech archival system, which in this respect is rather unique in international comparison.

It is necessary to add to this the time that Czech archives—as required by Czech archival legislation—should devote to searching the Information System of Population Registration and determining whether the persons mentioned in the archival records are alive or not. Furthermore, archives should ask the living persons whether or not they agree to the disclosure of their personal data. The time and workload would be enormous, given that the archive would have to obtain all the necessary information (data from the population register, responses from persons whose personal data are included in the archival records), process it, organise all the associated agenda, and top it up by pseudonymisation. Given that a single cardboard file box often contains dozens or even hundreds of names of potentially living persons, the time-consuming nature of such work would be so great that it would become virtually unbearable for archives under current conditions. An exact empirical calculation of the time spent on the latter tasks could not be made. Based on cursory archival practice so far, only an estimate can be made of the total workload associated with the complete execution of the activities mentioned above, that is, to process a single carton would probably be close to 30 hours.

In addition to the financial requirements associated with the necessary staffing for these tasks, it is necessary to add the significantly increased costs associated with data pseudonymisation. This is particularly the cost of copying archival records before they are pseudonymised. In this case it is also remarkable to look at the specific empirical figs. A single box of post-1945 modern records contains on average 750–1000 sheets, most of which would have to be copied, in some circumstances even twice due to 100% blacking out of the information.

2. The second level, on which the anonymisation/pseudonymisation of personal data in archival records may seem controversial, is the content: The actual core of the problem of irreversible anonymisation and, from the perspective of the researcher, reversible pseudonymisation of personal data lies in the fact that at the end of the process, the applicant, including historians and other scientists,

> receives material devoid of specific links to specific persons and historical actors, material that is, so to speak, "depopulated". The implications not only for historical research and understanding of our past, and therefore ourselves, are enormous in such a case. Apart from this chapter, Chap. 5, also discusses some specific examples.

In the future, it remains open to what extent and in what situations archives—both public and private—will approach the pseudonymisation of personal data in the process of making archival material available to the public. Provisions on pseudonymisation are gradually being incorporated, for example, into donation agreements between record donors and public and private archives; the latter can be demonstrated by the example of the German Archives for the History of Psychoanalysis.[62]

Even at the legislative level, there has been a gradually increasing pressure to enforce the principle of data minimisation, especially in the form of breaking the link between data and its specific carrier. In a stronger form, data minimisation represents the tool of irreversible data anonymisation; in a weaker form it represents data pseudonymisation. It is not just the European GDPR that has come up with the principle of data minimisation and the requirement to break the links between the data and their subjects. For example, in Germany, at the federal level, the Data Protection Act of 2017, as part of the process of transforming the GDPR principles into German legislation, established an obligation of maximum "data economy" ("Datensparsamkeit"), meaning that "as few personal data as possible" should generally be processed.[63] At the same time, this legislation seeks to promote the application of the process of anonymisation of personal and especially sensitive personal data (in the diction of the GDPR special categories of personal data). However, it explicitly mentions anonymisation in the case of research and statistical purposes, but does not mention anonymisation in the case of archiving in the public interest.[64]

[62] The contractual relationship between the German Archive for the History of Psychoanalysis and the donors is demonstrated by a model contract here: http://www.archivverein-psychoanalyse.de/pdf/donatorenvertrag.pdf

[63] "Insbesondere sind die Verarbeitung personenbezogener Daten und die Auswahl und Gestaltung von Datenverarbeitungssystemen an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu verarbeiten. Personenbezogene Daten sind zum frühestmöglichen Zeitpunkt zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verarbeitungszweck möglich ist." Bundesdatenschutzgesetz, § 71 (1).

[64] Bundesdatenschutzgesetz, §§ 27–28.

However, it is unlikely that archives would choose the "hard" irreversible anonymisation of personal data in archival materials by eliminating them directly from the original. The vast majority of archivists are people educated in fields close to historical sciences. They look at archival sources from this "distant perspective" and broad horizon. They do not view archiving through the media lens of "close perspective", topicality, and "fast-moving time", let alone through the eye of a tabloid looking for all sorts of juicy titbits the material may contain. On the contrary, archivists, in the process of creating archival-historical sources, seek to preserve and allow to emerge a formative reflection of reality, society, and culture, and to establish this in a tradition that will be passed on to future generations. However, this reflection and mirror of reality, the basis of historical consciousness and individual and social memory, and at the same time one of the important pillars of the formation of human civilisation and culture, would be fundamentally reduced, bent, and shifted in its message were it not for certain specific people and their traces preserved in historical sources. The depth of tradition, the understanding of our past and the understanding of man himself would be seriously compromised.

It is a completely different question whether and in which cases the path of "hard" irreversible anonymisation will not be chosen for records moments before their archiving and their hypothetical transfer to a public archive. In Chap. 7, I have used census records to provide an international comparison of the situation of irreversible anonymisation of personal data in records in the moment before being archived.

The difference between the irreversible "hard" anonymisation and the reversible "soft" pseudonymisation of data correlates with the proposed model of the four categories of the right to be forgotten, which I first introduced in Chap. 5. The proposed concept of the four categories of the right to be forgotten (1. temporary limited, 2. temporary absolute, 3. permanent limited, 4. permanent absolute) suggests that in the case of such records and data for which it is necessary with regard to the protection of personality, privacy, and personal data to opt for the fourth and strongest category, that is, the "permanent absolute" right to be forgotten, neither archives nor purposes of archiving in the public interest should have the right to maintain these records and data; that should remain the fact even if such records would be completely exempt from the system of closure periods and remain closed. This applies to data that another German case law from the late 1980s, this time by the Federal Constitutional

Court,[65] referred to when it defined the inviolable sphere of personality rights. This case law then stood at the heart of the newly crystallised model of personality spheres. Alongside the social sphere encompassing in principle the public life of individuals, there is the private sphere comprising of the small circle of family and close friends and the private life in one's own home. And finally, there is the intimate sphere. Although it has not yet been precisely defined by the German Federal Constitutional Court, it has determined the existence of "an ultimate inviolable sphere of private life, which is absolutely separate from public power. Even serious interests of the general public cannot justify interventions in this sphere."[66] And it is in these cases that either irreversible destruction of the data in question or at least their irreversible anonymisation should be chosen as the surest way and means to ensure that this sphere is never breached and the extremely sensitive data it contains are never misused in the future—bearing in mind the fragility of today's democracies and the uncertain geopolitical constellation.

The time capsule tool the Australians and the Irish use for archiving census records as analysed above, belongs to the second category of the "temporary absolute" right to be forgotten. The relevant data are closed and access to them is completely restricted, but only for a limited period of time. In the case of this "temporary absolute" right to be forgotten, there is no need to use either the pseudonymisation or the anonymisation tools simply because the data are completely inaccessible for a given period.

However, a high percentage of the records maintained in public and private archives corresponds to the first category of "temporarily restricted" right to be forgotten, to which access for legitimate official purposes is allowed on a virtually permanent basis, but access for private purposes is prevented for various reasons (closure periods, personality and privacy protection, banking secrecy, classified information, etc.). This covers the vast majority of records maintained in public archives belonging to the group of records created after 1945. Records and archives falling under the "temporary limited" right to be forgotten represent by far the largest part of the material undergoing pseudonymisation, provided that its

[65] Bundesverfassungsgericht. Beschluss des Zweiten Senats vom 14. September 1989, 2 BvR 1062/87.

[66] Bundesverfassungsgericht. Beschluss des Zweiten Senats vom 14. September 1989, 2 BvR 1062/87. Cf. Chap. 2.

definition also includes the process of blacking out or other means of data redaction on copies and records.

The last and very high proportion of the content of archives (in the case of large state, provincial, regional, and similar public archives, this represents a significant majority of material) is archival material that is not subject to access restrictions for data protection reasons and that, based on our analyses, is not subject to the right to be forgotten in any of the four categories. Moreover, in the vast majority of archives, the volume of maintained records increases continuously as more and more archival acquisitions are made.

There are four interconnected processes that are fundamental to the whole issue of access to archives and the protection and processing of archived data. The first two are the process of "ageing of archives and data" and the process of "disappearance of personal data" as people who have left their mark on archival sources gradually pass away. Most archives across countries are based on the principle of continuous acquisition of new materials as more and more records are created and transferred to the archives; these archives should thus experience a continuous increase in the group of materials exempt from all the categories of the right to be forgotten.

This corresponds to the third process of disappearance or transformation of personal data sensitivity. It is ultimately linked to a fourth process, which I briefly mentioned above and which is discussed in more detail in Chap. 2. It is the process of weakening of post-mortem protection of the personality rights of the deceased, which the German Federal Court of Justice aptly described in the cited judgement—paradigmatic also for the subsequent development of the interpretation of the post-mortem personality protection—and stated that the need to protect the rights of the deceased that "disappears as the memory of the deceased fades".[67]

All of this certainly does not mean that the right to be forgotten has been radically marginalised in archives over time. Not only will "young" records always represent a significant part of the content of the archives in terms of volume, but it is also true that the "youngest" of the records belong among the most attractive for researchers, analogous to the interest of historians in "young history". Similarly, there is a significant percentage of requests for access to archival material that touch on people's private and, in a number of cases, intimate spheres. Archives will therefore

[67] Bundesgerichtshof. Urteil vom 20. März 1968, I ZR 44/66.

still have to take into account in which respects the right to be forgotten manifests in any particular case and which category of the proposed system of the right to be forgotten comes into play. Archives should then act accordingly and decide on the manner of access to the relevant archival records.

8.2.3 Deanonymisation and Reidentification

Ultimately, archives will have to increasingly consider the growing risks of deanonymisation of anonymised or pseudonymised personal data and reidentification of individuals. These risks are manifested in the vast majority of cases in the area of digital data and records and at the level of their digitally pseudonymised or anonymised form. In principle, however, they can also be applied to analogue records and analogue pseudonymisation or anonymisation. On the one hand, various anonymisation and pseudonymisation techniques are being developed, which are not yet used to any significant extent in and by the archiving sector, even taking into account the fact that "hard" anonymisation of data in archival materials is opted for only exceptionally. On the other hand, tools for data deanonymisation and reidentification of individuals are being improved. The Working Party on the Protection of Individuals with regard to the processing of personal data has identified three risk areas for successful anonymisation or pseudonymisation.[68]

The first area is the so-called singling out, that is, the ability to isolate a particular group or all records that are linked to and identify a particular person in a given data set. The second risk area is "linkability", where two or more records relating to a particular person or group of persons can be linked, whether from one or more data sets. The third risk is "inference" by which it is highly likely to derive the value of an attribute from the values of a set of other attributes and thus deanonymise the data. The means used to prevent deanonymisation and reidentification of individuals should then tackle these three risk areas.

It is neither the aim nor the scope of this text to provide a detailed analysis of the various anonymisation/pseudonymisation techniques. It can briefly mention the systematisation of two groups of anonymisation/pseudonymisation techniques applicable to data sets presented by the

[68] Article 29 data protection working party. (2014). Opinion 05/2014 on Anonymisation Techniques, pp. 11–12.

Working Party.[69] The first is "randomization", which consists in changing the credibility of data whose certainty is disturbed by introducing an element of randomness. If the data uncertainty is sufficiently significant, it can no longer be linked to a specific identifiable person. These techniques include, for example, noise addition, by which attributes in a data set are altered and the resulting data set is less accurate, but the overall data assignment is preserved. It also includes the permutation technique that swaps the attribute values and in some cases assigns them to be carried by different subjects than in reality. Randomisation techniques also include differential secrecy due to which the resulting data set contains some random inaccuracies that are additionally assigned. The second group of anonymisation techniques applicable to data sets is "generalization" which generalises certain subject attributes. For example, the original data set territorial reference to a municipality is extended to a region. This expands the set of potential carriers of the relevant data and makes it more difficult to identify them.

Currently, there are many cases pointing to the real risks of deanonymisation of anonymised or pseudonymised personal data and reidentification of individuals. There are studies that empirically demonstrate the real possibilities of deanonymisation using specific cases and data sets. For example, Bradley Malin, using the IdentiFamily software program, demonstrated the possibility of linking depersonalised family ties to specific individuals and the possibility of reconstructing large-scale genealogies within the current population from available online sources, typically from the media space, obituaries, and the like.[70] In a remarkable study, Luc Rocher, Julien M. Hendrickx, and Yves-Alexandre de Montjoye attempted to quantify the probability of correctly reidentifying a particular person including very incomplete data sets.[71] They created a model in which they estimated the degree of individual uniqueness. In the case of the American population, they concluded that 99.98% of Americans can be correctly reidentified in any data set using 15 demographic characteristics. Their conclusions point to weaknesses in some of the current standard anonymisation methods.

[69] Ibid., pp. 12–19.

[70] Malin, B. (2006). Re-identification of Familial Database Records. *AMIA Annual Symposium Proceedings Archive* 2006, 524–528.

[71] Rocher, L., Hendrickx, J. M., de Montjoye, Y.-A. (2019). Estimating the success of re-identifications in incomplete datasets using generative models. *Nature Communications*, 10, 3069. https://doi.org/10.1038/s41467-019-10933-3

Arvind Narayanan and Vitaly Shmatikov have developed and introduced an algorithm for people-centric reidentification of social media data.[72] In doing so, they demonstrated that one-third of users with both a Twitter account and a Flickr account can be reidentified on an anonymous Twitter graph with an error rate of only 12%. The operator mistakenly assumed that the pseudonymisation they carried out—typically when selling the data to other entities, in particular for advertising and marketing purposes—prevents any reidentification. Narayanan and Shmatikov showed that pseudonymisation was not a sufficient guarantee in this case. Reidentification was enabled by means of relationships between different persons that are unique and can be used as an identifier. Their study is one of a number of those that prove that pseudonymisation of personal data and anonymity in social media environment is merely fictitious and not sufficient to protect privacy.

Narayanan and Shmatikov address the topic of deanonymisation and reidentification comprehensively and using concrete examples they demonstrate other ways in which supposedly anonymous data can be reidentified after they had been anonymised/pseudonymised. They applied the deanonymisation method to the Netflix Prize database containing movie ratings from 500,000 Netflix subscribers.[73] Using data from the Internet Movie Database, they identified Netflix records related to identified users. In doing so, they revealed, among other things, their political preferences and other potentially sensitive data.

The "Unique in the crowd: The privacy bounds of human mobility" study is a significant contribution to the field of reidentification.[74] The authors focused on the question to what extent it is possible to reidentify individuals by using information on the movements of persons. They performed a unicity test to verify how many points in terms of spatio-temporal traces a person must leave in order to uniquely identify the mobility trace of an individual. The data that can be used for the purpose of reidentification usually include data from various public sources such as the address of

[72] Narayanan, A., Shmatikov, V. (2009). De-anonymizing Social Networks. *2009 30th IEEE Symposium on Security and Privacy*, 173–187. https://doi.org/10.1109/SP.2009.22

[73] Narayanan, A., Shmatikov, V. (2008). Robust De-anonymization of Large Sparse Datasets. *2008 IEEE Symposium on Security and Privacy* (sp 2008), 111–125. https://doi.org/10.1109/SP.2008.33

[74] De Montjoye, Y.-A., Hidalgo, C. A., Verleysen, M., Blondel, V. D. (2013). Unique in the Crowd: The privacy bounds of human mobility. *Scientific Reports*, 3, 1376. https://doi.org/10.1038/srep01376

residence, the address of employment (usually it is the address of residence or employment that is known about the person), geolocation data provided directly by the person concerned, and so on. The authors based their research on a data set of 1.5 million individuals, the vast majority of whom moved within 100 kilometres, over a period of 15 months. They then concluded that only four spatio-temporal points are sufficient to uniquely identify 95% of individuals and two randomly selected spatio-temporal points allow for the identification of more than 50% of individuals. Based on the findings, a general conclusion can be drawn stating that "mobility traces are highly unique, and can therefore be reidentified using little outside information". Similarly, another study demonstrated that mobile phone data can be reidentified by means of the user's top locations.[75] Deanonymisation via geolocation data is becoming both one of the increasingly common tools of data misuse and a hot research topic.[76]

However, the risks of deanonymisation and reidentification are becoming highly attractive and intensively researched topic on multiple levels. Very recent research has demonstrated the possibility of deanonymising data by using records on music preferences and selections by the users of various streaming services. It has revealed the possibility of reidentifying users based on these records, albeit stored in anonymised/pseudonymised form.[77] In a similar context, specific models for assessing the risks of data reidentification (including the use of quantifications based on available statistical data) in mobile applications are being developed, both by public authorities and by citizens themselves, with the aim to evaluate the specific level of risk of data reidentification and privacy leakage risk.[78]

In recent years, some (personal) data protection authorities have already started to include a general reidentification risk assessment in their

[75] Zang, H., Bolot, J. (2011). Anonymization of location data does not work: a large-scale measurement study. In *MobiCom '11: Proceedings of the 17th annual international conference on Mobile computing and networking*. September 2011, 145–156. https://doi.org/10.1145/2030613.2030630

[76] Cf., for example, Gambs, S., Killijian, M.-O., del Prado Cortez, M. N. (2014). De-anonymization attack on geolocated data. *Journal of Computer and System Sciences*, 80(8), 1597–1614. https://doi.org/10.1016/j.jcss.2014.04.024

[77] Hirschprung, R. S., Leshman, O. (2021). Privacy disclosure by de-anonymization using music preferences and selections. *Telematics and Informatics*, 59, 101,564. https://doi.org/10.1016/j.tele.2021.101564

[78] Yang, Z., Wang, R., Luo, D., Xiong, Y. (2020). Rapid re-Identification risk assessment for anonymous data set in mobile multimedia scene. *IEEE Access*, 8, 41,557–41,565. https://doi.org/10.1109/ACCESS.2020.2977404

methodological recommendations for the management of (personal) data, containing an analysis of the potential risks of data deanonymisation and reidentification of persons.[79] It focuses mainly on situations in which the data custodian intends to disclose or publish anonymised data. In such cases, the custodian should analyse the hypothetical risks of future deanonymisation and reidentification of persons and carry out a reidentification risk assessment to ensure an adequate protection of personal data, personality rights, and privacy. Archives and archiving should take inspiration and incorporate data reidentification risk assessments into their records management processes.

To sum up, it is not possible to perceive anonymisation as a perfectly effective irreversible act of destruction of certain data, or of the link between the data and their carriers. Data custodians, which of course also includes archives, should take the risks involved seriously. The digital world, including digital data management and archiving, has significantly increased the risks of data misuse. Access to data has been greatly facilitated, especially with the possibility of remote online access. Technological advances and, in particular, the expected development of artificial intelligence capabilities increase the risks of deanonymising anonymised or pseudonymised data and reidentifying individuals. This context should be given substantial consideration, particularly at the level of the application of the principle of data minimisation and storage limitation, including in the field of data archiving.

[79] Cf., for example, Canadian Information and Privacy Commissioner of Ontario. (June 2016). *De-identification Guidelines for Structured Data*. https://www.ipc.on.ca/wp-content/uploads/2016/08/Deidentification-Guidelines-for-Structured-Data.pdf, p. 22. Similarly in Australia see the Office of the Information Commissioner Queensland. (2020, 9 July, last updated). *Privacy and de-identified data. Guideline Information privacy act 2009.* 1 February 2019. https://www.oic.qld.gov.au/__data/assets/pdf_file/0007/38644/Privacy-and-de-identification.pdf. Similarly in Victoria, Australia: Chief data officer. (2018, 21 February). *De-identification Guideline.* Issued by the Chief data officer on 21 February 2018 under section 33 of the Victorian Data sharing act 2017. https://www.vic.gov.au/sites/default/files/2019-03/Victorian-Data-Sharing-Act-2017-De-identification-guidelines.pdf

8.3 Conclusion

Data minimisation and storage limitation in relation to archives and archiving are implied by an underlying question that is also decisive for the specific field of data retention: What data on their citizens the state and public authorities have the right to maintain and exploit, taking into account the need to ensure the basic functions of the state, local government, necessary internal security, the administration of justice, and other public interests. Patrik van Eecke and Peter Craddock described this situation succinctly—albeit in relation to the European GDPR, but the statement is generally valid for archives: "the main challenges to public archives are not whether data needs to be erased, but how to ensure that only the personal data that is truly necessary is processed and that personal data is anonymised or at least pseudonymised where possible".[80]

The principle of data minimisation and storage limitation in the context of the protection of (not only) personality rights, privacy, and personal data in the area of archiving and records management is based on a fundamental tension in which on the one hand, the state, public administration, and public authorities need to acquire and store a set of certain data on citizens to ensure their basic functions and, on the other hand, they need to deal with the ever increasing risk of misuse of such collected, stored, and possibly archived data. I have outlined some of the possible tools by which records management and archiving in particular can respond to this tension and seek outcomes that are consistent with a democratic legal order and that balance the polarised scales as much as possible. The conclusion of the book will then provide a set of recommendations that may be implemented in archival and records management practice, and will summarise the conclusions of the analyses conducted in this book.

The principle of data minimisation in the field of archiving and preservation expresses two interrelated basic issues: What data can the state, public authorities, and society have the right to keep on their citizens and, where appropriate, what data they can preserve permanently or for a very long time.

The book has asked questions about the risks to data, personality, and privacy protection in situations when data are stored and, in specific cases,

[80] Van Eecke, P., Craddock, P. (2018). The right to be forgotten … and to remember (section Conclusion and Recommendations). In K. Van Honacker (Ed.), *Right to be forgotten vs the right to remember: data protection and archiving in the public interest.* VUBPRESS Brussels University Press.

archived. This tension, however, reflects one of the paradoxes of archiving: On the one hand, the very act of storing data, especially personal data, poses security risks of potential misuse, typically in the form of ransomware. On the other hand, archiving serves in certain cases as one of the tools of data protection and even as one of the defences against the risk of data theft and leakage, including some types of ransomware attacks, especially those that block access to data. In this case, appropriately configured processes of archiving and storage backups (including the important issue of the frequency of such backups in the form of archiving) outside the information systems of the creator, that is, in an archive, can under certain circumstances enable the recovery of the blocked data.

The tension also demonstrates on an economic level. On the one hand, any retention of personal data poses a potential risk of negative economic consequences for data controllers in a situation in which data protection is breached and, for example, blackmail occurs. On the other hand, data represent the imaginary "black gold" of the twenty-first century and are a source of profit for the private and, by extension, the public sector.

Based on the performed analyses, the relationship of the archival sector and archiving to the process of minimisation and storage limitation of (personal) data, can be summarised into several important and decisive moments.

Although the analyses have provided indications of a gradually decreasing percentage of records transferred into archives for permanent retention, relative to the records determined by the process of archival appraisal for permanent destruction, the continuously increasing volume of archived materials represents a constant (cf. Chap. 6) that needs to be taken into account in the context of the issue of data minimisation.

Public archives created less than approximately 100 years ago, or public records with archival potential, contain mostly personal, including very sensitive, data of living persons. This applies to archival material during the initial phase of its existence, when it relates to individuals who are still alive. This phase corresponds approximately to the average probable life expectancy, which gradually increases, and this trend is likely to continue (barring any other serious epidemic situations such as the COVID-19 pandemic or other catastrophic social developments). Archival records at this stage, during which they relate to living persons, are subject to a significant risk of misuse of the personal data of those concerned in them.

At the same time, the archiving process bears a feature that I refer to as "disappearance of personal data", if we understand personal data as data

relating only to living persons. In view of the fact that archives are destined for permanent preservation, the proportion of deceased individuals concerned in the archives in relation to the living increases over time. This is another important process that takes place within data archiving, and which can be described, again using some literary hyperbole, as the "ageing" of archives and data. Closely related to this are two other processes that occur during archiving, namely the disappearance or transformation of personal data sensitivity and the weakening of post-mortem protection of the personality rights of the deceased. These four formative processes will be discussed in more detail below and in the final section "Recommendations".

On the other hand, archives constantly acquire more material, with a significant share of records subject to shorter retention periods; very frequent is the period of five years after the record is closed. These are very young records, which will often carry information about living persons for almost 100 more years. Archiving in the public interest will therefore have to deal with the preservation of personal and sensitive personal data of living persons in the future as well.

A principle paradigmatic for the relationship between archiving and data minimisation is embodied in the European GDPR: If it is possible to erase the specific identity of a person, provided that the public interest of archiving, together with the purposes of historical research and statistical purposes are not compromised, there is an obligation to perform such de-identification. However, this general rule is not in itself a solution to the whole problem. On the contrary, archiving stands before a key question and a very wide room for interpretation: How and according to what criteria to determine whether the purpose of archiving in the public interest can be fulfilled in the case of specific groups of records, even in case of irreversible loss of personal identifiability. It remains equally important and open to answer who will assess this issue, whether it will be, for example, expert bodies, who will nominate the members, and how apolitical and professional decision-making will be ensured.

Records management and archives play an important role in the application of fundamental human rights. First, it is the right to know, the right of access to information and records, and second, the protection of privacy and personality rights.

There is a fundamental tension not only between data minimisation and its relation to data preservation, but within archiving in its entirety: On the one hand, the best protection for any data is their irreversible

destruction. To put it the other way round using the words of the Court of Justice of the European Union interpreting the impact of general retention of traffic and location data: "the mere retention of that data by the providers of electronic communications services entails a risk of abuse and unlawful access".[81] Similarly, in order to protect privacy, personality, and personal data, it is usually most effective to simply irreversibly destroy the potentially or actually sensitive data. The "Archive of National Socialism" ("NS-Archive") analysed above—which the East German communist dictatorship used to coerce, compromise, and blackmail own citizens as well as those from "enemy" countries—demonstrated how easy it is for the public authorities to massively misuse sensitive data on people if such data are preserved. One of the fundamental pillars of official legal records destruction that occurs as a part of archival appraisal resonates with the intent to destroy sensitive and potentially exploitable personal data; it is the condition that a record that had been through the process of archival appraisal and had been destined for destruction should be irretrievable.

On the other hand, for a specific individual as well as for the functioning of the whole state and society, it is absolutely necessary to preserve certain data for a certain period of time, which can sometimes be very long and extend over several decades, and possibly even to a hypothetically infinite period of time; and this is the moment archives enter the field with the vision of (feasible?) permanent data archiving. In a slightly different perspective, but in a similar circle, is the right to know, the right of access to information and records, a right no functioning and free society can do without.

The tension and the need to balance between the need to preserve and the need to destroy/not preserve is a defining motive far beyond data management and archiving. This applies to inanimate as well as to animate structures. However, while psychology more often focuses on how memory works and how to maximise its potential, and sees forgetting as a kind of necessary and rather distracting pendant,[82] philosophy has been able to take the phenomena of memory and forgetting further in many respects, in some cases equating them and defining them as somewhat equal

[81] Judgment of the Court (Grand Chamber) 6 October 2020 in Case C-623/17, par. 73.

[82] However, this is not always the case. On the need of memory and forgetting in relation to data archiving and knowledge management, cf., for example, *Vernichten um zu bewahren? Détruire pour conserver? Distruggere per conservare?* (2016). Arbido, 3. https://arbido.ch/assets/files/arbido_2016_3_low_161127_132457.pdf. For example, Preissmann, D. (2016). Mémoire et oubli: un éclairage de la psychologie et des neurosciences, *Arbido* 3, 4–7.

partners. Friedrich Nietzsche expressed this in the second half of the nineteenth century when he addressed the relationship between knowledge and life and the function that history (historical science) fulfils or should fulfil for the performance of life. He asked himself what is the relationship between the past, its knowledge and life itself.[83] (Historical) knowledge does not exist by itself, but always relates in some way to life and must be judged as such. The question of knowledge is as important as the question of life. Nietzsche asks what (historical) knowledge is to life, what life needs it for, and what place knowledge should occupy in it. Life is constantly threatened by excess of knowledge that could ultimately destroy it. In this respect, it is necessary to set reasonable boundaries so that life is not stifled or outright destroyed by "the explosion of knowledge". If we translate this for the purpose of our research, a lot of data and records must be destroyed and not preserved, "forgotten" as a sine qua non condition for the possibility of preserving, processing, and making meaningful use of that tiny and most valuable part of the created data.

The second crucial point is a level on which balancing is or should be taking place. Data preservation and especially long-term archiving should seek a balance between the two positions: On the one hand, it is a constant, unchanging protection of some basic values and layers of an individual's rights, personality, and privacy. On the other, there is the phenomenon characterised and defined as early as 1968 by the German Federal Court of Justice giving the definition of post-mortem protection by means of direct proportionality: the need to protect the rights of the deceased "disappear as the memory of the deceased fades".[84] Post-mortem personality protection is not, according to this judgement—which foreshadowed the subsequent case law of the German courts up to the present day—"timeless". In other words: Just as the memory of the deceased gradually fades, the protection of the personal data, personality, and privacy of the dead should weaken and diminish proportionally. This includes two abovementioned processes: namely the disappearance or transformation of personal data sensitivity and the weakening of post-mortem protection of the personality rights of the deceased. A specific example illustrating the "disappearing

[83] Nietzsche, F. (1988). O užitku a škodlivosti historie pro život [On the Advantage and Disadvantage of History for Life]. In: F. Nietzsche, *Nečasové úvahy* [*Untimely Meditations*]. Athenaeum, 83–171, here, for example, pp. 87, 105–107, 168. Nietzsche provides a different perspective on the relation between life and knowledge in Nietzsche, F. (2001). *Radostná věda* [*The Gay Science*]. Aurora, § 110, pp. 104–106, § 324, p. 170.

[84] Bundesgerichtshof, Urteil vom 20. März 1968, I ZR 44/66.

sensitivity" of data in records and archival materials, or the transformation of the nature of their sensitivity, is the history of the so-called fichiers juifs in France, which I have discussed in detail in Chap. 7 in Sect. 7.3. It is therefore necessary to consider the "ageing" of archives and data as it relates to people who died some time ago and that time gets more and more distant. This process and the post-mortem protection of personality in general are discussed in Chaps. 2, 3 and 4.

Let us apply this balancing act to one specific example from the history of European civilisation: For example, information about the intimate life of the Roman emperor and Czech king Charles IV, who died almost 650 years ago, should be subject to the same protection of the most intimate privacy sphere as is the case with the same categories of data about, say, Václav Havel, who died in 2011, a dissident fighting against the communist regime in the former Czechoslovakia and the first president of the state free from the communist-Soviet control. Their "hacking" would result in exactly the same tabloid-like gossip, whether it concerns a long-dead emperor or a recently deceased president. It is still a case of breaching the protection of the most intimate privacy sphere, whether concerning 500-year-old or 1-day old data. This protection should never be broken. On the contrary, however, in the case of other data, which are currently often classified as sensitive personal data, such as health or ethnic origin, the more than 600-year-old information relating to Charles IV is not equal in sensitivity to the same information relating to Václav Havel. After all, in the case of philosophical beliefs, religious beliefs, and the like, the sensitivity of the information of these two public figures is practically no different, and in both cases it is an area open to the public.

Data minimisation and storage limitation should take account of this context, which applies to both phases of their "life"—that is, during its "active life",[85] whether in the context of records management or specific

[85] Under the traditional concept of the records life cycle, as developed, for example, in the classic form of the "three ages of documents" ("trois âges des archives") by the French archivist Yves Pérotin in the early 1960s. He divided records/archives into "active" ("actives" or also "courantes"), as they are created by the administration and used by it on a daily basis; "semi-active" ("semi-actives" or "intermédiaires"), which have not completely lost their administrative function, but which cannot yet be destroyed or transferred to the archives, and finally, "definitive" or "historical archives" ("archives définitives" or "historiques"), which have practically lost their administrative value and have instead acquired historical value (indeed, in France, the term "definitive" or "historical archives" is also used in this sense for the records as such). Cf. the famous essay by Pérotin, Y. (1961). L'administration et "les trois âges" des archives. *Seine et Paris*, 20 (October), 1–4.

individuals, as well as in their post-archiving phase. Respectively, an essential moment of the process of data minimisation and limitation of their storage happens just at the borderline, at the transition between "active life" and their "passivation" during the retention period and archival appraisal, during which the absolute largest part of records and data is destroyed and the remaining minority—as I demonstrated in the first part of this text—is transferred to the archive for permanent archiving.

We may begin to see that the inclusion of the possibility of granting consent to the maintenance and archiving of personal and sensitive personal data repeatedly comes to light as one of a number of tools for finding balance between the need and right to remember together with the right to know and, on the other hand, the right to be forgotten and the protection of personality and privacy. Some countries have already implemented the first steps towards making the archiving of public records containing sensitive personal data in the public interest subject to the consent of the person concerned in them. I have demonstrated this using the example of census records in Australia and Ireland and their archiving inside time capsules, with absolute restriction of access to their contents for 99 and 100 years respectively. Only the census records of citizens who gave their explicit consent are archived; at the same time, these people were given the opportunity to include a personal message to future generations. This, in a way, manifests something I would call the "right to be remembered" as a kind of counterpart to a right a person can claim, that is, the "right to be forgotten". It is the right of man to leave a certain memory, an imprint in reality, and to preserve and care for it in such a way that it will be distinct even after many decades and centuries. The model of archiving census records in Australia and Ireland demonstrates the combination of these two rights on two levels: (1) the freedom of choice of citizens to preserve their data is introduced; (2) in the case of consent to archiving, the right to be forgotten is effectively applied for the first 99 and 100 years respectively by means of an absolute restriction of access to these data. After this period, the records are opened and the right to be remembered is activated.

The final chapter concludes the whole book by summarising a set of recommendations that I view as suitable for implementation in archival policies on data minimisation and storage limitation in the context of protecting (not only) personality rights, personal data, and privacy of those who have left their traces in archival records.

Conclusion

"Consider the cattle, grazing as they pass you by: they do not know what is meant by yesterday or today, they leap about, eat, rest, digest, leap about again, and so from morn till night and from day to day, fettered to the moment and its pleasure or displeasure, and thus neither melancholy nor bored."[1]

In the deepest foundations of archives and archiving there is a cornerstone whose mission is to counter the attachment to that fleeting moment of which Friedrich Nietzsche wrote when he asked about the role history should play in human life. Indeed, one of the first and perhaps the most important step in the history of man, civilisation, and culture was the moment when man recorded information in order to preserve it for further use. In a sense, archiving, as it developed in modern times, represents the ultimate form of this endeavour, as across countries and continents, almost without exception, its fundamental pillar still rests on the fact that archives maintain their records not temporarily but permanently. This moment is also reflected by archives taking enormous care of the physical condition of the archived material. That is to say if the archival material does not decay physically or digitally, it should "live forever".

However, the sole act of data preservation and archiving would be completely nonsensical and pointless, preserved or archived information

[1] Nietzsche, F. (1997). On the uses and disadvantages of history for life. In: F. Nietzsche, *Untimely meditations*. Cambridge University Press, p. 60.

M. Čtvrtník, *Archives and Records*,
https://doi.org/10.1007/978-3-031-18667-7

no one could ever access, would lose its meaning. The preservation and archiving of data must necessarily go hand in hand with making the data available. This, of course, does not mean providing immediate access to the whole public; it means setting the policy of access to information maintained both in active records management and in the archiving phase.

On the other hand, as many of the examples provided in this book demonstrate, any preservation of information, even for a fleeting moment, always poses a potential risk of misuse. The same risk is present in any case of opening access to information. These threats spread over several different levels. Most serious, however, is the risk of data misuse against an individual if it violates the protection of their rights, privacy, and sensitive personal data. Often, such a violation constitutes a threat to life itself and the quintessential rights of an individual, as the book has shown in some of the striking cases of data misuse in the twentieth and twenty-first centuries. The provided detailed analyses dealt, among other things, with the misuse of data from census, medical records, Jewish registries, as well as some others.

This book concentrated mainly on the relationship between, on the one hand, the need to preserve and open access to data, primarily in the specific field of public records management and archiving in the public interest, and, on the other hand, the concomitant need to protect these data. The main focus remained on the protection of personal data or the protection of personality rights and privacy. As Chap. 4, showed, there is a specific paradox within which archives and archiving exist: Archiving itself poses a potential risk to the protection of (not only) personality rights and privacy, and yet, it represents one form of protection of the very same (not only) personality rights and privacy.

The book provided a look at the protection of personal rights and human privacy in the field of archiving in the public interest and public records management in a broadly comparative international perspective. Based on the provided comparisons, it intended to distil a set of recommendations and, in some respects, principles that might in one form or another be implemented in the policies of records management and archiving in the public interest. Given the need to look away from the specific features of individual national legal systems and their systems of records management and archiving in the public interest, these recommendations and principles had to generalise to a certain extent. Nevertheless, they compile a corpus of recommendations and principles applicable in practice.

The protection of (personality) rights and privacy in the perspective of archives is divided into two main branches: One of them is pre-mortem and the other is post-mortem protection. While pre-mortem protection concentrates primarily on the level of protection of personal and sensitive personal data—which legal systems mostly link to living persons—and is usually regulated by legal systems by means of laws concerning personal data protection in general or data protection, post-mortem protection extends beyond the life of a person. Among the institutions focusing on the care of records, it is archives and archiving where the post-mortem protection of rights and privacy acquires one of the most prominent positions. This is due to the fact that the overwhelming majority of archive content consists of materials containing information about the deceased.

Archives, however, have one more specific feature. They spread between pre-mortem and post-mortem protection, bridging and connecting the two domains. This significance is enhanced by the fact that archival materials also undergo a transition from pre-mortem to post-mortem protection during the archiving process. Archives continuously take over records that are currently being created and which thus, during the first phase of their existence in the archives, contain information about living people. Over time, as archival records "age", the individuals concerned in the records die and pre-mortem protection of their personal rights and privacy transforms into post-mortem protection; the nature of the protection of the data contained in these records also changes. It weakens in some respects, sometimes it disappears completely, but on some levels it persists for a long time, even permanently. In Chap. 2, I mentioned the paradigmatic statement of the German Federal Court of Justice that the need to protect the rights of the deceased "disappears as the memory of the deceased fades".[2] However, at least for a certain period of time, some rights and forms of protection persist even after the death of a person, for example the protection of memory of the dead and their dignity, as the Federal Constitutional Court confirmed.[3]

Archives, as well as other institutions managing records in the long term, find themselves in this very complicated situation: they must assess

[2] Bundesgerichtshof, Urteil vom 20. März 1968, I ZR 44/66.

[3] Bundesverfassungsgericht, Beschluss vom 24. Februar 1971, Az. 1 BvR 435/68 ("Mephisto"); Bundesverfassungsgericht, Beschluss der 1. Kammer des Ersten Senats vom 22. August 2006, 1 BvR 1168/04 ("Der blaue Engel"); Bundesverfassungsgericht, Beschluss der 1. Kammer des Ersten Senats vom 19. Oktober 2006, 1 BvR 402/06.

not only the static form of protection of personal data, privacy, and personal rights, but also its dynamics. They must take into account its evolution and changes over time and adapt the settings of protection and access to these data accordingly. If these data controllers are to approach the task responsibly, they face a formidable challenge not only in the legal, but also in ethical and procedural fields. This dynamic occurs not only between pre-mortem and post-mortem protection, but also in the post-mortem protection itself. There is a difference between the protection of data from court materials relating to Joan of Arc, who lived in the first half of the fifteenth century, and the post-mortem protection of those murdered by the Russian Army in Russia's military aggression against Ukraine in 2022.

Where do archives, archiving, and records management stand in this design? How should they set up information protection and management processes, policies, and procedures for opening access to records and archives? Especially in Chaps. 2, and 3, the book sought, among other things, some models as well as legal and procedural tools that archives and records management implement in the protection of personal data, personal rights, and human privacy. Chapters 6, 7, and 8, addressed the question whether and how this protection can be implemented in the form of data reduction and minimisation, pseudonymisation, anonymisation, or in the form of retention periods. Archiving and records management move metaphorically in a magnetic field between the mutually interacting and colliding right to be forgotten and the right to be remembered together with the right to know in a broad sense. The forms these encounters and clashes take on were outlined in Chap. 5.

A significant common denominator that can be traced throughout this book is the escalating tension in which archiving, records management, and all information management currently exist. On the one hand, there is a growing social demand for information and open access to it; at the same time, the digital era has opened up an infinite space for the creation, dissemination, and consumption of information. On the other hand, contemporary society is beginning to pay an ever-higher tax for this benefit. We have witnessed increasingly massive leaks and misuse of data with ever more fundamental forms of violation of the protection of an individual, their personal rights, and privacy. While open access to information, its free creation, dissemination, sharing, freedom of speech and expression represent one of the key tools of open democracy, the rule of law and a free world, in certain contexts this tool can be transformed into the very opposite. It can hypertrophy, be misused, and become an instrument of

totalitarian power, injustice, unwarranted interference, surveillance, control, and manipulation of citizens. As a result, it can be used to destroy the democratic rule of law and open, free society.

How will archives, archiving in the public interest, and records management succeed in a world in which the individual, their personality, thinking, and inner self, as well as their private and intimate sphere, are facing increasingly harsh attacks from some states and private companies, in a world in which open and accessible data pose a considerable risk to these protected spheres of personality? In what forms will archives and records management continue to serve as an important tool for the preservation of a functioning democracy and the rule of law? What should the mechanisms and processes in archiving and records management be like, so as to support an open democratic society and the rule of law and do not become instruments of the very tendencies that threaten them? How should future legal systems, public policies, and specific procedural settings in public interest archiving and records management be modelled and transformed so that data preservation, archiving, and opening access to public records and archives serve the rule of law, free society, and democracy? This book intended to be a contribution to the debate in this field.

Recommendations

Archival systems usually assume a certain way of protecting the persons concerned in archival records, their rights, privacy, and, if necessary, also other legitimate interests. However, the instruments by which this protection is implemented and their specificity vary depending on the particular legislative system. Although as a rule, there are laws specifically regulating the protection of (personal) data, there is usually also special archival legislation that comments in some way on the protection of data concerned in the materials managed by archives and sets out rules for the processing and protection of personal data contained in archival records.

To conclude, I shall present a set of recommendations that can be made on the basis of the performed analyses and that seem suitable for application in archival practice and for possible implementation into archival legislation. The key starting point for most of the recommendations is the fact that introduces the whole text: The whole process of managing public records—from their creation to their final archiving—commences at a crucial moment: everything happens without the explicit consent of those concerned. Public administration collects the personal data of all of us

without our explicit consent and transfers them for permanent archiving, once again, without our consent. And finally, our consent still missing, our data are made available to researchers. In many cases, this happens during our lifetime, and after our death, we essentially lose control of the preservation and accessibility of our data completely. We do not know what data about us will be disclosed, to whom, and for what purpose, and it is not in our power to direct and control this process. This is extremely important for all archives' activities in the field of processing personal data in records and, in particular, providing public access to them. Of course, it is not the aim that every citizen should be completely free to determine what information about them is preserved, retained, and ultimately disclosed. However, archives should be aware of the absence of the proverbial consent of the person concerned and of the de facto impossibility for a person to express their free will and wishes as to how their data should be managed, both during their lifetime and after death. In a way, this is a reflection of the position in which Franz Kafka found himself in what is probably the best-known similar case, even though the records in question were not public but private. Although in his last will Kafka chose that practically almost all of his work and personal estate be destroyed, the executor of his will, Max Brod, violated his last wishes and instead of destroying the inheritance, Brod not only preserved it, but turned to publishing it.

Archives operate in this initial context and, in the absence of the imaginary consent, they should be all the more careful to preserve tact, discretion, and respect for an individual who, in all their many layers, with all their good and bad traits is reflected in records and archives.

1. Introduction of post-mortem protection of personality and privacy in the field of archiving and records management

For archival systems, it seems appropriate to introduce the above-analysed mechanism implementing the right of persons, including those deceased, which the French archivists Lemoine and Ricardo called (with a slight literary exaggeration) "temporary right to be forgotten" ("droit à l'oubli temporaire"). Sticking to literary imagery, I would suggest that this "temporary right to be forgotten" disappears gradually just as the proverbial tail of the comet in László Majtényi's image gradually disappears into the darkness of the universe, a comet that leaves a temporary trace in the universe, just as personality does not suddenly disappear with the person's biological death, but in a way persists, whether in the memories of loved

ones, in social memory and so on. However, as the German Federal Court of Justice and the Federal Constitutional Court ruled in the above judgements from the late 1960s and early 1970s, just as the memory of the deceased gradually fades in the memories of loved ones, so should the need to protect their personality rights. Post-mortem personality protection—as German judges put it—is not "limitless".

In relation to the archival field and expressed in prosaic terms: Archival law should incorporate, in an appropriate manner, mechanisms that allow for certain categories of particularly sensitive personal information to be subject to restrictions on access even after the death of the person concerned and do so for a limited period of time. The best tool seems to be the introduction of closure periods that would be in place for a certain period of time after the death of a person, as introduced, for example, by German archival law. However, with regard to the public interest in access to records and information, it seems to be more suitable to implement a system that introduces such closure periods only for certain categories of archival material and the information this material contains. In this respect, the French archival system appears to be the most progressive, having abolished the 30-year general closure periods in 2008 and retaining specific closure periods for selected categories of records.

There are, however, other tools for applying post-mortem protection, such as delegating the authority to assess the sensitivity of a deceased person's data to expert bodies and heads of archives managing the data in question. In such a manner, US legislation has left the authority to assess the sensitivity of personal data in this case in federal records potentially violating the privacy of living persons to the Archivist of the United States (i.e. the head of the National Archives and Records Administration, NARA). The Archivist may thus disclose such data in a situation when they decide that "enough time has passed that the privacy of living individuals is no longer compromised". The data protection system, including the archival sector in the United Kingdom, follows a similar line. Here, it mainly concerns the level of breach of the duty of confidentiality and it is the relevant data administrators, including archives, who decide whether disclosure would constitute such breach. In certain cases, this confidentiality also applies to information relating to deceased persons, typically in the case of medical records.

These protection tools are often combined in one way or another. Thus, in the USA, in addition to the authority of the head of NARA (in the case of records maintained at NARA), specific closure periods are in

place concerning personal and especially sensitive personal data. Similarly, France implements closure periods concerning access to data on a person's private life, though access can be requested before the expiry of these periods in certain exceptional cases. Such requests are then considered by a central ministerial body or a special Appeal Board.

2. Application of the right to be forgotten, restrictions on permanent archival storage, and the principle of archived data minimisation

In certain cases, the personality protection in archives and archival records should be able to implement the "right to be forgotten" on two basic levels. First, it is advisable to determine particular cases in which personal data contained in archival material shall never be disclosed to third parties, with the exception of specific purposes such as police investigations, medical history or family health history to determine hereditary diseases, and so on. Second, archival systems should seriously consider that at certain moments it may be appropriate to apply the "right to be forgotten" in the way that the European General Data Protection Regulation (GDPR) primarily intends, albeit particularly in relation to the private-law information administrators—by irreversibly destroying or deleting the records in question. Such a group of categories of information would, however, need a very explicit definition. At the same time, this procedure would be consistent with the "data minimisation" principle, one of the fundamental concepts of the GDPR. From my point of view, many court records and case files could serve as illustrative examples with some civil agendas, such as divorce cases, providing striking evidence for my claim. For administrative purposes, there are no compelling reasons for these materials to be permanently archived. Nor will historical science collapse by failing to preserve this group of materials for future research. Finally—or rather, first and foremost—family members, especially descendants being the most frequent requesters for access to their ancestors' divorce files, should take into account their ancestors' wishes as to whether they would consent to the disclosure of those records. It is without much debate that the absolute majority of people would oppose opening their divorce materials to their descendants or anyone else. This may be supported by the above case of Australia, where access to family law court records (including, inter alia, divorce files) is permanently restricted.

The topic of data minimisation, permanent access restrictions, including the issue of the possible destruction of personal data in the context of archival appraisal of records, is analysed in Chap. 8.

3. *Introduction of personality protection mechanisms in the form of legislative and procedural tools guaranteeing the preservation of documentation important for the protection of rights and controlled access to it*

While in some cases the protection of personality is most securely guaranteed by the irreversible destruction of particularly sensitive personal data and thus preventing unauthorised access, in some cases the opposite is true.[4] This case has been demonstrated and analysed in Chap. 4, using selected examples of child sexual abuse records and their management, including the issue of permanent archiving illustrated by examples of civil and religious institutions. The protection of human rights, including the protection of their personality in certain situations, is achieved by ensuring the preservation of certain documentation—usually one that indicates harm to the person and their rights—and at the same time ensuring access to it. The specific recommendations correspond in many respects with the conclusions and recommendations in Sect. 4.3, within Chap. 4. It introduces several specific tools, among which the following shall be mentioned:

- Prevention of uncontrolled and arbitrary handling of certain categories of records not only in public but also in private institutions such as churches (typically, the ill-conceived role of the exclusive powers of the bishops of the Roman Catholic Church over access to and management of records maintained in diocesan so-called secret archives).
- Appropriate setting of retention periods during which there is an obligation to maintain the records and not destroy them.
- Identification of certain record categories that shall be maintained for a very long period of time and possibly permanently archived. A related recommendation is to reconsider the setting of the so-called disposal tags, that is, determining which records should be permanently archived and which may be destroyed when the retention period expires.

[4] Although in a different context of the use and misuse of records and archives by repressive, dictatorial regimes, in times of wars, revolutions, and the like, Eric Ketalaar mentioned a similar moment: "Records, then, may be instruments of power, but, paradoxically, the same records can also become instruments of empowerment and liberation, salvation and freedom". Ketelaar, E. (2005). Recordkeeping and Societal Power. In S. McKemmish, M. Piggott, B. Reed, F. Upward (Eds.), *Archives: Recordkeeping in Society* (pp. 277–298). Charles Sturt University, p. 287.

– It is worth considering whether certain record categories created by private entities should be transferred to public archives for permanent preservation, or for archival assessment and selection of those records worth archiving in a public archive (typically illustrated by the example of some of the contents of the Roman Catholic Church diocesan archives containing information on child sexual abuse). The purpose is to allow a degree of public scrutiny, the absence of which could also have been one of the reasons why there was such a massive spread of child sexual abuse, for example, within the Church. In the same way that public scrutiny is beginning to be enforced in the area of social networks and the information these networks spread and store, public authorities should consider establishing certain minimum control mechanisms for other entities, including churches, particularly those working with minors.

4. Public interest and proportionality testing of individual public interests

At the very heart of the protection of (personality) rights in the context of the management of information contained in archival records is the principle of examining and testing public interests that enter into the field of protection of personality rights, personal data, and the privacy of those concerned in records and archives on the one hand and into the field of public interest in access to public records, archives, and information on the other hand. Archival systems should incorporate mechanisms to ensure that public interest tests are implemented and that they are proportionate. The United Kingdom has a well-developed system in this respect, but in one way or another, public interest testing is expected in most of the developed archival systems. In some countries, however, the scope for such testing is insufficient, or rather there are no appropriate and functioning tools to carry out public interest tests and to ensure a balance between the protection of personality rights and the associated restriction on access to records on the one hand and archives and its openness on the other hand.

5. *Tools guaranteeing the balance of protection of personal data, personality, privacy, and free access to information and flexible consideration of the evolving public interest in access to information, records, and archives*

Especially in situations when the relevant archival system imposes closure periods, it should at the same time create tools that allow access to otherwise withheld specific records, typically, but not exclusively, for research purposes. The aim is to ensure that the public interest in access to information, records, and archives is sufficiently considered, including the ability to flexibly monitor the evolution and transformation of such public interest within the changing general context of social and historical development. Closure periods, which are inherently general in nature, are not in themselves capable of providing such flexibility and cannot consider the evolving public interest in access to information. It is therefore essential that archival systems introduce other corrective tools to counterbalance the general and restrictive nature of closure periods and to act as a tool for opening specific records, for specific situations, and so on.

France, for example, uses the institute of general and individual derogations, but other analysed countries, such as Germany or the United Kingdom, also allow special access to archives in certain cases. However, there are two levels at which a problem may occur, as shown by the example of France: (a) insufficient application of general derogations. According to the calculations mentioned in Chap. 3, there have been 23 general derogations since 1979. However, we need to bear in mind that in some cases a single derogation may cover a very wide range of archives. (b) Long time delay in providing access to archives under general derogations. At present, the vast majority relates to archival records from World War II. A significant part of general derogations is further characterised by the opening of archives relating to controversial or problematic moments and phenomena in French history that have come to be discussed and reflected in society at large. Providing access to these materials to the whole public thus reflects a social demand for accessibility of materials indicative of historical events the society needs to deal with in some way.

The model applied for example in the Czech archival sector seems to be insufficient. In particular, it lacks adequate tools to allow access to specific records, which are otherwise withheld (closure periods, protection of the personal data of living persons). The Czech system does not sufficiently

consider and guarantee public interest in access to archives. The only existing exemptions given directly at the legislative level are grossly inadequate, especially as it is impossible for the legislation to react in a flexible manner—in the light of changing general and other circumstances—to the evolving public interest in access to various categories of records and archives.

6. Removal of obsolete and unfeasible legislative provisions, or such provisions, that if strictly applied in archival practice, would lead to the actual closure of access to archives

In some cases, the legislation is—most often procedurally—specific, but its strict application would lead to a drastic restriction on access to archival wealth to researchers. The following subsection 6a provides just one example.

6a. Inappropriate obligation to verify whether the person concerned in the archives is still alive

When it comes to the process of access to archival records and personal data protection, some archival systems, albeit a minority, implement the obligation to verify whether the requested data relate to a living person or not. The Czech Republic is a typical example. This procedural step is completely inappropriate and represents an example of the provisions characterised in Recommendation 6. This is a requirement that ultimately leads to withholding public records and archives as it is non-viable in the absolute majority of practical cases. It is almost impossible for archives and researchers to verify whether the person concerned in the records is alive, especially in the case of records less than 100 years old. The requested material is then anonymised in some cases, but it is very often completely withheld as the limited capacity of the archives does not allow for the anonymisation to be performed.

In any case, the model applied by most developed archival systems in Western democracies, as we have seen in the United Kingdom, France, Germany, and the USA, seems to be a more appropriate tool. The model consists of determining a certain period for the duration of which personal data in the archives remain withheld that serves as a substitute tool based on the expected life expectancy. This is in fact one of the forms of closure periods (see also one of the following recommendations). In the United Kingdom, this period is 100 years; if the age of the person concerned is

not known, it is assumed that they were 16 years of age at the time the document was created (unless they were a minor). German archives also impose a 100-year period for the protection of personal data unless the date of death is known. If neither the date of birth nor the date of death is known, then a period of 60 years after the creation of the record applies at federal level and the individual federal states impose similar slightly varying periods. In France, the protection of privacy generally works with a period of 50 years; the period is 100 years in the case of minors and in some specific cases (statistical materials, court records) these periods range from 75 to 100 years. The USA lays down specific rules for the disclosure of records, access to which would "violate the privacy of living persons" stipulating a protection period of 75 years from the time of the event to which the data relates.[5] In particular, these concern "personal and medical files and similar records", which correspond to the data defined as "sensitive personal data" under European Union legislation.

7. Complex system of closure periods

An appropriate tool for the protection of citizen's personal data and (personality) rights and balancing the right to access information is a structured system of closure periods imposed on certain categories of records. The example of the utilisation of closure periods in a situation in which it is not certain whether the person concerned is alive or not, as demonstrated above in Recommendation 6a, is only one of the levels at which closure periods should be applied. Of the countries analysed above, France has created the most sophisticated system. Rather than introducing general blanket closure periods, a model of determining those periods only for selected groups of records seems more appropriate, with, for example, the protection of privacy in the archives of the persons concerned becoming one of the categories to which closure periods would apply.

8. Specificity and accuracy of archival legislation governing personality protection and the removal of key vague concepts and categories

Even when archival legislation touches on the area of personality protection, very often the statutory provisions are too general, vague, and

[5] Code of Federal Regulations, 36, § 1256.56 (a); Freedom of Information Act. 5 United States Code, Ch. 5, subch. II, § 552, (b) (6).

indeterminate, or the key categories underpinning the structure of personality protection are unclear and equivocal. One such example is the concept of "legitimate interests of data subjects" ("schutzwürdige Belange") in the German archival legislative space. It is an essential, key term and the only criterion decisive for granting or denying access to archival records concerning persons deceased for more than 10 years, but it is also crucial for opening records testifying about living people. And yet, this term is fundamentally vague; it is an indeterminate legal concept.[6] The uncertainty of this concept then has negative effects on the practice of German archives granting access to records, which is inconsistent as a result. Another such example is the term "persons of contemporary history" ("Personen der Zeitgeschichte") used in German legislation and the category of "contemporary history" itself ("Zeitgeschichte"), the meaning of which had to be clarified with the help of the German Federal Court.

The specificity of archival legislation in the field of access to archival records and protection of personality rights may very well be realised by establishing a comprehensive system of closure periods, as characterised in Recommendation 7.

9. Multi-criteria assessment of requests for access to specific archives, including archives containing personal data

One of the appropriate solutions for the protection of citizens' rights in archives is a mechanism based on a multi-criteria assessment of access requests. Of the cases analysed above, the Stasi Records Archive carries out the most comprehensive assessment when granting access to the records of the former East German State Security Service, the Stasi. Bearing in mind that these are very specific records of an organisation that, among other things, acted as standard intelligence services, whose materials are usually completely withheld from the public, the Stasi archives access and data protection model can offer some specific inspirational tools that could be applied in other categories of public archives, including general state, provincial, and regional archives.

[6] Axel Metz, the head of the Würzburg City Archive, came to the same conclusion at the German Archive Conference in 2019 in his contribution Metz, A. (2019). Die Rechte der Nachkommen—oder: Schutz jenseits der Schutzfristen und die Konsequenzen für die Benutzung von Archivalien. Conference contribution at: RECHTsicher—Archive und ihr rechtlicher Rahmen. 89. Deutscher Archivtag in Suhl.

10. Expert and independent mechanisms for assessing the accessibility of archives under exemptions, extension of closure, and retention periods, including the control level

A very important element that a quality model for managing access to public archives and records should have is the establishment of appropriate tools based on expertise and independence, which should be involved in the decisions on access to these materials. France and the United Kingdom have sophisticated systems in place, particularly at the national level, where the roles are determined and fulfilled by the Advisory Council on National Records and Archives, as analysed in detail earlier. While the expert element can be provided by specialists from the relevant archive and ensured for example by the establishment of an expert committee within the archive, as is the case with NARA in the USA, for example, there are always questions regarding the independence of such a committee and the risk of conflict of interests when the public archive is part of the public administration, as are many of the records and archives creators who submit their material to and are supervised by the archive. In this respect, a public archive is not completely independent. This is typically reflected in the debates that have been taking place in recent years, for example in Germany, on the issue of the management of classified records, their (non) transfer to the archives for preservation, and their withholding and non-declassification. Most recently, the President of the Federal Archives, Michael Hollmann, faced criticism in this regard from leading historians and journalists in a debate at the national congress of German archivists.[7]

The archival system for example in the Czech Republic is fundamentally deficient at this point. Archival legislation and practice should establish sufficiently professional and independent mechanisms that would form a part of the process of access to archives, protection of personality rights and privacy, and that would also participate at the control level.

[7] For a reflection on this debate as well as the entire archival congress, see Čtvrtník, M. (2019). "Spolehlivé, správné, pravé—demokracie potřebuje archivy!". 88. německý archivní sjezd v Rostocku 2018 [Reliable, correct, true—democracy needs archives! 88th German Archival Congress, Rostock 2018]. *Archivní časopis* [*Journal on Archives*], 69(3), 295–314.

11. Consideration of the right to be forgotten in records management policies and archiving in the field of personal data, personality, and privacy protection and access to records and archives

A specific modelling of the right to be forgotten into one of the four categories captured and characterised within the systematics outlined in Chap. 5, can be used as an auxiliary tool. Starting from the closure periods, regulation of groups of persons with authorised access, its purposes and motivations, to the setting of protective measures against the risks of unauthorised access and data misuse, it seems to be suitable to utilise the four basic branches or categories of the right to be forgotten: temporary limited, temporary absolute, permanent limited, and permanent absolute. The use of the model of four categories of the right to be forgotten considering data pseudonimisation and anonymisation is analysed in Chap. 8.

12. Adaptation of records archiving policies in the field of archival appraisal, taking into account the multiple layers of the right to be forgotten

There are significant deficits in the records archiving policy in determining which records should be transferred into archives for permanent preservation and which can be designated for irreversible destruction in the archival appraisal and disposal of records. In the context of optimising these archival policies, the right to be forgotten needs to be taken much more into account, not only in its narrow and legalistic sense, as for example within the European GDPR, but also with regard to the foundations from which the right to be forgotten originates. These foundations cannot be reduced to a purely legal horizon; they are much broader. They encompass the ethical and moral level, interpersonal relations, discretion and tact towards the area of personal privacy, personality rights, as well as intimacy.

13. Implementing expert and independent examination when assessing the principle of data minimisation

In the European Union, the GDPR articulates this principle in a specific form by imposing the obligation to de-identify a specific person, provided that the public interest of archiving and the scientific and historical research objectives or statistical purposes are not compromised. However, the GDPR does not specify how such an assessment should be carried out. The principle of data minimisation has much broader boundaries than

those stipulated by the GDPR; it is more multifaceted and universal. Chapter 8, provides a closer look at this issue. Data archiving is one of the important domains in which the principle of data minimisation should be applied in a fundamental way; independent expert bodies and commissions seem to be an appropriate tool for such application. Some examples and possible inspiration are highlighted in Chaps. 3 and 7. These include the Advisory Council on Australian Archives in Australia, the Advisory Council on National Records and Archives in the United Kingdom, the Access Review Committee in the USA, and the Commission for Access to Public Documents (Commission d'accès aux documents administratifs) in France. In controversial and complex situations, and in particular in the area of the highly sensitive private and most intimate sphere, independent expert bodies should assess how the principle of data minimisation should be applied, whether the data should be destroyed and anonymisation applied or whether pseudonymisation is sufficient, how long should access to the data remain restricted, and so on. In case the subjects concerned do not consent, the decision would be provided by a final instance, that is, the administrative and, as a last resort, the constitutional courts.

14. ***Archives should hold a stronger role as a control and supervisory body in the preservation of records and data and in cases of their illegal destruction, especially by public administrations, public authorities, and public officials, including political figures***

In other words, archives should be one of the important guarantors of the right to preservation and access to information, the right of the individual and society to know, the right to and duty of memory.

15. ***Opening a new field of research on the relationship between artificial intelligence and the right to be forgotten and analysis of the possibilities of its application in archival practice***

There are fundamental deficits in the research on the relationship between AI and the right to be forgotten, regarding both data protection in general and data archiving and archiving in particular.[8] In the field of archiving

[8] In general and not in relation to archiving, the relationship between AI and the right to be forgotten is addressed by Villaronga, E. V., Kieseberg, P., Li, T. (2018). Humans forget, machines remember: Artificial intelligence and the right to be forgotten. *Computer Law & Security Review*, 34(2), 304–313. https://doi.org/10.1016/j.clsr.2017.08.007

in the public interest, a new field of research and subsequent practical application should be established focusing on the relationship between AI and the right to be forgotten at the legislative, technological, and procedural levels. Particular emphasis should be placed on new risks and threats of data misuse including the risks of deanonymisation and reidentification of persons using new AI tools.

16. Content of archives should be and should remain a mirror and a reflection of reality, a very important source of individual and social memory, historical consciousness, and our own self-reflection

It forms one of the important pillars of the formation of human civilisation and culture. Without historical sources, the formation of tradition would be impossible, the understanding of our past and of man himself would be threatened. Although the issue of data minimisation in archives opens a fundamental perspective on what data should not be archived and should be subject to a process of irreversible destruction, the aspiration given to archival science by the eminent German archivist, Hans Booms, remains valid: The aim of archiving is to create documentation on the whole of society and public life in its utmost complexity.[9] This aim is directly contradicted by policies that impose obligations to destroy certain categories of data, including personal data.

The content of archives devoid of links to specific people and actors in history would lead to a "depopulated history" and ultimately result in the destruction of historical research and the very memory of society. But no human society and civilisation can exist and survive without memory.

17. Relationship and the impact of long-term or permanent data preservation and destruction on the protection of persons, their personality and privacy, and their inclusion in the archiving process, archival appraisal, and data minimisation

Models of archiving, including the methods of archival appraisal, should in a way reflect the paradigmatic situation—analysed in Chap. 7, in Sect. 7.3—a double decision by the French Minister of the Interior, Édouard

[9] Booms, H. (1972). Gesellschaftsordnung und Überlieferungsbildung—Zur Problematik archivarischer Quellenbewertung. *Archivalische Zeitschrift*, 68, 3–40, pp. 37–40. Published in English as: Booms, H. (1991–92). Uberlieferungsbildung: Keeping Archives as a Social and Political Activity. *Archivaria*, 33(Winter), 25–33, pp. 28–30. https://archivaria.ca/index.php/archivaria/article/view/11796

Depreux, in the immediate aftermath of World War II. He first decided in 1946, based on the misuse of the Jewish files created by the prefectures of the French police that had disastrous consequences during the Holocaust, to destroy "all records based on the distinction of the French by race". In 1947, however, he changed this decision. While in 1946 the main principle of protecting persons and their sensitive data indicative of ethnicity, intending to eliminate potential risk of their misuse outweighed everything else, the 1947 decision boiled down to the protection of the rights of Holocaust victims and the need to retain their sensitive data for the purposes of rehabilitation and correcting the injustices and damage, both material and non-material.

The principle of data minimisation and storage limitation in the field of archiving should, just like Depreux's decisions of 1946 and 1947, include both: first, it needs to take into account the protection of persons, their sensitive data, personality rights and privacy; and second, it needs to consider the protection of the rights of citizens in situations when records including sensitive data need to be retained for the very same purpose.

18. Proportionality test of records value in terms of their potential future use on the one hand, and the risk of misuse on the other

The previous recommendation is accompanied by the following: In their policies of opening and regulating access to archival records, and in their procedures, archives should include the essential element of proportionality testing of the records' value in the perspective of their future use for various purposes on the one hand, and on the other testing of the data sensitivity and the potential risks of misuse of sensitive data contained in the records in the case of their hypothetical archiving.

19. Differentiation of the purposes of data preservation and their archiving

Archival data management policies should differentiate between the purposes of data preservation and archiving, that is, what is the purpose of the preservation of the data and who it is intended to benefit. The above "Depreux" decision represents a purpose that benefits the Holocaust victims in France; it is in fact an administrative purpose. The situation is completely different when the purpose is purely scientific, for example, the needs of historical sciences. However, the case of the Jewish files in France shows how complicated the situation is even when it comes to correct

determination of the future potential purposes for which the materials may one day be used. When Serge Klarsfeld discovered in 1991 parts of the Jewish files that should not have been archived, it triggered a serious debate about the state of the entire French archival system and, according to some of its prominent representatives, it showed the "archive crisis" in the country. Yet, in the end, Klarsfeld himself called for these files not to be destroyed. Half a century after the Holocaust, it became clear that the purpose of their existence as a memorial to the Holocaust has prevailed and the risk of their misuse as a source of information about the ethnic origin of the French population disappeared—at least it seemed to be the case—or rather the fear of this risk faded.

20. Transformation of the purposes of data, records, and archives preservation over time as a factor in records management and archiving

It is not only the above example that also points to one of the fundamental phenomena in the field of archiving: Not only do the purposes of preservation need to be differentiated, they are also not static and set in stone. The very foundations of archiving are based on the principle of fundamental change in the purposes of data preservation over time. These transformations have multiple layers. On a general level, it is a fundamental transformation, when the original purpose for which the record was created (official, professional, business, etc.) is transformed into a significantly different one, and concerns archiving especially for the purpose of preserving historical memory, future research, and so on. The minimisation of data applied in archiving should take this into account. In doing so, however, it must not lose sight of the potential risks of misuse of archived data.

21. Permanent data archiving, when and under what conditions

Archives should only accept for permanent archiving data that will not lose their value over a long period and that are worth investing in their maximum security; at the same time they should take a certain level of risk that these data may be misused in the future.

22. The Rubicon of permanent archiving

Implementing the principle of personal data minimisation and storage limitation, archives should consider whether, in certain situations, to abandon the traditional assumption of permanent archiving of transferred records, which are, in principle, kept permanently with the slight exception of material discarded as part of internal shredding procedures (most often duplicity and multiplicity).

23. Security protection mechanisms in the management of sensitive data in archiving

Security protection mechanisms should be implemented in archiving practice, especially in public archives, when managing particularly sensitive personal data. Archival systems should have a contingency plan in place for situations of a significant increase in the risk of misuse of sensitive personal data in particular.

First, there are the risks of war, occupation of a country by enemy forces, threats to democracy, and the rise of totalitarian regimes. In Chap. 7, and its Sect. 7.2, I have provided a detailed analysis of several cases in which data from census records had been misused in a fundamental way, both by totalitarian regimes and by democratic states during periods of heightened threat to the state or in times of civil wars and so on. However, such a threat also emerges with political pressures from "above" and with orders that go against the principles of good data management and protection in general. In Chap. 7, I analysed several illustrative examples from modern history as evidence of how sensitive personal data can be fundamentally misused. The so-called National Socialism Archive ("NS-Archive"), existing within the East German State Security Service (Stasi), is excellent evidence of the risk inherent in the combination of two moments: (1) the absence of a democratic rule of law and (2) the existence and retention of personal and especially sensitive personal data on citizens that can be misused, compromised, and so on.

The crucial point is that we cannot rely on the fact that a country may currently be in a period of relatively decent democracy and rule of law. This state of affairs may change very rapidly. The geopolitical developments in recent years have clearly demonstrated that an established democratic rule of law is not an unwavering and absolute constant even in developed European countries. It cannot be excluded that they will cease

to exist or that their existence will be seriously disrupted. The risks dramatically increase by the proximity of non-democratic states with great power ambitions. This applies as much to the European area as to Asia, as evidenced by current developments on both continents.

Historical developments in the twentieth century, in the form of the Nazi and Communist totalitarian regimes that had taken over formerly democratic countries, have clearly demonstrated how fragile the rule of law, decency, and civility is even in countries where we would not have expected them to be seriously undermined. The final part of Chap. 7 in Sect. 7.5, sums up some of the risks. Using the example of the so-called Archive of National Socialism (NS-Archiv), it identified the extreme risk entailed in the connection of two moments: (1) the violation of the fundamental principles of the democratic rule of law in totalitarian non-democratic regimes, and (2) the existence and preservation of sensitive data about citizens that are potentially damaging and compromising.

Archives and data archiving should take these risks very seriously. Archives, and entire archive policies, should implement contingency plans and decide what materials to destroy in a situation of serious threat to the country, democracy, and the rule of law and the associated risks of misuse of sensitive personal data stored in archives. This is, in a way, an anticipation of a situation analogous to the Dutch resistance against the German Nazi occupation power during World War II. By bombing the Amsterdam civil registry in 1943, the Dutch resistance fighters managed to destroy at least part of the population register used by the Nazi occupation power for the implementation of the Holocaust and the unprecedented persecution of the population.

Second, there are additional risks of data misuse, typically in the form of ransomware viruses and hacker attacks, which in principle apply to electronically archived data. The most frequent target of these attacks is medical records and materials that provide information on the health of citizens, as shown in Chap. 7 in Sect. 7.1. Here again, archival systems should not rely on the 100% security of digital archives, quite the contrary; the risk of misuse of data stored in digital archives is high and growing over time. Archival policies should take this risk into account and incorporate it into their contingency plans and digital records acquisition policies.

An effective element of contingency plans for the destruction of sensitive data in a situation of an extremely increased risk of their misuse, for example in the event of an external threat, could be time capsules in which certain groups of records containing highly sensitive data would be

archived and whose contents would be destroyed in a situation of a serious threat to the state, the rule of law, and democracy. For it is true that a lawless, arbitrary, malicious totalitarian power, and oppressed society will not hesitate to violate the sanctity of the seal of the capsules, as well as the protection of confidentiality of information and contractual agreements, which is honoured by the rule of law and democratic state, the public power, as well as the honest man.

24. Radically increased risk of sensitive data misuse in the area of digital data and records

The risk of misuse of sensitive data increases dramatically in the case of digital data management and archiving. This is evidenced by cases of massive misuse of sensitive personal data, with the largest cases of leaks and misuse of digital data registered in the area of medical records, as I demonstrated in Chap. 7 in Sect. 7.1.

25. Higher financial costs of management and protection of personal and sensitive data, especially in a digital environment

The financial costs of preserving digital records and maintaining digital archives are and will continue to increase significantly, also due to data management and protection. This is due to the creation of the necessary infrastructure for preserving and securing digital data, as well as the rising costs associated with eliminating the consequences of cyber-attacks, including often paying ransoms to blackmailers. These reasons were completely ignored by Viktor Mayer-Schönberger, among others, when he defended his thesis regarding the current and for the first time ever easier and cheaper "remembering" and preserving data compared to not preserving and "forgetting".[10]

26. Reduction of the risk of personal and sensitive data misuse by means of analogue archiving of originally digital data

The significantly increased risk of misuse of data archived in digital form can be reduced by maintaining them in analogue form, at least in certain

[10] Mayer-Schönberger, V. (2009). *Delete: The Virtue of Forgetting in the Digital Age*. Princeton University Press, p. 196.

cases when large amounts of sensitive personal data are accumulated; the risks associated with the use of "big data" can be reduced by archiving their analogue form, even though the original data file is digital. This is the solution that the Australians opted for in the case of archiving census records with non-anonymised data of citizens who gave their explicit consent; these are stored in a time capsule in the form of microfilm. Moreover, the analogue form is more suitable for long-term data preservation, as the need for continuous care of digital data is eliminated and access to the data is absolutely restricted for a substantial period of time. And this is exactly the case of archiving of census time capsules in Australia, as access to these records is completely restricted for 99 years.

27. Archival appraisal of records as a tool of personality and privacy protection, and a tool of data minimisation and storage limitations application in archiving

Archival appraisal and disposal of records should become essential tools for the application of the principle of minimising and limiting the storage of data, including personal data in long-term archiving. This relates to another recommendation, that is, the purpose of records reduction and disposal procedures in the future should not only be the need to reduce the volume of archived records that has increased extremely over the past decades, but also to protect the personality, privacy, and personal data of those concerned in the records (as demonstrated in one of the conclusions in Chap. 8). Moreover, it is very probable that this purpose will play an increasingly important role in the future, in particular due to the significantly higher risk of data misuse in the case of electronic data and records compared to paper documents. Unlike digital data and digital archives, in the case of paper archival material, it is much easier and more efficient to set up security protection measures for access. It is not only much easier to access digital data as compared to analogue data, also their quantity is almost unlimited and the risks of misuse increase proportionally.

A follow-up recommendation suggests that archival methodology and theory—which has so far focused primarily on the informational content of records—incorporate among the main perspectives of archival appraisal of records the protection of personal data, personality rights, and privacy of the person concerned in the records that have the potential to become archives as well as the security risks of breaching this protection in the archiving phase with the assumption of permanent data preservation.

Particular attention should be paid to digital archiving and digital archives. This perspective should be reflected in particular in deciding on which specific groups of records should be determined by the archival appraisal and retention procedures for irreversible destruction and which can be archived, with regard to the protection of personal data and the risks of their future misuse.

Archiving in the public interest preserves and processes records long before those concerned in the records pass away. Given the high frequency of personal data in public records, archives process and will continue to process personal data of living individuals. A well-set policy on archival appraisal that takes into account the protection of personal data, personality, and privacy of the individual will be able to serve as the main pillar of the justification explaining why some personal data were retained and others were destroyed.

28. Retention periods as a tool of sensitive data protection, application of data minimisation principle, and data storage limitations

An appropriately set policy of retention periods has shown to be an important and effective tool for implementing the principle of minimising and limiting the storage of personal data. Retention periods should become more important in the future. In the European Union (but not only there), they should be stronger especially when functioning as the main lever for the application of the principle of data storage limitation in the diction of the European GDPR, that is, the principle of maintaining personal data for no longer than strictly necessary. This is a principle that has been growing in importance along with the increasing risks and misuse of personal data, a principle that is quickly becoming one of the cornerstones of data protection. In this respect, the abovementioned "Depreux" decision is a symbolic predecessor. In his second appeal decision, the French Minister of the Interior, Depreux, determined a period after which the personal data should have been destroyed. The data were to be kept only as long as they could benefit the victims of Jewish origin. In current terms, he determined the point in time at which the "administrative need" for the retention of personal data would cease to exist, and at the same time he decided on the expiration of what we today call retention period, although he did not express it by a specific number. In many cases, however, it is very difficult to correctly determine the right point until which the relevant personal data can be useful and after which they can be destroyed.

Retention periods may be set either directly by archival legislation or by special legislation specifically for certain categories of records. Prime examples can be found in the category of medical records and the management of census data. Chapter 7, dealing with Sect. 7.2, mentioned the critical voices in Germany arguing the vagueness of the periods for which the statistical office could keep the non-anonymised form of the auxiliary characteristics that made it possible to identify those who participated in the census. Germany has removed this ambiguity since 2011, when a special census law set a maximum time limit of four years from the creation of the census report, during which the auxiliary characteristics must be destroyed.

29. Data Redaction, anonymisation, and pseudonymisation

Records destruction (and an appropriate setting of retention periods) is not the only tool for applying the principle of minimisation and storage limitation. In the context of records management in the pre-archival phase, anonymisation processes are commonly used across countries for certain groups of material containing sensitive personal data. This is clearly demonstrated on the census materials. The West German Federal Constitutional Court, as we have seen in Sect. 7.2, in Chap. 7, expressed this idea in the "Judgment on the Census" ("Volkszählungsurteil") of 1983: Already during the stage of data collection and immediately after their statistical evaluation, it is necessary to guarantee sufficient rules for the deletion of records containing personal data that allow "deanonymisation". In the same judgment, the Court drew from the Constitution and defined a new fundamental right of the citizen to informational self-determination; for future statistical research, it saw the principle of timely anonymisation of personal data as constitutive. The "Census Judgement" subsequently became the basis for giving greater weight to the side of the obligation to delete data compared to the obligation to offer public records for archiving in public archives.

Records management and archiving should make more frequent and sophisticated use of the tool of personal data anonymisation. From the point of view of security measures for the protection of personal data and the elimination of risks of their misuse, anonymisation, that is, the process whereby data are irreversibly destroyed and cannot be recovered, appears to be a strong form of protection in terms of long-term data retention and archiving. For some groups of archival records, archiving should

implement personal data pseudonymisation in its contingency plans, together with the setting of security processes for the potential destruction of additional information enabling the "impersonation" of data, that is, linking them to a specific individual, that would be implemented in times of crises of the country and its society. In other words, archiving in the public interest should incorporate additional data anonymisation processes into its contingency plans.

30. Risks of deanonymisation and reidentification of persons

Archival data minimisation, storage limitation, and access policies should in future take more serious account of the risks of deanonymisation of anonymised or pseudonymised data and reidentification of individuals, in particular by linking various data sets. The risks of deanonymisation have increased dramatically in the area of digital preservation and archiving. Not only has this facilitated access to electronic data, including the "big data" sets, but it has greatly increased the possibilities of deanonymising already anonymised or pseudonymised data. The risks of deanonymisation and reidentification of persons increase in proportion to the improving capabilities of information technology, including the possibilities of artificial intelligence and the assumption of its further turbulent development. Archives and archiving should also include a reidentification risk assessment as a new component in the overall complex archival and personal data management processes.

31. Four categories of the right to be forgotten

The model of the four categories of the right to be forgotten (elaborated in detail in Chap. 5) is a practical tool for the implementation of an appropriate data minimisation policy, including its application in the selection of the different tools, such as data anonymisation and pseudonymisation. In principle, the right to be forgotten can be divided into the following categories: (1) temporary limited, (2) temporary absolute, (3) permanent limited, and (4) permanent absolute. Each of these categories corresponds to a different approach to data minimisation and specific processes and tools for applying the data minimisation principle. Irreversible, "hard" data anonymisation, that is, the destruction of data or entire records, should be applied in situations dealing with highly sensitive data in which there is a great risk of potential future misuse. In such a case, it is only

appropriate to apply the permanent absolute right to be forgotten. Although there is no unified opinion in international comparison, serious candidates for this procedure are, for example, medical records, census records, some agendas of the courts, prosecution offices, and security forces. On the other hand, reversible pseudonymisation is sufficient when a temporary limited or permanent limited right to be forgotten is relevant. The time capsule tool "locking" access to data in absolute terms, but for a limited period of time used by some countries, for example, for archiving census records, is one of the appropriate means of exercising the temporary absolute right to be forgotten.

At the same time, the model of the four categories of the right to be forgotten and the different tools by which each category is implemented in the practice of data archiving and records management represent one of the appropriate tools for balancing the tension between, the need to obtain and preserve a set of certain data on citizens, and the increasing risk of misuse of these data.

32. Formative processes in archived data and their use for the protection of data, personality rights, privacy, and for data minimisation and their storage limitations

Archival data minimisation and storage limitation policies should take into account four important and interrelated processes that occur in the case of long-term and permanently archived data:

1. the "ageing" of archives and data.
2. disappearance of personal data.
3. disappearance or transformation of personal data sensitivity.
4. weakening of post-mortem protection of the personality rights of the deceased.
   - Ad 1. The process of "ageing" of archives and data preserved in archives is basically given by the fact that in the vast majority of archives there is a gradual and steady increase in the volume of archival records corresponding to the ongoing acquisitions. The average age of the archived records increases over time, counting from the moment it was created.
   - Ad 2. The process of the disappearance of personal data is embedded in the fact of permanence, or rather the extremely long time

for which the data are stored in archives. Over time, therefore, personal data, if we define them as data relating to living people (as is customary in legal systems across countries), disappear in proportion to the passing of the persons concerned. In this sense, this process can in a way be described as the "depersonification" of archival records.

- Ad 3. The process of disappearance or transformation of personal data sensitivity corresponds to the first two processes. As archival records/documents "age" and as personal data disappear together with the deaths of their holders, the data sensitivity in many cases disappears or is transformed. However, even in a situation when the personal data may no longer be personal in the strict sense (= the person concerned is deceased), the protection of the personality rights of the deceased may still prevail (see below), and therefore a certain data sensitivity together with the need for data protection may also remain. A prime example is the "Jewis files" ("fichiers juifs") mentioned above that were the subject of a special part in the book.
- Ad 4. The process of weakening of post-mortem protection of the personality rights of the deceased corresponds to the previous two processes and corresponds to the ever longer period since the death of those concerned in the archival records. Details on this process have been analysed throughout the book. The data sensitivity and the corresponding post-mortem personality protection gradually disappear. In some cases, however, it persists permanently. These processes can be translated—as I have demonstrated above—to the level of application in archival practice, inter alia, using the model of the four categories of the right to be forgotten introduced in Chap. 5.

Archival data minimisation, storage limitation, and access policies should take into account these four important processes, including the underlying principle of continuously increasing the proportion of archived material not subject to the right to be forgotten in any of its forms or categories. On the other hand, these same archival policies must be aware of the fact that assessment of the right to be forgotten will always play an extremely important role. Not only will further archival acquisitions continue to bring "young" and "youngest" records containing data about living people, these modern and contemporary documents belong among

the most attractive for research. Last but not least, they are crucial for self-reflection of man and society, the formation of individual and social memory, and historical consciousness. Very often, they serve as tools for coming to terms with one's own past, with injustice, as well as with the virtues of an individual, a social group, and entire nations. Without access to them, it would be impossible to hold even living historical actors accountable for their actions and to pursue justice and redress recent wrongs. For these reasons, archival access and data minimisation policies will have to constantly confront the clash of the right to be forgotten and the right to memory, the right to know, and seek balance and proportionality between the different public interests entering the field.

33. Implementation of a voluntary element in the archiving of personal data in the public interest

The implementation of a voluntary element in the archiving of personal data in the public interest may be a suitable tool to balance and ensure proportionality between the public interests of archiving and preserving data, and the right to be remembered on the one hand, and data protection (especially personal data) and the right to be forgotten on the other hand, at least in some cases relating in particular to sensitive personal data. This would mean introducing the possibility for the persons concerned to decide freely on the archiving of their personal data in the public interest. Archiving in the public interest does not yet envisage such consent to be a standard across countries in most cases of public records (apart from specific cases of records on the borderline between private and public character, typically in the case of top elected representatives and the like), and uses a statutory mandate for archiving public records including personal data contained therein. One of the harbingers in this field is the recent introduction of a time capsule for census records in Australia and for the 2022 census in Ireland analysed in Chap. 7 in Sect. 7.2. Australia is also proof that more than half of the citizens are interested in archiving their sensitive personal data in a time capsule.

Naturally, their consent to archiving does not automatically equate to consent to immediate accessibility. As in the case of, for example, personal funds and estates, this consent can very easily be conditional on a period of time during which the material is rendered inaccessible for any consultation purpose, including official purposes, which is also the case of the time capsules with census records in Australia and Ireland.

The consent of the citizen to the archiving of their sensitive personal data and, in this respect, their inclusion in the responsibility for the decision to preserve their data, being aware of any risks of misuse, is, at a time when these risks are significantly increasing, an appropriate instrument to maintain the proportionality of public interest in the preservation of a certain part of public records and historical memory, and public interest in the protection of citizens against misuse of their data.

Moreover, the inclusion of citizen consent to the archiving of their personal data—at least in some cases concerning highly sensitive data and when it is possible to implement such a step in practice—would at least partially compensate for the fact that, in the case of archiving in the public interest, citizens do not freely consent to the preservation of their personal data and do not know what sensitive personal data public archives maintain. At the same time, it would reflect, at least to some extent, the fact highlighted by the Court of Justice of the European Union in the specific context of traffic and location data retention: The retention of such data without informing the persons concerned constitutes a widespread and extremely serious interference with the fundamental rights guaranteed by the Charter of Fundamental Rights of the European Union, namely the right to respect for private and family life, home, and communications, and the right to the protection of personal data. The Court of Justice of the European Union then sees the fact that citizens are not informed about the state retaining and using their data as a risk as the citizens may feel to be under constant surveillance.[11]

However, this observation has relevance not only for the specific area of data retention, but for any data retention and protection, privacy protection, and data minimisation in general. A free society should counter the threat of an Orwellian Big Brother, and one suitable tool is the effort to enforce in archival policies, at least to some extent, the free consent of citizens to the archiving of their personal data.

[11] Judgment of the Court (Grand Chamber) of 8 April 2014, par. 37.

Summary

The common denominator of the book is the relationship between, on the one hand, the need to preserve and open access to data, primarily in the specific field of public records management and archiving in the public interest, and, on the other hand, the concomitant need to protect these data. The main focus turns to the protection of personal data or the protection of personal rights and privacy. As Chap. 4, shows, there is a specific paradox within which archives and archiving exist: Archiving itself poses a potential risk to the protection of personal rights and privacy, and yet, it represents one form of protection of the very same personal rights and privacy.

The book takes a look at the protection of personal rights and human privacy in the field of archiving in the public interest and public records management in a broadly comparative international perspective. Based on the provided comparisons, it proposes a set of recommendations and, in some respects, principles that might in one form or another be implemented in the policies of records management and archiving in the public interest.

The book considers the question of how archives and records creators set up information protection and management processes, policies, and procedures for opening access to records and archives. Especially in Chaps. 2 and 3, the book seeks for, among other things, some models as well as legal and procedural tools that archives and records management implement in the protection of personal data, personal rights, and human

M. Čtvrtník, *Archives and Records*,
https://doi.org/10.1007/978-3-031-18667-7

privacy that can be encountered in the archival systems of some countries, namely Germany, the United Kingdom, and France; it also touches on the situation in the USA and some other countries. Chapters 6, 7 and 8, address the question whether and how this protection can be implemented in the form of data reduction and minimisation, pseudonymisation, anonymisation, or in the form of retention periods. As part of the analysis of data minimisation tools, the book also mentions the increasingly current phenomenon of the dramatically growing possibilities and related risks of deanonymisation and reidentification. The analyses also concentrate on the recent changes and transformations of the specific field of archival appraisal and explore possible future trends in this field. Chapter 7, provides a detailed case study analysis of several examples of leaks and misuse of personal data in the twentieth century, some of which have had tragic impacts on broad groups of the population. The records that come into play include, for example, census records, medical records, Jewish files during the Nazi dictatorship, and archives of the former East German State Security Service. Archiving and records management move metaphorically in a magnetic field between the mutually interacting and colliding right to be forgotten and the right to be remembered together with the right to know in a broad sense. The forms these encounters and clashes take on are outlined in Chap. 5.

The book deals with protection of personality rights in archives in the broader context of the issue of access to archival records. It pays special attention to post-mortem protection of personality and privacy, which represents a very young domain within archival law and practice, and this also applies to research in this field. Yet, it is post-mortem protection of personality and privacy that should lie at the centre of the field of archiving as the vast majority of those concerned in the archives are now deceased. This is also the reason why the protection of privacy and personality rights in the field of archiving takes on specific contours, in contrast to the general protection of personal data.

The enduring mission of archives and archiving has always been, and should continue to be, to preserve in the very long term, with the ambition of permanently preserving information that is valuable to society and its memory, to make this information as accessible to the public as possible, but also to protect a certain segment of data. They should, in particular, protect such data that could harm the individuals concerned in the archival records. This book intends to be one perspective on how to seek a balanced approach in this field based on international comparisons, both

in the field of archiving and in records management. It also aims to present some of the already implemented and some yet-to-be-implemented or under-developed solutions and last but not least to summarise recommendations on how to address some of the fundamental issues in the field of citizen's rights, privacy, and personality protection in relation to access to archives and records.

Brief Glossary

Anonymisation Processing of personal data in a way that they can no longer be or should no longer under any circumstances be attributed to a specific data subject. Unlike pseudonymisation, it is an irreversible process of erasure or other forms of destruction of personal data.

Archives The term "archives" has several meanings, the main ones being: (1) The materials created, acquired, and collected by a specific entity (individual, legal entity, public and private organisations, families, clans, etc.) and preserved permanently or long term in an archive or similar institution; (2) an institution preserving, managing, and providing access to records and other materials of enduring value; and (3) a building in which records transferred into the archives as an institution and intended for permanent or long-term archiving are preserved.

Archiving in the Public Interest Archiving carried out by public authorities, public or private bodies that hold records of public interest and that have a legal obligation to acquire, preserve, appraise, arrange, describe, communicate, promote, disseminate, and provide access to records of enduring value for general public interest (definition based on the European General Data Protection Regulation (GDPR), Recital 158). In contrast, archiving in the private interest is not carried out in the public interest and for the public interest.

Closure Periods Closure periods for public records and archives are usually statutory periods for the duration of which a certain group of records, usually of public administration origin, cannot be made accessible to the public apart from legitimate official requests. These periods

M. Čtvrtník, *Archives and Records*,
https://doi.org/10.1007/978-3-031-18667-7

differ depending on individual national legislation. There are specific periods for certain groups of materials such as registers of births, marriages and deaths, and medical records. Classified records are "protected" in a different manner and access to them is often completely and permanently restricted. Closure periods have several functions at the same time. They protect some of the very recent, sensitive, and valuable information that could be misused, whether for commercial, business, and power purposes in general. At the same time, they represent a refuge for administration and for archives in which they seek shelter from the imminent necessity for an immediate and massive response to requests for disclosure. Contemporary history represents a very important field of scientific research and popular science work, and therefore "young" records represent highly sought-after materials by researcher. Above all, they are an important tool for privacy protection, although it is the laws governing the entire area of personal data protection that should play a major role.

Data Minimisation The reduction of data in relation to their content or the purpose for which they were created, collected, and preserved. Data minimisation covers in principle the management of any data, including records management and archiving. It most often applies to personal data. The European General Data Protection Regulation (GDPR, Article 5(1)) states that "personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed".

Deanonymisation The process of recovering anonymised data and thus reidentifying the individuals in the originally anonymised data set.

Personal Data The European General Data Protection Regulation (GDPR, Article 4(1)) defines them as "any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person". Personal data refer to living individuals.

Personality Rights Personality rights[1] are based on the recognition of a person as a physical as well as spiritual and moral entity. Personality rights and their protection are embedded in a number of legal systems. They include, among others, the right to physical liberty, privacy, identity, likeness and image, reputation, dignity, physical-psychological integrity, and also the right to life itself, sentience, and others. While in the common law system, "personality rights" are not recognised as a terminus technicus and rather include particular acts and torts protecting certain aspects of personality, such as misappropriation of name, breach of confidentiality, and so on, they have a stronger position in continental law. In some jurisdictions, personality rights also include post-mortem personality protection (see the entry "post-mortem personality protection").

Persons of Contemporary History ("Personen der Zeitgeschichte") Specific concept resonating across German not only archival legislation. Several German laws in the archiving and other fields implement the term "persons of contemporary history", which lacks a more precise definition.[2] None can be found in the archival laws nor other German legislation. However, there is already some case law that refers to the concept of "persons of contemporary history". A 2014 ruling by the German Federal Court, that is, the country's Supreme Court, including a photograph depicting people at a neighbourhood party published without the consent of those pictured had a significant impact. The court concluded that even in such cases of everyday and local phenomena, these are or may be events of "contemporary history" ("Zeitgeschichte") or "contemporary events"

[1] See a detail definition of personality rights in comparative legal perspective in Neethling, J. (2006). Personality Rights (entry). In J. M. Smits (Ed.), *Elgar Encyclopedia of Comparative Law*. Edward Elgar, pp. 530–547.

[2] The term appears outside the archival domain especially in the Act on Copyright for Works of Fine Arts and Photography (Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie of 9 January 1907. BGBl. I S. 266). On "persons of contemporary history" in archival space, cf. Unverhau, D. (Ed.). (2003). *Hatte "Janus" eine Chance? Das Ende der DDR und die Sicherung einer Zukunft der Vergangenheit.* Lit, pp. 161–171.

("Zeitgeschehen").[3] The Judgment of the Federal Court was groundbreaking in that it no longer linked "contemporary events" only to the so-called absolute persons of contemporary history, a term previously used in Germany to refer to, roughly speaking, the most prominent public figures. Instead, as a key moment, the Federal Court referring, inter alia, to the previous case law of the European Court of Human Rights, established under the "graduated concept of protection",[4] that it is necessary to examine the relevant context of the right to information and freedom of expression on the one hand and the personality rights of the persons depicted on the other hand.

Post-mortem Personality Protection Post-mortem personality protection is the protection of personality rights even after a person's death. Lilian Edwards and Edina Harbinja defined it as "the right of a person to preserve and control what becomes of his or her reputation, dignity, integrity, secrets or memory after death".[5] Asta Tūbaitė-Stalauskienė also relies on this definition.[6] On the other hand, Antoon de Baets defines it differently: "Given that the dead are former human beings, posthumous dignity is not the same as the human dignity of the living, but it is still closely related. Human dignity is an appeal to respect the actual humanity of the living and the very foundation of their human rights; posthumous dignity is an appeal to respect the past humanity of the dead and the very foundation for the responsibilities of the living."[7] From a legal point of view, the question is what rights are transferable and enforceable after the death of the person concerned. While the transferability of economic rights of the deceased is generally accepted, as manifested in particular in the law of succession and freedom of testation, copyright, and so on, there are considerable differences in per-

[3] Bundesgerichtshof, Judgment of 8 April 2014 - VI ZR 197/13, Art. 10 and 11. The court reasoning includes, for example, the following argument: "Der für die Frage, ob es sich um ein Bildnis aus dem Bereich der Zeitgeschichte handelt, maßgebende Begriff des Zeitgeschehens umfasst alle Fragen von allgemeinem gesellschaftlichem Interesse. Dazu können auch Veranstaltungen von nur regionaler oder lokaler Bedeutung gehören".

[4] Bundesgerichtshof, Judgment of 8 April 2014 – VI ZR 197/13, Art. 8.

[5] Edwards, L., Harbinja, E. (2013). Protecting Post-Mortem Privacy: Reconsidering the Privacy Interests of the Deceased in a Digital World, *Cardozo Arts & Entertainment Law Journal* 32(1), 83–130, p. 85.

[6] Tūbaitė-Stalauskienė, A. (2018). Data Protection Post-Mortem, *International Comparative Jurisprudence* 4(2), 97–104, p. 97.

[7] De Baets, A. (2004). A Declaration of the Responsibilities of Present Generations toward Past Generations, *History & Theory*, 43(4), 30–164, p. 136.

sonality rights. There are two lines of thought within the law, one of which accepts the existence and need for the protection of personality even after a person's death, the other does not as it claims that the protection of personality rights ends with the death of a person. In neither case, however, do the legal systems equate the protection of the personality rights of the living and the deceased. They usually gradually reduce the post-mortem protection of personality in proportion to the time that passed since the death of the person concerned.

Privacy The term occurs in a variety of contexts, legal, philosophical, ethical and moral, political, sociological, anthropological, technological, security, and others. It is not possible to provide a comprehensive definition of privacy, which is also why legislators and courts avoid explicitly formulating the concept. In the context of this book, the notion of privacy will be touched upon at various levels, especially in the context of archives, records management, archival practice, and data protection within archival practice, and consequently in the context of law and ethics. For a more detailed definition of privacy, including bibliography, see, for example, definitions in some encyclopaedias.[8] The concept of privacy is derived from the Latin term "privatus" meaning personal, separate, belonging to oneself. The significant feature is its distinction from the public sphere, or rather its concealment from the public gaze.[9] The area of privacy in one form or another includes the inviolability of the person and control over information about oneself, what data, how, to whom, and for what purpose is further communicated, disclosed, or published. Privacy protection includes, among other things, the protection of human dignity, integrity, autonomy, and independence. Privacy also includes the protection of a person's intimate sphere; it embraces the physical part of life (home, etc.) as well as the virtual part, including the online space. In legal systems, privacy is usually protected as a constitutional right and constitutes one of the personality rights of the individual.

Privileged Access to Archives The specific access to public archives, particularly for the purposes of research or other scholarly purposes, not

[8] For example, DeCew, J. (2018). Privacy. In *The Stanford Encyclopedia of Philosophy*. Spring 2018 Edition. https://plato.stanford.edu/archives/spr2018/entries/privacy/; Staples, W. G. (Ed.). (2007). *Encyclopedia of privacy*. Greenwood Press.

[9] Cf. Mates, P. (Ed.) et al. (2019). *Ochrana osobnosti, soukromí a osobních údajů*. Leges, p. 15ff.

exclusively of official nature is a specific phenomenon in the area of access to archival records, which is sometimes referred to as "privileged access to archives". National archival legislations deal with this system in a variety of ways. Some countries open the door to privileged access to archives, especially for research purposes wider, others not so wide. Most often, however, they introduce certain, albeit usually very limited, possibilities for exclusive access to archival records. However, a specific ("privileged") access to archives subject to different than general access rules is only justified if it serves as a specific tool for balancing, on the one hand, the right of free access to information and, on the other, the need to protect the personality rights and privacy of the persons in the records.

Pseudonymisation According to the definition in the European General Data Protection Regulation (GDPR, Article 4(5)), "[T]he processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person". Unlike anonymisation, this process is reversible and personal data can be recovered under certain circumstances using certain tools and auxiliary data.

Record Any written, visual, audio, or other recorded information, whether in analogue or digital form. The meaning of this term differs across countries. In principle, however, it can be summarised as material of which the absolute majority will not end up in archives and will not be permanently preserved as archives. In this respect, the term "record" is broader than "archives". Only a fraction of the emerging "records" ends up becoming archives.

Storage Limitation A principle specifically defined in the European General Data Protection Regulation (GDPR, Article 5(1)) in relation to personal data and stating that "personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed". It is therefore a reduction of (personal) data in relation to the period for which the data are stored.

Selected Bibliography[1]

200 Jahre amtliche Statistik in Bayern 1808 bis 2008. (2008). Bayerisches Landesamt für Statistik und Datenverarbeitung.

2018 Data Breach Investigations Report. (2018). 11th edition. Verizon. https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf.

2020 Data Breach Investigations Report. (2020). Verizon. https://enterprise.verizon.com/resources/reports/2020/2020-data-breach-investigations-report.pdf.

6e symposium du Groupe interdisciplinaire de recherche en archivistique (GIRA). (2010). *Les archives, de l'information à l'émotion. Congrès des milieux documentaires*, 3 November 2010. http://gira-archives.org/activites/6e-symposium-2010/.

A Letter on Justice and Open Debate. (2020, 7 July). *Harper's Magazine*. https://harpers.org/a-letter-on-justice-and-open-debate/.

Advisory Council on National Records and Archives. *14th Annual Report 2016–17*. https://www.nationalarchives.gov.uk/documents/advisory-council-annual-report-2016-17.pdf.

Advisory Council on National Records and Archives. *16th Annual Report 2018–19*. https://www.nationalarchives.gov.uk/documents/advisory-council-annual-report-2018-19.pdf.

Ahlquist, K. R. *Norwegian health archives. A new type of archive in The National Archives of Norway*. https://www.nordiskarkivportal.org/wp-content/uploads/2017/10/24.05_4.3-3_Kurt-Ahlquist_Norway_Norsk-helsearkiv-en-ny-type-virksomhet-….pdf.

[1] (legislation and case law not included)

M. Čtvrtník, *Archives and Records*,
https://doi.org/10.1007/978-3-031-18667-7

Aly, G. (2019). Seit 40 Jahren der Geschichte auf der Spur. Warum mich ein Archivbesuch glücklich macht. *Conference contribution at: RECHTsicher – Archive und ihr rechtlicher Rahmen*. 89. Deutscher Archivtag in Suhl.

Aly, G., & Roth, K. H. (2000). *Die Restlose Erfassung. Volkszählen, Identifizieren, Aussondern im Nationalsozialismus*. Fischer E-Books.

Anderson, M. (2015a). Public management of big data: Historical lessons from the 1940s. *Federal History, 15*, 17–34.

Anderson, M. (2015b). *The American census. A social history*. Yale University Press.

Anderson, M., & Seltzer, W. (2000). After Pearl Harbor. *The proper role of population data systems in time of war. Material prepared for the meeting "Human Rights, Population Statistics, and Demography: Threats and Opportunities"*, organised by the Population Association of America, 23–25 March 2000, Los Angeles.

Anderson, M., & Seltzer, W. (2007). *Census confidentiality under the second war powers act (1942–1947)*. Paper prepared for presentation at the session on "Confidentiality, Privacy, and Ethical Issues in Demographic Data". Population Association of America Annual Meeting, 29–31 March 2007, New York, NY.

Anderson, M., & Seltzer, W. (2009). Federal statistical confidentiality and business data: Twentieth century challenges and continuing issues. *The Journal of Privacy and Confidentiality, 1*(1), 7–52. https://doi.org/10.29012/jpc.v1i1.563

Anker, J. (2009, 3 March). Klaus Kinskis Akten bleiben verschlossen. *Berliner Morgenpost*. https://www.morgenpost.de/berlin/article103914505/Klaus-Kinskis-Akten-bleiben-verschlossen.html.

Aodha, G. N. (2019, 10 July). For the first time, you can write a message for future generations on the Census. *The Journal*. https://www.thejournal.ie/census-2021-time-capsule-4718938-Jul2019/.

Apostolic Letter Issued Motu Proprio by the Supreme Pontiff Francis "Vos Estis Lux Mundi" (2019, 7 May).

Arbeitshilfe. Erstellung eines Dokumentationsprofils für Kommunalarchive. Beschluss der BKK von 2008-09-15/16 in Erfurt. (2009). *Der Archivar*, 62, 122–132. https://www.bundeskonferenz-kommunalarchive.de/empfehlungen/Arbeitshilfe_Dokumentationsprofil.pdf.

Archives et coopération européene: enjeux, projets et perspectives. Les données personnelles, entre fichiers nominatifs et jungle Internet. (2009). La Gazette des archives, 215(3).

Archives nationales. *Rapport d'activité* 2014.

Archives nationales. *Rapport d'activité* 2015. http://www.archives-nationales.culture.gouv.fr/documents/10157/11405/Rapport-d-activite-2015.pdf/1c9cf41e-7094-4f90-b257-4211023eecdb.

Archives nationales. *Rapport d'activité* 2019. http://www.archives-nationales.culture.gouv.fr/documents/10157/11405/Rapport+d%27activit%C3%A9%20des+AN+-+2019/652514a1-a16f-4852-91f0-118fc2dec805.

ARK-Arbeitsgruppe. (Mai 2008). Bewertung von Statistikunterlagen. Abschlussbericht. https://www.bundesarchiv.de/DE/Content/Downloads/KLA/abschlussbericht-statistikunterlagen.pdf?__blob=publicationFile.

Article 29 data protection working party. (2014). Opinion 05/2014 on Anonymisation Techniques. 0829/14/EN. WP216. Adopted on 10 April 2014. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.

Association of Records Managers and Administrators. (1992). *The code of professional responsibility.* https://www.usna.edu/Users/cs/adina/teaching/it360/spring2013/ethics/ARMACodeOfProfessionalResponsibility.pdf.

Association of Records Managers and Administrators. *Code of ethics.* https://www.arma.org/page/IGP_Ethics#.

Australian Bureau of Statistics. (2011a, 28 April). *2903.0 – How Australia takes a census, 2011.* https://www.abs.gov.au/ausstats/abs@.nsf/lookup/2903.0Main%20Features52011.

Australian Bureau of Statistics. (2011b, 4 August). *Census time capsule – it's time!.* https://www.abs.gov.au/websitedbs/censushome.nsf/home/CO-42.

Australian Bureau of Statistics. (July 2006). *2902.0 – Census update (Newsletter).* https://www.abs.gov.au/ausstats/abs@.nsf/7d12b0f6763c78caca257061001cc588/ea2223b65f7787aaca2573210017ede3!OpenDocument.

Australian Catholic Bishops Conference and Catholic Religious Australia's Response to the Royal Commission into Institutional Responses to Child Sexual Abuses. (August 2018). https://www.catholic.org.au/acbc-media/media-centre/media-releases-new/2139-acbc-and-cra-response-to-the-royal-commission/file.

Barry, R. (2005). Ethics issues for creators, managers, and users of records. In M. Procter, M. Cook, & C. Williams (Eds.), *Political pressure and the archival record* (pp. 131–149). Society of American Archivists.

Becker, I. C., & Rehm, C. (Eds.). (2017). *Archivrecht für die Praxis. Ein Handbuch.* MUR-Verlag.

Benedict, K. M. (2003). *Ethics and the archival profession: Introduction and case studies.* Society of American Archivists.

Bensoussan, A. (sous la dir. de). (2018). *Règlement européen sur la protection des données. Textes, commentaires et orientations pratiques.* Bruylant.

Bierce, A. (1890, 5 January). The Major's Tale. First published as: A Practical Joke: Major Broadwood Recalls the Heroic Past. *San Francisco Examiner.*

Blais, G. (1995). *Access to archival records. A review of current issues. A RAMP study.* UNESCO.

Blanke, H.-J., & Perlingeiro, R. (Eds.). (2018). *The right of access to public information. An international comparative legal survey*. Springer. https://doi.org/10.1007/978-3-662-55554-5

Booms, H. (1972). Gesellschaftsordnung und Überlieferungsbildung – Zur Problematik archivarischer Quellenbewertung. *Archivalische Zeitschrift, 68*, 3–40.

Booms, H. (1991–92). Uberlieferungsbildung: Keeping Archives as a Social and Political Activity. *Archivaria*, 33 (Winter), 25–33. https://archivaria.ca/index.php/archivaria/article/view/11796.

Braibant, G. (Ed.). (1996). *Les Archives en France: Rapport au Premier ministre*. La Documentation française (Collection des rapports officiels). https://www.vie-publique.fr/sites/default/files/rapport/pdf/964093000.pdf.

Buchmann, W., & Wettengel, M. (1996). Auslegung des Bundesstatistikgesetzes bei der Archivierung von Statistikunterlagen. *Der Archivar, 49*(1), 67–74.

Buitelaar, J. C. (2017). Post-mortem privacy and informational self-determination. *Ethics and Information Technology, 19*, 129–142.

Bundesbeauftragte für den Datenschutz und die Informationsfreiheit. Volkszählung 2011. https://www.bfdi.bund.de/DE/Datenschutz/Themen/Melderecht_Statistiken/VolkszaehlungArtikel/Volkszaehlung.html.

Bütikofer, N. (1995). Bewertung als Priorisierung. *Arbido, 10*(11), 14–16.

Canada shares Residential School documents with National Centre for Truth and Reconciliation. (2022). https://www.canada.ca/en/crown-indigenous-relations-northern-affairs/news/2022/01/canada-shares-residential-school-documents-with-national-centre-for-truth-and-reconciliation.html.

Census Time Capsule delivered to the National Archives vaults today. (2007, 13 September). *Joint media release from Australian Bureau of Statistics and National Archives of Australia*. https://www.abs.gov.au/AUSSTATS/abs@.nsf/mediareleasesbyReleaseDate/FE3AE1DF58707778CA257354007FC7D9?OpenDocument.

Central Statistics Office. (2019, 10 July). *Press Statement Census 2021 date and questions approved by Government*. Press Statement.

Central Statistics Office. *Census through history*. https://www.cso.ie/en/census/censusthroughhistory/.

The National Archives. (2019a). *Closure periods*. https://www.nationalarchives.gov.uk/documents/information-management/closure-periods.pdf.

Cobain, I. (2016). *The history thieves*. Portobello Books.

Codex Iuris Canonici (CIC), 1983.

Cofone, I. N. (Ed.). (2020). *The right to be forgotten. A Canadian and comparative perspective*. Routledge. https://doi.org/10.4324/9781003017011

Combe, S. (1994). Archives interdites. Les peurs françaises face à l'histoire contemporaine. .

Combe, S. (2013). Confiscated histories. Access to sensitive government records and archives in France. *Zeithistorische Forschungen/Studies in Contemporary History*, *10*(1), 123–130. https://zeithistorische-forschungen.de/1–2013/id=4435.

Commission of Investigation. (July 2009). *Report into the Catholic Archdiocese of Dublin*. http://www.justice.ie/en/JELR/Pages/PB09000504.

Commonwealth of Pennsylvania. Office of Attorney General. (2018). *Report I of the 40th statewide investigating grand jury*. Redacted By order of PA Supreme Court 27 July 2018. https://www.attorneygeneral.gov/wp-content/uploads/2018/08/A-Report-of-the-Fortieth-Statewide-Investigating-Grand-Jury_Cleland-Redactions-8-12-08_Redacted.pdf.

Commonwealth of Pennsylvania. Office of Attorney General. (March 2016). *A report of the thirty-seventh statewide investigating grand jury*. http://www.bishopaccountability.org/reports/2016_03_01_Pennsylvania_Grand_Jury_Report_on_Diocese_of_Altoona_Johnstown.pdf.

Cook, M. (2006). Professional ethics and practice in archives and records management in a human rights context. *Journal of the Society of Archivists, 27*(1), 1–15.

Cook, T. (1996). Building an archives: Appraisal theory for architectural records. *The American Archivist, 59*(Spring), 136–143.

Cook, T. (1997). What is past is prologue: A history of archival ideas since 1898, and the future paradigm shift. *Archiv*, *43*(Spring), 17–63. https://archivaria.ca/index.php/archivaria/article/view/12175.

Cook, T. (2005). Macroappraisal in theory and practice: Origins, characteristics, and implementation in Canada, 1950–2000. *Archival Science, 5*, 101–161. https://doi.org/10.1007/s10502-005-9010-2

Cook, T. (April 1991). *The archival appraisal of records containing personal information: A RAMP study with guidelines*. PGI-91/WS/3. Paris.

Court as the European Court of Human Rights. (2021). *Guide to the case-law of the European court of human rights: Data protection*. Updated on 31 December 2021. https://www.echr.coe.int/Documents/Guide_Data_protection_ENG.pdf.

Čtvrtník, M. (2011a). Die Theorie von der "macroappraisal" im Sinne Terry Cooks und die Frage der archivischen Bewertung. *Archivalische Zeitschrift, 92*, 73–98. https://doi.org/10.7788/az.2011.92.1.73

Čtvrtník, M. (2011b). Terry Cook. *Archivní časopis [Journal on Archives], 61*(1), 79–87.

Čtvrtník, M. (2012). Eric Ketelaar. *Archiwista Polski*, *67*(3), XVII, 129–137.

Čtvrtník, M. (2014a). Máme právo být zapomenuti?! [Do we have the right to be forgotten?!]. *Archivní časopis* [*Journal on Archives*], 64(2), 190–191.

Čtvrtník, M. (2014b). Zrušení § 37 archivního zákona a vylidnění dějin [Repeal of Section 37 of the Archives Act and the depopulation of history]. *Archivní časopis [Journal on Archives], 64*(4), 356–360.

Čtvrtník, M. (2014c, 6 September). Vylidnění dějin [Depopulation of history]. *Lidové noviny*, p. 22/IV (Orientace supplement).

Čtvrtník, M. (2018). Právo být (ne)zapomenut. Výmazy dějin, inflace historických pramenů, ochrana soukromí, vy(zne)užívání dat a prekérní situace archivů v mladém 21. století—podněty k diskusi [The right to be (not) forgotten. Erasure of history, inflation of historical sources, protection of privacy, (mis)use of data and the precarious situation of archives in the early 21st century—stimuli for discussion]. *Archivní časopis [Journal on Archives], 68*(3), 266–297.

Čtvrtník, M. (2019). "Spolehlivé, správné, pravé—demokracie potřebuje archivy!". 88. německý archivní sjezd v Rostocku 2018 ["Reliable, correct, true—democracy needs archives!". 88th German Archival Congress, Rostock 2018]. *Archivní časopis [Journal on Archives], 69*(3), 295–314.

Čtvrtník, M. (2021a). Closure periods for access to public records and archives. Comparative-historical analysis. *Archival Science, 21*(4), 317–351. https://doi.org/10.1007/s10502-021-09361-4

Čtvrtník, M. (2021b). Public versus private status of records and archives and analysis of the implications for their access. An example demonstrating top political representatives of political power in the United States, France and Germany. *Archival Science*, 2021. https://doi.org/10.1007/s10502-021-09375-y.

Čtvrtník, M. (2022). Classified records and the archives. *Archival Science*, 2022, 129–165. https://doi-org.ezproxy.lib.cas.cz/10.1007/s10502-021-09370-3.

De Baets, A. (2004). A declaration of the responsibilities of present generations toward past generations. *History & Theory, 43*(4), 130–164.

De Baets, A. (2009). *Responsible history*. Berghahn Books, pp. 173–196.

De Groot, J. (2020, 1 December). The history of data breaches. *Digital Guardian*. https://digitalguardian.com/blog/history-data-breaches.

De Montjoye, Y.-A., Hidalgo, C. A., Verleysen, M., & Blondel, V. D. (2013). Unique in the Crowd: The privacy bounds of human mobility. *Scientific Reports, 3*, 1376. https://doi.org/10.1038/srep01376

De Vries, K., Bellanova, R., Hert, P. D., Gutwirth, S. (2011). The German constitutional court judgment on data retention: Proportionality overrides unlimited surveillance (doesn't it?). In *Computers, privacy and data protection: an element of choice* (pp. 3–23). https://doi.org/10.1007/978-94-007-0641-5_1.

DeCew, J. (2018). Privacy. In *The Stanford encyclopedia of philosophy*. Spring 2018 Edition. https://plato.stanford.edu/archives/spr2018/entries/privacy/.

Déclaration du Président de la République sur la mort de Maurice Audin. (2018, 13 September). https://www.elysee.fr/front/pdf/elysee-module-950-fr.pdf.

Department of Health. (November 2003). *Confidentiality. NHS code of practice*. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/200146/Confidentiality_-_NHS_Code_of_Practice.pdf.

Department of Health. (November 2010). *Confidentiality: NHS code of practice. Supplementary guidance: Public interest disclosures*. https://assets.publishing.

service.gov.uk/government/uploads/system/uploads/attachment_data/file/216476/dh_122031.pdf.

Derrida, J. (1995). *Mal d'archive. Une impression freudienne.* Galilée.

Des Archives en France – 2005. L'activité de la direction des Archives de France et des services publics d'archives. (2006). https://francearchives.fr/file/b742bae0d42bc0accdefb6c7905ec591fb5c6f5a/static_1176.pdf.

Des Archives en France. L'activité des services d'archives 2019. (2019). https://francearchives.fr/file/6d139a81db2d82b09aedc3ed2828c6cbb57f7a53/BD-rapport-2019-2020-ArchivesenFrance.pdf.

Deutsche Bischofskonferenz. FAQ zur MHG-Studie. https://www.dbk.de/themen/sexueller-missbrauch/faq-mhg-studie/.

Die Bevölkerung des Deutschen Reichs nach den Ergebnissen der Volkszählung 1933. Heft 5: Die Glaubensjuden im Deutschen Reich. (1936). Verlag für Sozialpolitik, Wirtschaft und Statistik.

Doležal, D. (2016). Malé zamyšlení nejen nad jedním výsledkem generální inventury 2012–13. K situaci českých archivů na příkladu SOA Praha [A brief reflection not only on the result of one stocktaking 2012–2013. On the situation of Czech archives using the example of SOA in Prague]. *Archivní časopis [Journal on Archives], 66*(3), 262.

Duclert, V. (1999). Les historiens et les archives. Introduction à la publication du rapport de Philippe Bélaval sur les Archives nationales. *Genèses. Sciences sociales et histoire*, *36. Amateurs et professionnels*, 132–146.

Duclert, V. (2001). Les historiens et la crise des archives. *Revue d'histoire moderne & contemporaine, 5*(48-4bis), 16–43.

Duclert, V. (2003). La politique actuelle des archives. In S. Laurent (sous la dir.), *Archives "secrètes", secrets d'archives. L'historien et l'archiviste face aux archives sensibles* (pp. 21–56). CNRS Éditions.

Dumschat, S. (2007). Archiv oder "Mülleimer"? Das "NS-Archiv" des MfS der DDR und seine Aufarbeitung im Bundesarchiv. *Archivalische Zeitschrift*, *89*, 119–146. https://doi.org/10.7788/az-2007-jg05. https://www.bundesarchiv.de/DE/Content/Downloads/Aus-unserer-Arbeit/ns-archiv-des-mfs1.pdf?__blob=publicationFile.

Edwards, L., & Harbinja, E. (2013). Protecting post-mortem privacy: Reconsidering the privacy interests of the deceased in a digital world. *Cardozo Arts & Entertainment Law Journal, 32*(1), 83–130.

EFE. (28 November 2017). Encuentran una cápsula del tiempo oculta dentro del trasero de un Cristo del XVIII. *El Mundo*. https://www.elmundo.es/f5/comparte/2017/11/28/5a1d5fd7468aebc0358b4599.html.

Epping, V. (2010). *Grundrechte*. Springer.

European Archives Group. (October 2018). *Guidance on data protection for archive services. EAG guidelines on the implementation of the General Data*

Protection Regulation in the archive sector. https://ec.europa.eu/info/sites/info/files/eag_draft_guidelines_1_11_0.pdf.

European Commission. Shaping Europe's digital future. *eHealth*. https://digital-strategy.ec.europa.eu/en/policies/ehealth.

European Union Agency for Fundamental Rights. (2018). *Experiences and perceptions of antisemitism. Second survey on discrimination and hate crime against Jews in the EU*. https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-experiences-and-perceptions-of-antisemitism-survey-summary_en.pdf.

Exner, G. (2002). Die Volkszählung von 1939 in Deutschland und Österreich – ein Beitrag zum Holocaust? *Austrian Journal of Statistics, 31*(4), 249–256.

Farge, A. (2013). *The allure of the archives*. Yale University Press.

Forsyth, F. (2010). *The Cobra*. G. P. Putnam's Sons.

Franz, E. G. (1984). The archivist and the inflation of contemporary records. In *Conférence internationale de la table ronde des archives, 22ème, Bratislava, 17–20 October 1983*. Conseil international des archives, French version pp. 19–52, English version pp. 117–145.

Friesen, I. (2020). Rückblick auf das Jahr 2019. Jahresbericht des Landesarchivs Baden-Württemberg. *Archivnachrichten*, *60*, 36–42, https://www.la-bw.de/media/full/69705.

Fuchs, P., Rotzoll, M., Müller, U., Richter, P., & Hohendorf, G. (Eds.). (2007). *"Das Vergessen der Vernichtung ist Teil der Vernichtung selbst". Lebensgeschichten von Opfern der nationalsozialistischen "Euthanasie"*. Wallstein-Verlag.

Galland, B. (2018). Le procès de Klaus Barbie, entre archives, témoignage et éthique. *La Gazette des archives, 249*(1), 163–177.

Gambs, S., Killijian, M.-O., & del Prado Cortez, M. N. (2014). De-anonymization attack on geolocated data. *Journal of Computer and System Sciences, 80*(8), 1597–1614. https://doi.org/10.1016/j.jcss.2014.04.024

Gasnault, F. (2013). L'affaire du "fichier juif", ou l'éveil d'une nouvelle sensibilité documentaire. In D. Fabre (sous la dir.), *Émotions patrimoniales* (pp. 237–258). Éditions de la Maison des sciences de l'homme, Ministère de la Culture.

Ghezzi, A, Guimarães Pereira, Â., & Vesnić-Alujević, L. (Eds.). (2014). *The ethics of memory in a digital age. Interrogating the right to be forgotten*. Palgrave Macmillan.

Gieseke, J. (Ed.). (2011). *Die Stasi 1945–1990*. Pantheon.

Glaudemans, A., Jonker, R., & Smit, F. (2014). Beyond the traditional boundaries of archival theory. An interview with Eric Ketelaar. In F. Smit, A. Glaudemans, & R. Jonker (Eds.), *Archives in liquid times* (pp. 294–305). Stichting Archiefpublicaties.

Gloutnay, F. (2019, 27 March). *Abus sexuels: ce que pourraient révéler les archives diocésaines*. https://presence-info.ca/article/societe/abus-sexuels-ce-que-pourraient-reveler-les-archives-diocesaines/.

Greenberg, A. (2009, 24 November). The Year Of The Mega Data Breach. *Forbes*.

Grundsätze der Wertermittlung für die Aufbewahrung und Kassation von Schriftgut der sozialistischen Epoche in der DDR. (1965). Staatliche Archivverwaltung.

Grütters, M. (2019). Grußwort anlässlich des Festaktes "100 Jahre Reichsarchiv" am 22. Oktober 2019 im Deutschen Historischen Museum in Berlin. *Forum 2019. 100 Jahre Reichsarchiv*. Bundesarchiv. https://www.bundesarchiv.de/DE/Content/Publikationen/Forum/forum-2019.pdf?__blob=publicationFile, 7–10.

Guibert, N. (2019, 5 February). La marine va rechercher l'épave du sous-marin "Minerve". *Le Monde*.

Guideline for the E-ARK Content Information Type Specification for eHealth1 (CITS eHealth1). (2021, 1 February). https://dilcis.eu/images/2020review/18_Draft_Guideline_CITS_eHealth1.pdf.

Guptil, M. B. (1986). *Evaluation et tri des documents d'archives dans les organisations internationales: Une étude RAMP accompagnée de principes directeurs*. Programme général d'information et UNISIST. UNESCO.

Hacker claims to have stolen 1 bln records of Chinese citizens from police. (2022, July 6). *Reuters*. https://www.reuters.com/world/china/hacker-claims-have-stolen-1-bln-records-chinese-citizens-police-2022-07-04/.

Hammerschmidt, P. (2014). *Deckname Adler. Klaus Barbie und die westlichen Geheimdienste*. S. Fischer.

Handbook on European data protection law. (2018). Publications Office of the European Union. https://doi.org/10.2811/343461.

Hänger, A. (2019). Die Geschichte des Bundesarchivs. *Forum 2019. 100 Jahre Reichsarchiv*. Bundesarchiv, 107–116. https://www.bundesarchiv.de/DE/Content/Publikationen/Forum/forum-2019.pdf?__blob=publicationFile.

Hao, K., Liang, R. (2022, 4 July). Vast cache of Chinese police files offered for sale in alleged hack. *The Wall Street Journal*. https://www.wsj.com/articles/vast-cache-of-chinese-police-files-offered-for-sale-in-alleged-hack-11656940488.

Harbinja, E. (2017). Post-mortem privacy 2.0: Theory, law, and technology. *International Review of Law, Computers & Technology, 31*(1), 26–42. https://doi.org/10.1080/13600869.2017.1275116

Harris, V. (1999). Knowing right from wrong: The archivist and the protection of people's rights. *Janus, 1*, 32–38.

Health and Social Care Information Centre. (2014). *Code of practice on confidential information*. https://digital.nhs.uk/binaries/content/assets/legacy/pdf/8/9/copconfidentialinformation.pdf.

Herrmann, T. (2013). Das Bundesarchiv in Zahlen. *Forum 2013*, I–IV. https://www.bundesarchiv.de/DE/Content/Publikationen/Forum/forum-2013.pdf?__blob=publicationFile.

Het Koninkrijk der Nederlanden in de Tweede Wereldoorlog. (1969). *Deel 6. Tweede helft Juli '42 – mei '43. Rijksinstituut voor oorlogsdocumentatie.*

Heymann, N. (2009, 28 April). Kinskis Krankenakte soll für immer zu bleiben. *Der Tagesspiegel.* https://www.tagesspiegel.de/berlin/stadtleben/datenschutz-kinskis-krankenakte-soll-fuer-immer-zu-bleiben/1800012.html.

Hirschprung, R. S., & Leshman, O. (2021). Privacy disclosure by de-anonymization using music preferences and selections. *Telematics and Informatics, 59*, 101564. https://doi.org/10.1016/j.tele.2021.101564

Hoffman, S., & Podgurski, A. (2013). The use and misuse of biomedical data: is bigger really better? *American Journal of Law & Medicine, 39*(4), 497–538.

Hollmann, M. (2001). Das "NS-Archiv" des Ministeriums für Staatssicherheit der DDR und seine archivische Bewältigung durch das Bundesarchiv. *Mitteilungen aus dem Bundesarchiv, 9*(3), 53–62.

Hora, J., & Wanner, M. (2015). Národní dědictví v roce 2015 [National Archival Heritage in 2015]. *Archivní časopis [Journal on Archives], 65*(3), 252–271.

House of Representatives Committees. Standing Committee on Legal and Constitutional Affairs. (May 1998). *Saving our census and preserving our history.* https://www.aph.gov.au/parliamentary_business/committees/house_of_representatives_committees?url=/laca/inquiryincensus.htm http://www.archives-nationales.culture.gouv.fr/documents/10157/11405/Rapport_d'activit%C3%A9_2014_des_Archives_nationales_%28France%29.pdf/9a5ea923-ac06-4c67-a983-fd0e2aceac60 http://www.nzdl.org/gsdlmod?e=d-00000-00%2D%2D-off-0hdl%2D%2D00-0%2D%2D%2D%2D0-10-0%2D%2D-0%2D%2D-0direct-10%2D%2D-4%2D%2D%2D%2D%2D%2D%2D-0-1l%2D%2D11-en-50%2D%2D-20-about%2D%2D-00-0-1-00-0%2D%2D4%2D%2D%2D%2D0-0-11-10-0utfZz-8-10&cl=CL1.1&d=HASHe14ace1b9d178e777de9c9.8&gt=2.

Hudson, P. S. *The "archaeological duty" of Thornwell Jacobs: The oglethorpe atlanta crypt of civilization time capsule.* https://crypt.oglethorpe.edu/history/detailed-history/.

Hugo, V. (1832). Guerre aux démolisseurs. *Revue des Deux Mondes.* Période Initiale, t. 5, 1832, 607–622.

Hurley, Ch. (2002). Recordkeeping, Document Destruction, and the Law (Heiner, Enron and McCabe). *Archives & Manuscripts, 30*(2), 6–25. https://publications.archivists.org.au/index.php/asa/article/view/9597.

Chabin, M.-A. (2017, 17 September). Détruire ou conserver les données sensibles… il y a 70 ans. *Petit éclairage historique pour la mise en œuvre du Règlement général pour la protection des données personnelles (RGPD).* https://www.marieannechabin.fr/2017/09/detruire-ou-conserver-les-donnees-sensibles-il-y-a-70-ans/.

Chief data officer. (2018, 21 February). *De-identification Guideline*. Issued by the Chief data officer on 21 February 2018 under section 33 of the Victorian Data sharing act 2017. https://www.vic.gov.au/sites/default/files/2019-03/Victorian-Data-Sharing-Act-2017-De-identification-guidelines.pdf.

Iacovino, L., & Todd, M. (2007). The long-term preservation of identifiable personal data: A comparative archival perspective on privacy regulatory models in the European Union, Australia, Canada and the United States. *Archival Science, 7*, 107–127. https://doi.org/10.1007/s10502-007-9055-5

IBM Security. *Cost of a data breach report* 2020. https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/pdf.

IDC's Global DataSphere Forecast Shows Continued Steady Growth in the Creation and Consumption of Data. (2020, 8 May). https://www.businesswire.com/news/home/20200508005025/en/IDCs-Global-DataSphere-Forecast-Shows-Continued-Steady-Growth-in-the-Creation-and-Consumption-of-Data.

In the European Court of Human Rights. Application No. 57292/16 between Hurbain and Belgium. Written Comments of Article 19: Global Campaign for Free Expression, Centre for Democracy and Rule of Law, Prof. David Kaye, Digital Security Lab Ukraine, Electronic Frontier Foundation, The European Centre for Press & Media Freedom, Guardian News Media Limited, The Helsinki Foundation for Human Rights, The Human Rights Centre of Ghent University, The Hungarian Civil Liberties Union, International Press Institute, Times Newspapers Ltd, Mass Media Defence Centre, Media Defence, Nyugat, Open Net Association. (2022, 21 January). http://www.concernedhistorians.org/content_files/file/le/731.pdf.

Information and Privacy Commissioner of Ontario. (June 2016). *De-identification guidelines for structured data*. https://www.ipc.on.ca/wp-content/uploads/2016/08/Deidentification-Guidelines-for-Structured-Data.pdf.

Information Commissioner's Office (ICO). (2013). *The prejudice test. Freedom of information act*. https://ico.org.uk/media/for-organisations/documents/1214/the_prejudice_test.pdf.

Information Commissioner's Office (ICO). (n.d.-a). *Information Provided in Confidence (Section 41). Freedom of Information Act*. https://ico.org.uk/media/for-organisations/documents/1432163/information-provided-in-confidence-section-41.pdf.

Information Commissioner's Office (ICO). (n.d.-b). *Information about the deceased*. Freedom of Information Act. Environmental Information Regulations. https://ico.org.uk/media/for-organisations/documents/1202/information-about-the-deceased-foi-eir.pdf.

Information Commissioner's Office (ICO). (n.d.-c). *The Public Interest Test*. Freedom of Information Act. https://ico.org.uk/for-organisations/guidance-

index/freedom-of-information-and-environmental-information-regulations/the-public-interest-test/.

Institut für Urheber- und Medienrecht: Rechtsstreit um Krankenakte von Klaus Kinski endet mit Vergleich. (2009, 29 April). http://www.urheberrecht.org/news/3625/.

Instrukce Ministerstva spravedlnosti ze dne 19. prosince 2008, č. j. 94/2007-OIS-ST, kterou se vydává skartační řád pro okresní, krajské a vrchní soudy. Příloha č. 1 Spisový a skartační plán [Instruction of the Ministry of Justice of 19 December 2008, 94/2007-OIS-ST, issuing the retention schedule for district, regional, and high courts. Appendix 1 Records Retention Schedule].

International Council on Archives. (1996). *ICA code of ethics.*

Jenkinson, H. (1922). *A manual of archival administration*. Clarendon Press.

Jones, M. L. (2016). *Ctrl + Z. The right to be forgotten*. New York University Press.

Kafsack, H. (2015, 18 December). Im Tausch gegen Daten. *Frankfurter Allgemeine*. http://www.faz.net/aktuell/wirtschaft/netzwirtschaft/was-taugt-die-eu-datenschutz-verordnung-13972055.html.

Kahlenberg, F. P. (1972). Aufgaben und Probleme der Zusammenarbeit von Archiven verschiedener Verwaltungsstufen und Dokumentationsbereichen in Bewertungsfragen. *Der Archivar, 25*(1), 57–70.

Kahn, A. (1993). *Le fichier*. Robert Laffont.

Keitel, Ch. (2019a). Archivcamp "Volkszählung 2021 und Rolle der digitalen Archive". In *23. Tagung des Arbeitskreises Archivierung von Unterlagen aus digitalen Systemen* (pp. 167–168). National Archives (Prague). https://www.nacr.cz/wp-content/uploads/2019/12/KnihaAUDS_e-kniha_DEF.pdf.

Keitel, Ch. (2019b). Statistik im Archiv – Eine schwierige Beziehung. In *23. Tagung des Arbeitskreises Archivierung von Unterlagen aus digitalen Systemen* (pp. 169–176). National Archives (Prag). https://www.nacr.cz/wp-content/uploads/2019/12/KnihaAUDS_e-kniha_DEF.pdf.

Kerr, O. (2017, 15 August). A closer look at DOJ's warrant to collect website records. *Washington Post*. https://www.washingtonpost.com/news/volokh-conspiracy/wp/2017/08/15/a-closer-look-at-dojs-warrant-to-collect-website-records/?utm_term=.395abbf5952d.

Ketelaar, E. (1995). The right to know, the right to forget? Personal information in public archives. *Archives & Manuscripts, 23*(1), 8–17.

Ketelaar, E. (1998a, 23 October). Archivalization and archiving. Unpublished inaugural address as Chair of Archivistics, University of Amsterdam. As cited In V. Harris, Knowing right from wrong: the archivist and the protection of people's rights. *Janus*, *1*, 32–38.

Ketelaar, E. (1998b, 3 October). *Professional ethics: The moral defence of the archivist*. Paper presented at the conference "Cyber, Hyper or Resolutely Jurassic? Archivists and the Millennium". University College Dublin.

Ketelaar, E. (2000). Archivistics research saving the profession. *The American Archivist, 63*(Fall/Winter), 322–340. https://doi.org/10.17723/aarc.63.2.0238574511vmv576

Ketelaar, E. (2001). Tacit narratives: The meanings of archives. *Archival Science, 1*, 131–141. https://doi.org/10.1007/BF02435644

Ketelaar, E. (2005). Recordkeeping and societal power. In S. McKemmish, M. Piggott, B. Reed, & F. Upward (Eds.), *Archives: Recordkeeping in society* (pp. 277–298). Charles Sturt University.

Ketelaar, E. (2012). Cultivating archives: Meanings and identities. *Archival Science, 12*, 19–33. https://doi.org/10.1007/s10502-011-9142-5

Kistenich-Zerfaß, J. (2018). Überlieferungsbildung, Erschließung und Nutzung im gesellschaftspolitischen Fokus: Der Bestand "Odenwaldschule" im Hessischen Staatsarchiv Darmstadt. *Conference: Verlässlich, richtig, echt: Demokratie braucht Archive! 88*. Deutscher Archivtag in Rostock.

KLA-Arbeitsgruppe. (June 2016). *Bewertung von Statistikunterlagen. Abschlussbericht*. https://www.bundesarchiv.de/DE/Content/Downloads/KLA/abschlussbericht-bewertung-statistikunterlagen.pdf?__blob=publicationFile.

Klarsfeld, S. (1996, 6 July). *L'embarras de la commission Rémond*. .

Körting, E. (2014, 1 July). Namennennung von Opfern der NS Euthanasie von 1939 bis 1945. *Expert opinion*. https://www.gedenkort-t4.eu/sites/default/files/media/file/gutachten_namensnennung_copyright_erhart_koerting.pdf.

Kotlorz, T. (2008, 22 July). Krankenakten werden möglicherweise wieder geschlossen. *Die Welt*. https://www.welt.de/regionales/berlin/article2240109/Krankenakten-werden-moeglicherweise-wieder-geschlossen.html.

Kretzschmar, R. (2006). Das Landesarchiv Baden-Württemberg im ersten Jahr seines Bestehens. Jahresbericht für 2005. *Archiv*, *32*, 12–15. https://www.landesarchiv-bw.de/media/full/44485.

Kretzschmar, R. (Ed.). (2002). *Methoden und Ergebnisse archivübergreifender Bewertung*. Verband deutscher Archivarinnen und Archivare e. V. Frankfurt a.M.: Selbstverlag.

Kunze, A. (2013, 31 October). Behandelt und verkauft. Ärzte und Apotheker geben die Kranken- und Rezeptdaten von Millionen Patienten weiter – ohne deren Wissen. Es ist ein dickes Geschäft. *Die Zeit*. https://www.zeit.de/2013/45/patientendaten-marktforschung-pharmaindustrie.

L'affaire du "fichier juif". (2020, 5 October). *France culture*. https://www.franceculture.fr/emissions/lsd-la-serie-documentaire/politique-et-race-en-france-un-mariage-dangereux-14-episode-1-laffaire-du-fichier-juif.

Lambert, P. (2017). *Understanding the new European data protection rules*. CRC Press.

Lambert, P. (2019). *The right to be forgotten: interpretation and practice*. Bloomsbury Professional. https://doi.org/10.5040/9781526510136.

Landesarchiv Baden-Württemberg – Eröffnungsbilanz und Betriebsergebnisse. (2005). http://www.landesarchiv-bw.de/sixcms/media.php/120/Eroeffnungsbilanz_und_Betriebsergebnisse_2005.pdf.

Landesbeauftragter für Datenschutz und Informationsfreiheit Nordrhein-Westfalen. (2015). *Zweiundzwanzigster Datenschutz- und Informationsfreiheitsbericht des Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen Ulrich Lepper für die Zeit vom 1. Januar 2013 bis zum 31. Dezember 2014.* https://www.ldi.nrw.de/system/files/media/document/file/22_dib.pdf.

Lauder, R. S. (2019, 25 October). In Birthplace of Nazism, "Never Again" Must Really Mean "Never Again". *Frankfurter Allgemeine Zeitung*. https://www.faz.net/aktuell/feuilleton/debatten/in-birthplace-of-nazism-never-again-must-really-mean-never-again-16449527.html?printPagedArticle=true#pageIndex_2.

Le "Fichier Juif". Rapport de la Commission présidée par René Rémond au Premier ministre. (1996). Plon.

Lemay, Y., & Boucher, M.-P. (2010–2011). L'émotion ou la face cachée de l'archive. 6e symposium du Groupe interdisciplinaire de recherche en archivistique (GIRA). *Archiv*, *42*(2), 39–52.

Lemoine, H. (2016, 27 May). *#EUdataP: 3 ans après le début de la mobilisation*. http://www.archivistes.org/EUdataP-3-ans-apres-le-debut-de-la-mobilisation.

Lemoine, H., & Ricard, B. (2018). Les données personnelles dans les archives publiques françaises. Loi, accès et sécurité. In K. Van Honacker (Ed.), *The right to be forgotten vs the right to remember*. VUBPRESS Brussels University Press.

Lépine, Ch. (2019, 27 March). *Agressions Sexuelles Faire La Lumière*. https://plus.lapresse.ca/screens/bf9f1586-e3ef-4be6-a215-ee24dd05b616__7C___0.html?utm_medium=Facebook&utm_campaign=Microsite+Share&utm_content=Screen&fbclid=IwAR23nBcZLXws4oGGMSxVnklLx8g7yYnD2fbQCwb6DL1uKB4N6KkMgFn-shY.

Les espaces du musée-mémorial. http://www.memorialdelashoah.org/le-memorial/les-espaces-du-musee-memorial/la-crypte-et-le-fichier-juif.html.

Letter of agreement between Department of Veterans Affairs: veterans benefits administration (VBA) and National Archives and Records Administration (NARA). (2019, 9 August). https://www.archives.gov/files/digitization/pdf/va-letterofagreement-final-signed.pdf.

Library and Archives Canada. (2006–2007). *Report on plans and priorities*. http://www.tbs-sct.gc.ca/rpp/2006-2007/lac-bac/lac-bac-eng.pdf.

Limon-Bonnet, M.-F. (2014). Le régime des dérogations. In S. Monnier, K. Fiorentino (Sous la dir.), *Le droit des archives publiques, entre permanence et mutations*. La Gazette des archives, *234*(2), 29–45.

Lockwood, E. (1990). "Imponderable Matters": The influence of new trends in history on appraisal at the national archives. *The American Archivist, 53*(Summer), 394–405. https://doi.org/10.17723/aarc.53.3.w66t31032j7528t4

Lord, N. (2020, 28 September). Top 10 biggest healthcare data breaches of all time. *Digital Guardian*. https://digitalguardian.com/blog/top-10-biggest-healthcare-data-breaches-all-time.

Lübben, V. (2019). Stolperfallen im Netz. Postmortaler Persönlichkeitsschutz und die Belange von Hinterbliebenen. In I. Christa Becker, C. Rehm, & U. Schäfer (Eds.), *Nicht nur Archivgesetze… Archivarinnen und Archivare auf schwankendem rechtlichem Boden? Best Practice – Kollisionen – Perspektiven. Beiträge zum 22. Archivwissenschaftlichen Kolloquium der Archivschule Marburg* (pp. 151–169).

MacNeil, H. (1992). *Without consent. The ethics of disclosing personal information in public archives*. Society of American Archivists, Scarecrow Press.

Malin, B. (2006). Re-identification of familial database records. *AMIA Annual Symposium Proceedings Archive*, 524–528.

Mallet, J. (2018). Les dérogations générales. 31 January 2018. https://siafdroit.hypotheses.org/764.

Mas, S., & Gagnon-Arguin, L. (2010–2011). Considérations sur la dimension émotive des documents d'archives dans la pratique archivistique. La perception des archivistes. 6e symposium du Groupe interdisciplinaire de recherche en archivistique (GIRA). *Archiv*, *42*(2), 53–64.

Mas, S., & Klein, A. (2010–2011). L'émotion: une nouvelle dimension des archives. Contexte et résumé des exposés du 6e symposium du GIRA tenu le mercredi 3 novembre 2010 au Palais des Congrès de Montréal. *Archives*, *42*(2), 5–8.

Mates, P., et al. (Eds.). (2019). *Ochrana osobnosti, soukromí a osobních údajů*. Leges.

Mayer, D. (1985). The new social history: Implications for archivists. *The American Archivist*, *48*(Fall), 388–399. https://doi.org/10.17723/aarc.48.4.l107660916858k13

Mayer, T. S. (2002). *Privacy and confidentiality research and the US census bureau. Recommendations based on a review of the literature*. Research Report Series (Survey Methodology #2002–01). https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.8.3379&rep=rep1&type=pdf.

Mayer-Schönberger, V. (2009). *Delete: The virtue of forgetting in the digital age*. Princeton University Press.

McCallig, D. (2014). *Data protection and the deceased in the EU*. Paper presented at the Computers Privacy Data Protection. Brussels 2014. As cited in: Buitelaar, J. C. (2017). Post-mortem privacy and informational self-determination. *Ethics and Information Technology*, *19*, 129–142.

Metz, A. (2019). Die Rechte der Nachkommen – oder: Schutz jenseits der Schutzfristen und die Konsequenzen für die Benutzung von Archivalien.

Conference contribution at: RECHTsicher – Archive und ihr rechtlicher Rahmen. 89. Deutscher Archivtag in Suhl.

Miller, F. (1981). Social history and archival practice. *The American Archivist, 44*(Spring), 113–124. https://doi.org/10.17723/aarc.44.2.r5x54qq0r71275w4

Miller, F. (1986). Use, appraisal, and research: A case study of social history. *The American Archivist, 49*(Fall), 371–392. https://doi.org/10.17723/aarc.49.4.e1251j7r1125525n

Mills, T. (May 2005). *Strategic approaches to appraisal. In international council on archives. Guidelines on appraisal*. https://www.ica.org/sites/default/files/CAP_2005_guidelines_appraisal_EN.pdf.

Moore, T. (2014, 2 July). No Heiner trial for Goss ministers: Bleijie. *Brisbane Times*. https://www.brisbanetimes.com.au/national/queensland/no-heiner-trial-for-goss-ministers-bleijie-20140702-zstrm.html.

Moore, T. (2021, 1 January). Goss cabinet knew it destroyed documents wanted for court case. *Brisbane Times*. https://www.brisbanetimes.com.au/politics/queensland/goss-cabinet-knew-it-destroyed-documents-wanted-for-court-case-20201230-p56qw9.html.

Morgan, L. W. (2001). Strengthening the lock on the bedroom door: The case against access to divorce court records on line. *Journal of the American Academy of Matrimonial Lawyers, 17*, 45–67. https://cdn.ymaws.com/aaml.org/resource/collection/F5239802-0DED-4BAC-9F7E-AC93E2DB4D4D/strengthening_the_lock_on-17-1.pdf.

Mourby, M., et al. (2018). Are 'pseudonymised' data always personal data? Implications of the GDPR for administrative data research in the UK. *Computer Law & Security Review, 34*(2), 222–233. https://doi.org/10.1016/j.clsr.2018.01.002

Müller-Enbergs, H. (2008). *Inoffizielle Mitarbeiter des Ministeriums für Staatssicherheit. Teil 3: Statistiken*. Ch. Links. https://www.bstu.de/assets/bstu/de/Publikationen/E_Mueller-Enbergs_Inoffizielle_Teil3.pdf.

Müller-Enbergs, H. (2011). *Inoffizielle Mitarbeiter des Ministeriums für Staatssicherheit. Teil 2: Anleitungen für die Arbeit mit Agenten, Kundschaftern und Spionen in der Bundesrepublik Deutschland*. Ch. Links.

Müller-Enbergs, H. (2012). *Inoffizielle Mitarbeiter des Ministeriums für Staatssicherheit. Teil 1: Richtlinien und Durchführungsbestimmungen*. Ch. Links.

Murray, S. (2020, 20 October). The CSO has alerted the gardaí after extracts from the 1926 Census were published on social media. *The Journal*. https://www.thejournal.ie/cso-1926-census-5238786-Oct2020/.

Mutch, S. (2001). Public Policy Revolt: Saving the 2001 Australian Census. *Archives and Manuscripts, 30*(2), 26–44.

NARA Statement Regarding Defective CMRS Disk Drive. (2009, 13 October). *Press release*. https://www.archives.gov/press/press-releases/2010/nr10-05.html.

Narayanan, A., & Shmatikov, V. (2008). Robust De-anonymization of Large Sparse Datasets. *2008 IEEE symposium on security and privacy* (sp 2008), 111–125. https://doi.org/10.1109/SP.2008.33.

Narayanan, A., Shmatikov, V. (2009). De-anonymizing Social Networks. *2009 30th IEEE Symposium on Security and Privacy*, 173–187. https://doi.org/10.1109/SP.2009.22.

National Archives and Records Administration. (2010, 4 January). Statement on Notification Letters relating to PII Information from Clinton Hard Drive. *Press Release*. https://www.archives.gov/press/press-releases/2010/nr10-41.html?_ga=2.116140486.152971816.1604912356-605976007.1604912356.

National Archives and Records Administration. (2013). *Annual Report 2013: Preserving the past to protect the future. Summary. National Archives and Records Administration. Performance and Accountability Report*. https://www.archives.gov/files/about/plans-reports/performance-accountability/2013/par-summary.pdf.

National Archives and Records Administration. (n.d.). *Fact Sheet Regarding the National Archives and Records Administration Breach of a Hard Drive Containing Personally Identifiable Information (PII)*. https://www.archives.gov/files/press/press-releases/2010/pdf/nara-breach-notification-faq-2010-01-12.pdf.

National Archives Warns Former Clinton Staff, Visitors of Major Data Breach. (2015, December 23). *Fox News*. https://www.foxnews.com/politics/national-archives-warns-former-clinton-staff-visitors-of-major-data-breach.

Neazor, M. (2008). Recordkeeping Professional Ethics and their Application. *Archivaria*, 64 (April), 47–87. https://archivaria.ca/index.php/archivaria/article/view/13146.

Nečasová, E. (2006). *Cui bono restituce?*. Český svaz bojovníků za svobodu.

Nečasová, E. (2007). *Cui bono restituce II*. Český svaz bojovníků za svobodu.

Neethling, J. (2006). Personality rights (entry). In J. M. Smits (Ed.), *Elgar encyclopedia of comparative law* (pp. 530–547). Edward Elgar.

Nietzsche, F. (1988). O užitku a škodlivosti historie pro život. In: F. Nietzsche, *Nečasové úvahy*. Athenaeum, 83–171.

Nietzsche, F. (1997). On the uses and disadvantages of history for life. In: F. Nietzsche, *Untimely meditations*. Cambridge University Press.

Nietzsche, F. (2001). *Radostná věda* [*The Gay Science*]. Aurora.

Nora, P. (1984). Entre Mémoire et Histoire. La problematique des lieux. In P. Nora (sous la dir.), *Les Lieux de mémoire, vol. 1 (La République)* (pp. XVII–XLII). Gallimard.

Norwegians' digital health data to be preserved for future generations (2019, 30 January). https://www.piql.com/news/norwegians-digital-health-data-to-be-preserved-for-future-generations/.

Nougaret, Ch. (2017). *Une stratégie nationale pour la collecte et l'accès aux archives publiques à l'ère numérique. Rapport à Madame Audrey Azoulay, Ministre de la Culture et de la Communication*. (2017, 24 March). https://francearchives.fr/file/b0d6555950508ab637adb10ece33d381644d6d37/2017_03_24_RAPPORT_DEFINITIF_NOUGARET.compressed.pdf.

Office of the Information Commissioner Queensland. (2020, 9 July, last updated). *Privacy and de-identified data. Guideline Information privacy act 2009*. 1 February 2019. https://www.oic.qld.gov.au/__data/assets/pdf_file/0007/38644/Privacy-and-de-identification.pdf.

One in Four US Consumers Have Had Their Healthcare Data Breached, Accenture Survey Reveals (2017, 20 February). *Accenture*. https://newsroom.accenture.com/subjects/technology/one-in-four-us-consumers-have-had-their-healthcare-data-breached-accenture-survey-reveals.htm.

Pánek, J. (2020, 7 February). Justiční aktivista dostal pokutu 50 tisíc za databázi soudních jednání [Judicial activist fined 50,000 for court hearings database]. *Idnes*. https://www.idnes.cz/zpravy/domaci/tomas-pecina-databaze-soudnich-jednani-archivace-data-jmena-urad-osobni-udaje.A200207_075022_domaci_iri.

Pérotin, Y. (1961). L'administration et les "trois âges" des archives. *Seine et Paris, 20*(October), 1–4.

Peschanski, D. (1997). Le fichier juif. Table ronde. *La Gazette des archives*, 177–178. *Transparence et secret. L'accès aux archives contemporaines*, 241–249.

Posner, E. (1972). *Archives in the ancient world*. Harvard University Press.

Poznanski, R. (1997). Le fichage des juifs de France pendant la Seconde Guerre mondiale et l'affaire du fichier des juifs. *Gazette des archives*, 177–178. *Transparence et secret. L'accès aux archives contemporaines*, 250–270.

Preissmann, D. (2016). Mémoire et oubli: Un éclairage de la psychologie et des neurosciences. *Arbido, 3*, 4–7.

Principles for Determining the Access Status of Records on Transfer. (2019). *The national archives*. https://www.nationalarchives.gov.uk/documents/information-management/principles-for-determining-the-access-status-of-records-on-transfer.pdf.

Příkaz Úřadu na ochranu osobních údajů [The Office for Personal Data Protection Order], ref. no. UOOU-05226/19–3 of 5 February 2020.

Report on Archives in the enlarged European Union. Increased archival cooperation in Europe: action plan. (2005). Office for Official Publications of the European Communities. https://ec.europa.eu/transparency/regdoc/rep/1/2005/EN/1-2005-52-EN-F1-2.Pdf.

Rescriptum ex audientia SS.MI: Rescritto del Santo Padre Francesco con cui si promulga l'Istruzione Sulla riservatezza delle cause. (2019, 17 December).

Review of Statutory Prohibitions on Disclosure, Department for Constitutional Affairs. (2005). https://webarchive.nationalarchives.gov.uk/ukgwa/+/http://www.dca.gov.uk/StatutoryBarsReport2005.pdf.

Robinson, J. (2020, 9 September). US Healthcare Data Breach Statistics. *Privacy Affairs*. https://www.privacyaffairs.com/healthcare-data-breach-statistics/.

Rohr, W. (1958). Zur Problematik des modernen Aktenwesens. *Archivalische Zeitschrift, 54*, 74–89.

Rocher, L., Hendrickx, J. M., & de Montjoye, Y.-A. (2019). Estimating the success of re-identifications in incomplete datasets using generative models. *Nature Communications, 10*, 3069. https://doi.org/10.1038/s41467-019-10933-3

Rossi, L., & Vinagre e Silva, P. (2017). *Public access to documents in the EU*. Hart Publishing.

Roth, M. (2016, 29 June). *Bericht zur Tagung "Den Opfern einen Namen geben"*. https://www.holocaustliteratur.de/deutsch/Den-Opfern-einen-Namen-geben-Gedenken-und-Datenschutz-im-Zusammenhang-mit-der-F6ffentlichen-Nennung-der-Namen-von-NS-Opfern-in-Ausstellungen2C-Gedenkbuechern-und-Datenbanken-2039/.

Rottmann, V. S. (1987). Volkszählung 1987 – wieder verfassungswidrig? *Kritische Justiz, 20*(1), 77–87.

Royal Commission into Institutional Responses to Child Sexual Abuse. (2017a). *Final Report, Recordkeeping and information sharing*, vol. 8. Commonwealth of Australia. https://www.childabuseroyalcommission.gov.au/sites/default/files/final_report_-_volume_8_recordkeeping_and_information_sharing.pdf.

Royal Commission into Institutional Responses to Child Sexual Abuse. (2017b). *Final Report. Religious Institutions*, vol. 16, Book 1. Commonwealth of Australia. https://www.childabuseroyalcommission.gov.au/sites/default/files/final_report_-_volume_16_religious_institutions_book_1.pdf.

Sante, G. W. (1957). Archive und Verwaltung – historische Provenienz und Probleme der Gegenwart. *Der Archivar, 10*, 7–16.

Sante, G. W. (1958). Behörden – Akten – Archive. Alte Taktik – neue Strategie. *Archivalische Zeitschrift, 54*, 90–96.

Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R., Khan, R. A. (2020). Healthcare Data Breaches: Insights and Implications. *Healthcare* (Basel), 133 June 8(2). https://doi.org/10.3390/healthcare8020133.

Sexueller Missbrauch an Minderjährigen durch katholische Priester, Diakone und männliche Ordensangehörige im Bereich der Deutschen Bischofskonferenz. Projektbericht. (2018, 24 September). https://www.dbk.de/fileadmin/redaktion/diverse_downloads/dossiers_2018/MHG-Studie-gesamt.pdf.

Schäfer, U. (1997). Die Pflicht zur Anbietung und Übergabe von Unterlagen in der archivarischen Praxis. In R. Kretzschmar (Ed.), *Historische Überlieferung aus Verwaltungsunterlagen. Zur Praxis der archivischen Bewertung in Baden-Württemberg* (pp. 35–46). Kohlhammer.

Schäfer, U. *Vertikale und horizontale Bewertung der Unterlagen der Wasserwirtschaftsvervaltung in Baden-Württemberg*. https://www.landesarchiv-bw.de/media/full/46752.

Schellenberg, T. R. (1956, October). The Appraisal of Modern Records. *Bulletins of the National Archives*, 8.

Schellenberg, T. R. (2003). *Modern archives. Principles and techniques*. Society of American Archivists.

Schlebaum, P. (2019, 1 September). *Raid on the population registry of Amsterdam*. https://www.tracesofwar.com/articles/5329/Raid-on-the-Population-Registry-of-Amsterdam.htm.

Schulten, S. (2014, 20 November). Sherman's Maps. *The New York Times*.

Singel, R. (2009, 10 January). Probe targets archives' handling of data on 70 million vets. *Wired*. https://www.wired.com/2009/10/probe-targets-archives-handling-of-data-on-70-million-vets/.

Smith, C. (1998). Review commentary. Saving our census and preserving our history: Report of the House of Representatives Standing Committee on Legal and Constitutional Affairs. *Archives and Manuscripts, 26*(2), 410–417.

Society of American Archivists. *Code of ethics for archivists*. Approved by the SAA Council, February 2005; revised, January 2012 and August 2020 https://www2.archivists.org/statements/saa-core-values-statement-and-code-of-ethics.

Solove, D. J., & Schwartz, P. M. (2018). *Information privacy law*. Wolters Kluwer.

Staples, W. G. (Ed.). (2007). *Encyclopedia of privacy*. Greenwood Press.

Statista. (3 December 2020). *Volume of data/information created, captured, copied, and consumed worldwide from 2010 to 2024*. https://www.statista.com/statistics/871513/worldwide-data-created/.

Státní oblastní archiv v Praze. (2017). *Zpráva o činnosti za rok 2016* [State Regional Archives in Prague, *Activity Report 2016*]. http://www.soapraha.cz/Files/vyrocni-zprava-soa-2016.pdf.

Stein, L. (1997, 5 June). ADL to Aid Swiss Bank Guard Who Turned over Documents. *Jewish Telegraphic Agency*. https://www.jta.org/1997/06/05/lifestyle/adl-to-aid-swiss-bank-guard-who-turned-over-documents.

Swiss end bank guard investigation. (1997, 2 October). *Washington Post*. https://www.washingtonpost.com/archive/politics/1997/10/02/swiss-end-bank-guard-investigation/5bc310f0-c2ba-4f99-a92f-bdab58240798/.

Székely, I. (2017). Does it matter where you die? Chances of post-mortem privacy in Europe and in the United States. In D. J. B. Svantesson & D. Kloza (Eds.), *Trans-Atlantic data privacy relations as a challenge for democracy* (pp. 313–320). Intersentia.

Šimůnková, K., & Šisler, M. (2019). Zur Problematik der elektronischen Archivierung von Volkszählungen 2011 und 2021 in der Tschechischen Republik. In *23. Tagung des Arbeitskreises Archivierung von Unterlagen aus*

digitalen Systemen (pp. 177–183). National Archives. Prague 2019. https://www.nacr.cz/wp-content/uploads/2019/12/KnihaAUDS_e-kniha_DEF.pdf.

Tagung "Archive und Aufarbeitung sexuellen Kindesmissbrauchs". Unabhängige Kommission zur Aufarbeitung sexuellen Kindesmissbrauchs, Darmstadt 2019. https://www.aufarbeitungskommission.de/meldung-27-03-2019-tagung-archive/.

The National Archives of Ireland. History of Irish census records. http://www.census.nationalarchives.ie/help/history.html.

The National Archives, Intelligence and security services. https://www.nationalarchives.gov.uk/help-with-your-research/research-guides/intelligence-and-security-services/#5-mi5-and-mi6-records.

The National Archives, the Society of Archivists, the Records Management Society and the National Association for Information Management. (2007). *Code of Practice for Archivists and Records Managers under Section 51(4) of the Data Protection Act 1998.* https://cdn.nationalarchives.gov.uk/documents/information-management/dp-code-of-practice.pdf.

The National Archives. (2011, 24 March, last updated). *Guide 8: Disposal of records.* http://www.nationalarchives.gov.uk/documents/information-management/rm-code-guide8.pdf.

The National Archives. (2012). *Annual report and accounts of the national archives 2011–12.* https://www.nationalarchives.gov.uk/documents/annualreport-11-12.pdf.

The National Archives. (2013). *Annual report and accounts of the national archives 2012–13.* https://www.nationalarchives.gov.uk/documents/annual-report-12-13.pdf.

The National Archives. (2014). *Annual report and accounts of the national archives 2013–14.* https://www.nationalarchives.gov.uk/documents/annual-report-13-14.pdf.

The National Archives. (2015). *Annual report and accounts of the national archives 2014–15.* https://www.nationalarchives.gov.uk/documents/annual-report-2014-15.pdf.

The National Archives. (2016a). *Annual report and accounts of the national archives 2015–16.* https://www.nationalarchives.gov.uk/documents/annual-report-and-accounts-2015-2016.pdf.

The National Archives. (2016b, reviewed 2019). *Freedom of information exemptions.* https://www.nationalarchives.gov.uk/documents/information-management/freedom-of-information-exemptions.pdf.

The National Archives. (2018a). *Annual report and accounts of the national archives 2017–18.* https://www.nationalarchives.gov.uk/documents/the-national-archives-annual-report-and-accounts-2017-18.pdf.

The National Archives. (2019b). *Annual report and accounts of the national archives 2018–19*. https://www.nationalarchives.gov.uk/documents/the-national-archives-annual-report-and-accounts-2018-19.pdf.

The National Archives. (2020). *Annual report and accounts of the national archives 2019–20*. https://www.nationalarchives.gov.uk/documents/annual-report-accounts-2019-2020.pdf.

The National Archives. (August 2018b). *Guide to archiving personal data*. https://www.nationalarchives.gov.uk/documents/information-management/guide-to-archiving-personal-data.pdf.

The National Archives' ability to safeguard the nation's electronic records. Hearing before the Subcommittee in information policy, census, and National Archives of the Committee on oversight and Government reform. (2009). House of Representatives. 111 Congress. First Session. November 5, 2009. Serial No. 111–63.

The Righteous Among the Nations Database, Willem Arondeus (Johannes Arondeus), 1894–1943. https://righteous.yadvashem.org/?searchType=righteous_only&language=en&itemId=4043044&ind=NaN.

The Universal Declaration on Archives. (2010). Endorsed by 36th Session of the General Conference of UNESCO Paris, 10 November 2011. Adopted at the General Assembly of ICA Oslo, September 2010.

Thénault, S., & Besse, M. (Eds.). (2019). *Réparer l'Injustice: l'Affaire Maurice Audin. Institut francophone pour la justice et la démocratie*. Institut francophone pour la justice et la démocratie.

Todd, M. (2006). Power, identity, integrity, authenticity, and the archives: A comparative study of the application of archival methodologies to contemporary privacy. *Archiv, 61*(Spring), 181–214.

Transparence et secret. L'accès aux archives contemporaines. La Gazette des archives, 177–178.

Treffeisen, J. (2003). The development in Germany of archival processing – The vertical and horizontal appraisal. *Archival Science, 3*(4), 345–366. https://doi.org/10.1007/s10502-004-2273-1

Tūbaitė-Stalauskienė, A. (2018). Data protection post-mortem. *International Comparative Jurisprudence, 4*(2), 97–104.

U.S. National Archives and Records Administration. National Archives Frequently Asked Questions. http://www.archives.gov/faqs/.

Uhl, B. (1994). Die Geschichte der Bewertungsdiskussion. In A. Wettmann (Ed.), *Bilanz und Perspektiven archivischer Bewertung. Beiträge eines Archivwissenschaftlichen Kolloquiums* (pp. 11–36).

UNESCO (General Information Programme and UNISIST). (1982). *Survey of archival and records management systems and services 1982*. PGI-82/WS/3. https://unesdoc.unesco.org/ark:/48223/pf0000048252.

United Nations. *Records and information management guidance 5: When and how can I destroy records?* https://archives.un.org/sites/archives.un.org/files/5-guidance_destroying_records.pdf.

United States Government Accountability Office. (October 2010). *GAO-11-15. Report to the ranking member, committee on finance, U.S. Senate. National archives and records administration. Oversight and Management Improvements Initiated, but More Action Needed.* https://www.gao.gov/assets/gao-11-15.pdf.

Unverhau, D. (Ed.). (2003). *Hatte "Janus" eine Chance? Das Ende der DDR und die Sicherung einer Zukunft der Vergangenheit.* Lit.

Unverhau, D. (Ed.). (2004). *Das "NS-Archiv" des Ministeriums für Staatssicherheit. Stationen einer Entwicklung.* Lit.

Valeska D. (2016, 8 February). Insulting a politician right after her death: Does the ECHR protect the reputation of the deceased? *Strasbourg Observers.* https://strasbourgobservers.com/2016/02/08/insulting-a-politician-right-after-her-death-does-the-echr-protect-the-reputation-of-the-deceased/#_ftn1.

Van Eecke, P., & Craddock, P. (2018). The right to be forgotten… and to remember (section Conclusion and recommendations). In K. Van Honacker (Ed.), *Right to be forgotten vs the right to remember: Data protection and archiving in the public interest.* VUBPRESS Brussels University Press.

Van Honacker, K. (Ed.). (2018). *The right to be forgotten vs the right to remember.* VUBPRESS Brussels University Press.

Vandevorde, É. (Ed.). (2005). La communication des archives. De la communication à l'accessibilité. .

Vavra, A. N. (2018). The Right to be forgotten: An archival perspective. *The American Archivist*, 81(1) (Spring/Summer), 100–111.

Vernichten um zu bewahren? Détruire pour conserver? Distruggere per conservare? (2016). Arbido, 3. https://arbido.ch/assets/files/arbido_2016_3_low_161127_132457.pdf.

Villaronga, E. V., Kieseberg, P., & Li, T. (2018). Humans forget, machines remember: Artificial intelligence and the right to be forgotten. *Computer Law & Security Review, 34*(2), 304–313. https://doi.org/10.1016/j.clsr.2017.08.007

Volkszählungen in Berlin seit Bestehen des Statistischen Amtes der Stadt Berlin. (2012). *Zeitschrift für amtliche Statistik Berlin Brandenburg*, 1+2, 36–57.

Von Cranach, M., Eberle, A., Hohendorf, G., & von Tiedemann, S. (2018). *Gedenkbuch für die Münchner Opfer der nationalsozialistischen "Euthanasie"-Morde.* Wallstein-Verlag.

Vrbata, J. (1979). K některým obecným otázkám výběru archiválií [On some general issues of archival selection]. *Zpravodaj Pobočky ČSVTS SÚA, 14*, 12–67.

Werro, F. (Ed.). (2020). *The right to be forgotten. A comparative study of the emergent right's evolution and application in Europe, the Americas, and Asia*. Springer. https://doi.org/10.1007/978-3-030-33512-0

Wietog, J. (2001). *Volkszählungen unter dem Nationalsozialismus*. Duncker und Humblot.

Wilson, K. (Ed.). (1996). *Forging the collective memory. Government and international historians through two world wars*. Berghahn Books.

Yang, Z., Wang, R., Luo, D., & Xiong, Y. (2020). Rapid re-Identification risk assessment for anonymous data set in mobile multimedia scene. *IEEE Access, 8*, 41557–41565. https://doi.org/10.1109/ACCESS.2020.2977404

Zang, H., Bolot, J. (2011). Anonymization of location data does not work: A large-scale measurement study. In *MobiCom '11: Proceedings of the 17th annual international conference on Mobile computing and networking*. September 2011, 145–156. https://doi.org/10.1145/2030613.2030630.

Zimmermann, N. M. Die Ergänzungskarten für Angaben über Abstammung und Vorbildung der Volkszählung vom 17. Mai 1939. *Vortrag auf dem Workshop "Datenbanken zu Opfern der nationalsozialistischen Gewaltherrschaft in Deutschland 1933–1945"*. https://www.bundesarchiv.de/DE/Content/Publikationen/Aufsaetze/aufsatz-zimmermann-ergaenzungskarten.pdf?__blob=publicationFile.

Archival Fonds

Archives nationales (Paris, France). Premier ministre; Organismes rattachés directement; Mission de réflexion sur les archives en France (Mission Braibant) (1995–1996). ID: 20000520/6–20000520/7, cotes 12 and 13.

Odenwaldschule (OSO), 1880–2015, HStAD Bestand N 25, Hessisches Staatsarchiv Darmstadt.

The National Archives (Kew, UK). PRO 42. Advisory Council on Public Records. (1959–1986). PRO 42/21: Advisory Council Series – Memoranda.

The National Archives (Kew, UK). PRO 42. Advisory Council on Public Records. (1959–1986). PRO 42/23: Access to records and introduction of thirty-year rule.

The National Archives (Kew, UK). PRO 42. Advisory Council on Public Records. (1959–1986). PRO 42/45: Minutes of meetings (1969–1976).

The National Archives (Kew, UK). PRO 42. Advisory Council on Public Records. (1959–1986). PRO 42/50: Memoranda: AC [69]1 – AC [72] 9.

The National Archives (Kew, UK). PRO 42. Advisory Council on Public Records. (1959–1986). PRO 42/50: Memoranda.

The National Archives (Kew, UK). PRO 42. Advisory Council on Public Records. (1959–1986). PRO 42/64: Memoranda: AC [77] 1 – AC [81] 13.

The National Archives (Kew, UK). PRO 42. Advisory Council on Public Records. (1959–1986). PRO 42/57: Correspondence and papers: Access to public records.

The National Archives (Kew, UK). PRO 42. Advisory Council on Public Records. (1959–1986). PRO 42/75: Memoranda: AC [84] 1 – AC [83] 21.

The National Archives (Kew, UK). PRO 42. Advisory Council on Public Records. (1959–1986). PRO 42/77: Access to public records.

The National Archives. PRO 70. Public Record Office: Lord Chancellor's Instruments: Retention by Department under Public Records Act 1958. (1982–2003). PRO 70/58: Retention of Public Records.

The National Archives. PRO 70. Public Record Office: Lord Chancellor's Instruments: Retention by Department under Public Records Act 1958. (1982–2003). PRO 70/66: Retention of Public Records.

The National Archives (Kew, UK). CAB. Records of the Cabinet Office. CAB 184/401: Disclosure of official information.

Index[1]

[1] Note: Page numbers followed by 'n' refer to notes.

M. Čtvrtník, *Archives and Records*,
https://doi.org/10.1007/978-3-031-18667-7