European Holocaust Research Infrastructure
H2020-INFRAIA-2019-1
GA no. 871111

Deliverable 3.2

Report on impact of GDPR

Dirk Luyten
SAB/CEGES

Emmanuelle Moscovitz
YV

Zohar Neumann
YV

Julia Parfiniewicz
ZIH

Rachel Pistol
KCL

Roxana Poppa
INSHR-EW

Frank Uiterwaal
NIOD-KNAW

Anna Ullrich
IfZ

Start: January 2021 [M5]
Due: August 2022 [M24]
Actual: October 2022 [M26]

EHRI is funded by the European Union

Document Information

Project URL	www.ehri-project.eu
Document URL	https://www.ehri-project.eu/deliverables-ehri-3-2020-2024
Deliverable	D3.2 Report on impact of GDPR
Work Package	WP3
Lead Beneficiary	2- SAB/CEGES
Relevant Milestones	MS3
Dissemination level	Public
Contact Person	Dirk Luyten dirk.luyten@arch.be
Abstract (for dissemination)	This deliverable gives an overview of the national legislations implementing article 89 of the GDPR in those countries where EHRI-3 has a partner. Article 89 of the GDPR allows derogations for processing of personal data for archiving in the public interest and for scientific, historical research and statistical purposes, on the condition that the national or the European legislator provides for appropriate safeguards for the rights and freedoms of the data subjects. In practice, it is the national legislator which has implemented these safeguards. This deliverable lists the national laws in the EU-member states where EHRI has a partner and in the UK and in Israël and briefly discusses the different safeguards in these national laws. The deliverable includes the results of a survey with the collection institutions partner in EHRI-3 on the practical implementation of the GDPR and relevant national law.
Management Summary	n.a.

Table of Contents

1 Introduction

The objective of this deliverable is twofold: to understand which rules have been implemented in national law for processing of personal data for (historical) research purposes and for archiving in the public interest and to assess the impact on the access to Holocaust archives and on Holocaust research. This also includes the question if national legislators have used the possibility offered by recital 158 of the GDPR to implement specific provisions for Holocaust research[1].

The General Data Protection Regulation (GDPR), which came into force in May 2018 in the European Union and repealed Directive 95/46/EC, changed the regime of personal data protection at some points and moreover tends to bring more uniformity in personal data protection within the EU. In contrast to a directive, a regulation has direct legal effect in the national legal order of the EU member states and since implementing national legislation is thus in principle no longer needed, there is less room for differences in data protection regimes between different countries as was the case with the Directive 95/46/EC. Most of the mechanisms for personal data protection as for instance the obligation for certain organizations or institutions to appoint a data protection officer or the obligation to, in some cases, keep a register of processing activities are uniform in the EU.

There remain however still fields of personal data protection in which transposition to national law is needed to implement the GDPR in a specific country. Two of these fields are the processing of personal data, more in particular special categories of personal data, for research purposes – including historical research - and for archiving in the public interest. The conditions for processing personal data for these purposes are laid down in art 89 of the GDPR. This article makes processing of personal data for these purposes depending on the putting in place of appropriate safeguards for the rights and the freedoms of the data subject and allows to derogate from articles 15 (right of access), 16 (right to rectification), 18 (right to restriction of processing) and 21 (right to object) in case personal data are processed for historical research purposes and also from article 19 (notification obligation regarding rectification, erasure or restriction of processing) and 20 (data portability) for processing for archiving in the public interest [2]. These safeguards can, according to art 89 of the GDPR, be implemented by Union law or by national law, but it appears that these safeguards have been put in place by national legislators, in personal data protection laws or alternatively in archival law.

The scope of the overview of national law implementing the GDPR are EU-member states in which the EHRI-3 consortium has a partner[3]. Further, we also consider the United Kingdom, which is after Brexit in a specific situation and Israel, which is an associated country of the EU and therefore indirectly impacted by the GDPR.

[1] 'Regulation (EU) 2016/679 of the European Parliament and 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)' in, *Official Journal of the European Union, Legislation. Volume 59*, 4 May 2016, Recital 158.

[2] 'Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016, Art 89.

[3] Austria, Belgium, Czech Republic, France, Germany, Greece, Hungary, Italy, Lithuania, the Netherlands, Poland, Romania Slovakia.

First, we will provide an overview of the national legislations pertaining to protection of processing of personal data implementing art 89 of the GDPR. This overview is based on desk research of the relevant legal texts. The aim of this overview is to focus on the general principles of the different legislations, rather than to offer a complete and detailed analysis the law concerned.

Second, in order to understand the practical implementation of the GDPR and of national law in an archival context, a survey was organized with the collection holding institutions that are partners in the EHRI-3 consortium. This survey focuses on the experiences of the collection holding institutions with the effects of the GDPR and national data protection legislation / archival law on access to Holocaust archives and Holocaust research. The results of this survey are analyzed in the third section of this deliverable.

2 National legislations

2.1 National legislations: general overview

Article 89 (1) of the GDPR defines in a general way the appropriate safeguards to be put into place for processing of personal data for (historical) research purposes and archiving in the public interest. The article mentions: technical and organizational measures, data minimization and pseudonymization[4]. These are general principles, but how are these principles made concrete in the different national legislations? Before answering this question, it is interesting to note that different types of law are used in EU-member states to implement the principles of art 89 GDPR.

Most often used is a national privacy law with a general reach, such as the GDPR itself. An example is **Belgium**: the law of 30 July 2018 'pertaining to the protection of physical persons with regard to the processing of personal data' is a general law, which is clearly not limited to the processing of personal data in one specific context. The law covers both the public and the private sectors and specific services as the passengers information unit (in the context of international travel) or the office for the coordination of threat assessment (in the context of anti-terrorism)[5]. The regime for processing of personal data for (historical) research purposes and for archiving in the public interest is also laid down in this law, but it is just one of the different domains covered by this so-called 'framework law'.

The same is true for **Greece**, where provisions regarding (historical) research and archiving in the public interest can be found Law nr 4624 of 29 August 2019 with the measures of the Hellenic Data Protection Authority for implementing the GDPR[6]. In **Romania** the implementation of art 89 is provided for in article 8 of the law on implementing measures to the GDPR[7]. In **Slovakia**, the situation is comparable to Romania, to the extent that

[4] 'Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016, art 89 (1).

[5] 'Loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel. 30 juillet 2018' in, *Moniteur Belge*, 5 septembre 2018, p. 68616-68684.

[6] 'Law nr 4624. Hellenic Data Protection Authority (HDPA), measures for implementing 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 transposition of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016, and other provisions' in, *Government Gazette of the Hellenic Republic*, 29 August 2019.

[7] Law no. 190/2018 on implementing measures to 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

processing of personal data for historical research purposes and archiving in the public interest is governed by the act of 29 November 2017 on personal data protection and amending and supplementing certain acts[8]. In **Austria**, the Datenschutzgesetz of 2018, a national privacy law as well, provides for the implementation of art 89 GDPR[9].

Italy has a 'personal data protection code' to adapt the national legislation to the GDPR, which has a general scope as well[10]. But this code should be combined with the Code of Cultural and Landscape Heritage, which contains provisions for the protection of personal data held by archival institutions[11].

In **France** a similar solution has been opted for. In the '*Loi Informatique et Libertés*' (Law Information technology and liberties), which initially traces back to 1978, title 2 contains the provisions regarding the implementation of the GDPR. However, as for historical research and archiving in the public interest, this title 2 is implemented further in archival law (*code du patrimoine et les autres dispositions législatives et réglementaires applicables aux archives publiques*) and in a decree of the for historical research[12].

In the **Netherlands**, the relevant law is the Implementation Act ("UAVG", "Uitvoeringswet Algemene verordening gegevensbescherming") of 16 May 2018, more in particular articles 44 for research and article 45 for archiving in the public interest[13]. Relevant as well is the Dutch archival law, which is currently under revision and will contain more detailed provisions concerning access to archives and processing of personal data[14].

In **Germany**, rules pertaining to archiving in the public interest and historical research are part of the federal data protection act[15]. However, archival laws should be considered as well, since according to German law, protection of personal data is not limited to living persons and as a consequence, archival law has special protection periods for personal archival records.

(General Data Protection Regulation). /www.dataprotection.ro/servlet/ViewDocument?id=1685 (Consulted 8 August 2022).

[8] 'ACT of 29 November 2017 on personal data protection and amending and supplementing certain Acts'https://dataprotection.gov.sk/uoou/sites/default/files/2019_10_03_act_18_2018_on_personal_data_protection_and_amending_and_supplementing_certain_acts.pdf (Consulted on 26 July 2022).

[9] ‚Bundesgesetz, mit dem das Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz – DSG) geändert wird' in, *Bundesgesetzblatt für die Republik Österreich,* 15. Mai 2018.

[10] Personal data protection code. Containing provisions to adapt the national legislation to 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, https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9740796. (Consulted on 26 July 2022).

[11] Code of the Cultural and Landscape Heritage. Legislative decree n° 42 of 11 January 2004.

[12] Loi informatique et libertés 17 juin 2019.

[13] Wet van 16 mei 2018, houdende regels ter uitvoering van Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PbEU 2016, L 119) (Uitvoeringswet Algemene verordening gegevensbescherming) in, *Staatsblad van het Koninkrijk der Nederlanden*, 22 mei 2018.

[14] Marieke Klomp, Veelgestelde vragen. Openbaarheid bij archiefdiensten 23 november 2021. https://kia.pleio.nl/blog/view/a6f732ea-6211-440a-b642-3b91f3107e20/veelgestelde-vragen-openbaarheid-bij-archiefdiensten (consulted 06 July 2022).

[15] Bundesdatenschutzgesetz vom 30. Juni 2017 https://www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.html.

The **Czech Republic** has issued since April 2019 an act on personal data processing, of which section 16 covers the processing of personal data for (historical) research purposes. There are no specific provisions for archiving in the public interest[16].

In **Lithuania** the law on legal protection of personal data as amended in June 2018 is to be considered as a national privacy law, but it does not contain specific provisions pertaining to archiving in the public interest or historical research, as a consequence, in the Lithuanian law is no exception defined for historical research[17].

In **Poland** the act of 10 May 2018 on the protection of personal data, does not contain specific provisions for processing of personal data for historical research purposes or for archiving in the public interest neither, except that according to article 9 research institutes are under the obligation to appoint a data protection officer[18].

In **Hungary**, the relevant law is the act CXII of 2011 on the right to informational self-determination and on the freedom of information, the Hungarian 'privacy-law'[19].

For the **United Kingdom**, the Data Protection Act of May 2018 is the relevant law[20]. This law is a national privacy law with a general reach, containing specific provisions for archiving in the public interest and historical research. As a consequence of Brexit, the legal situation is somewhat specific in the sense that the GDPR has been incorporated, with some changes, in the legal order of the United Kingdom with the UK GDPR since 1st January 2021[21].

In **Israel**, data protection is governed primarily by the Protection of Privacy Law, 5741-1981 as well as regulation enacted such as the Privacy Protection (Data Security) Regulations, 5777-2017. These are enforced by the Privacy Protection Authority. The law covers collection and use of personal data and sensitive data, sets the rights and obligations of the parties collecting and using the data, including security requirements with respect thereto, and sets the rights afforded to individuals whose data is collected and used.

The Privacy Law applies to all entities that hold or process electronic personal data. This includes the private, business and public sector. Other legislations impact data protection such as the Basic Law: Human Dignity and Liberty, 5752-1992 (Basic Law). These laws refer specifically to personal data and do include certain restrictions on publishing personal data - however, there is no specific reference as to the use of personal data in Archiving and Research. Thus, the Privacy laws must be considered together with the Archives Law, 1955 as well as the Archives Regulations (Access to archived materials held in the Archive), 2010.

Although the GDPR impacted the Protection of Privacy Regulations of 2017, the GDPR does not apply in Israel and there is no concurring law to art 89 GDPR in the Israeli privacy legislation. Moreover, there is no synergy between the Archives Law and the National Privacy law. It should be noted that efforts to update both the National Privacy law and the Archives law are currently under way in Israel. In addition, the Martys' and Heroes Remembrance Law (Yad Vashem) 5713-1953, under which specifically Yad Vashem abides,

[16] Act of 12 March 2019 on personal data processing

[17] 'Law on legal protection of personal data' in, *TAR*, 2018-07-11, Nr. 11733.

[18] 'Act of 10 May 2018 on the protection of personal data' in, *Journal of Laws of the Republic of Poland,* 2019, item 1781.

[19] Act CXII of 2011 on the right to informational self-determination and on the freedom of information (as in force on 1 January 2022) (https://www.naih.hu/about-the-authority/act-cxii-of-2011-privacy-act).

[20] Data Protection Act 2018,

[21] https://uk-gdpr.org/

states that the task of Yad Vashem is to "gather in to the homeland material regarding all those members of the Jewish people who laid down their lives, who fought and rebelled against the Nazi enemy and his collaborators, and to perpetuate their memory and that of the communities, organizations, and institutions which were destroyed because they were Jewish" and thus Yad Vashem shall be competent to "collect, examine and publish all testimony of the disaster and the heroism and to bring home its lesson to the people. "[22]

From the overview of all countries appears that the most common instrument to implement art 89 of the GDPR is a national privacy law with a general reach. In some countries archival law has to be taken into account as well since archival law may lay down more specific rules, procedures or impose retention periods for the access to archival files containing personal data. In a few countries, the national privacy law has only limited provisions for processing of personal data for historical research purposes or archiving in the public interest.

In none of the national privacy laws under research, recital 158 of the GDPR has been implemented.

2.2 Varieties of safeguards for the rights and freedoms of the data subjects

An overview of the safeguards for the rights and freedoms of the data subjects shows a degree of variation across the national legislations under discussion[23]. Some legislations limit themselves to general principles, whereas other laws impose more specific obligations, measures or procedures to be taken into account. Below, for the countries under study, the situation concerning the safeguards to implement art 89 GDPR will be described in more detail.

2.2.1 Legislations limited to general principles or with limited specific provisions

The Netherlands

In the Netherlands both safeguards and derogations are put in place in the national law when personal data are processed for purposes of archiving in the public interest or for historical research purposes.

Article 44 of the Dutch data protection law refers to research, whereas article 45 relates to archiving in the public interest. Article 44 states**: "**Articles 15, 16, and 18 of the GDPR do not apply in case personal data is processed by institutions or services for scientific research or statistics, and the required safeguards are put in place to ensure that the personal data can only be used for such purposes."[24] The required safeguards – or the format of the technical and organisational measures – are not specified in the law, leaving the responsibility basically with the controller (the research institution). Archival communities however have

[22] https://knesset.gov.il/review/data/eng/law/kns2_yadvashem_eng.pdf

[23] Poland and Israel will not be discussed further since it appears that Israel has, strictly speaking, not implemented art 89 of the GDPR and the Polish law gives, apart from the designation of data protection officer no further details on the implementation of art 89.

[24] Informal translation of the GDPR, provided by OneTrust DataGuidance. See: https://www.dataguidance.com/notes/netherlands-data-protection-overview

provided additional informal guidance. The working group GDPR of the Royal Society of Archivists in the Netherlands (KVAN) illustrate how a data controller can comply to articles 24 (responsibility of the controller) and 89 GDPR. The methods that are listed are:

- Anonymisation: by editing personal data in such a way that they cannot be traced back to the actual person (neither directly, nor indirectly).[25]
- Pseudonymisation: by editing personal data in such a way that they cannot be traced back to the actual person (neither directly, nor indirectly), without using additional data. This could be a 'key' that only authorized individuals have access to, which should be stored separately.[26]
- Data minimisation: by storing no more personal data than strictly necessary for the prescribed goal. This is not a safeguard in itself, but can reduce the need for other safeguards still[27].
- Privacy 'by default'**:** by implementing checks and balances into the system, such as authorised access, logging and monitoring;[28]
- Honouring the rights of whom the data concerns: by providing civilians the right to view, rectify and/or delete the data that concern them. Exceptions to this rule may apply, but always involve a careful weighing procedure of the rights of various stakeholders.[29]
- Information security: by implementing processes such as a risk analysis, data classification and auditing.[30]

Article 45 of the Dutch data protection law is not specific on the safeguards that are needed, but gives the data subject the right to access personal data and to add/correct his/her personal data in an archival context. Article 45 reads**: "**Articles 15, 16, 18(1)(a), and 20 of the GDPR do not apply in cases where personal data is processed that is included in archives within the meaning of the Public Records Act. The data subject has the right of access to the archived records, unless the request for access cannot reasonably be granted because the request is not specified sufficiently. A data subject has the right to add its own understanding of the relevant data to the archived records in cases where incorrect personal data is processed."[31] Article 45 is in fact a derogation, that limits the not-applicability of art 15,16, 18 (1)(a) and 20 of the GDPR to those archives as defined in the Dutch archival law, basically the National Archives and the Regional Historical Centres. Other institutions keeping archives as NIOD are excluded. KVAN however has lobbied very recently for a broader scope and did so successfully. In the future, Article 45 will apply to "archival collections of publicly accessible institutions that control collections with lasting value for the public good on a nonprofit basis" which includes archives such as NIOD.[32] This proposal implies a definition of the concept 'archiving in the public interest'.

[25] Working Group GDPR (Werkgroep AVG) of Information and Archive Knowledge Network (Kennisnetwerk Informatie en Archief – KIA), "Weten of vergeten? Handreiking voor het toepassen van de Algemene verordening gegevensbescherming in samenhang met de Archiefwet in de dagelijkse praktijk van het informatiebeheer bij de overheid" (2020) p.33-34. See: https://kia.pleio.nl/attachment/entity/a8e1caa5-0d59-4267-bbc0-4cd288b2a56c

[26] Idem, p.34-35.

[27] Idem, p.36.

[28] Idem, p.36

[29] Idem, p.37.

[30] Idem, p.37.

[31] Idem

[32] "Artikel 45 UAVG wordt gewijzigd op initiatief van KVAN/BRAIN" (10 April 2020) https://www.kvan.nl/nieuws/artikel-45-uavg-wordt-gewijzigd-op-initiatief-van-kvanbrain

Romania

The approach of the Romanian Law no. 190/July 2018 towards data protection regulation is quite general[33]. It includes provisions for processing several categories of special data and a title dedicated to derogations where we can find art 8. regarding the processing of personal data for scientific or historical research, for statistical purposes, or archiving in the public interest. This article also has a general approach, only mentioning the provisions of art. 15, 16. 17, 18, 19, 20, and 21 of the GDPR as not applying if the processing is made for the purposes mentioned above, as the rights referred to therein are of a nature to make it impossible or seriously affect the achievement of specific goals.

Art. 8 also specifies that the derogations are applicable only subject to the existence of adequate safeguards for the rights and freedoms of the data subjects referred to in Article 89 (1) of the GDPR. There are no other detailed provisions regarding general or specific safeguards that need to be enforced. Therefore, the Romanian law sets the general framework of the data protection regulation, without detail regarding how to collect and what technical and organizational measures to ensure the safeguards, but invoking the provisions of the GDPR. Considering this approach, the pseudonymization mentioned in Art 89 (1) of the 679/2016 GDPR would be a safeguard measure recommended by the Romanian law as well. The responsibility of implementing the safeguards asked for in art. 89 of GDPR belongs to the controller, so in practice the researcher.

Czech Republic

The Czech personal data protection law of 12 March 2019 implements art 89 GDPR in article 16 as far as historical research is concerned. Measures to protect the rights and freedoms of the data subject are necessary and must be 'appropriate to the state of the art, costs of implementation, nature, scope, context and purpose of processing, as well as risks to the rights and freedoms of natural persons of varying likelihood and severity'[34]. In contrast to other national legislations the Czech law presents a list of possible measures that can be taken. This list includes: logging of personal data processing activities and keeping these logs for two years; the designation of a data protection officer; pseudonymisation or limitation of access to personal data by the controller[35]. The choice of the most appropriate safeguards has to be made by the controller. For special categories of personal data (as defined in art 9 GDPR), further processing should be done in such a way that the data subject cannot be identified, except when this would make it impossible to attain the research aim[36]. If personal data are processed for historical research purposes, it is possible to postpone or 'apply *mutatis mutandis'* the exercise of the rights of the data subject listed in articles 15, 16, 18 and 21 of the GDPR if this is 'necessary and reasonable' with regard to the scope of the research. Moreover, the right of access (art 15 GDPR) must not be granted if this would ask a disproportionate effort and processing of personal data is necessary for the research objective[37]. Even if it does not appear directly from the wording on the title of the article, article 16 would also apply for archiving in the public interest[38].

[33] Law no. 190/2018 on implementing measures to Regulation (EU) 2016/679, art. 8.

[34] Act No. 110/2019 Coll. Act of 12 March 2019 on personal data processing, Section 16 (1)

[35] Act No. 110/2019 Coll. Act of 12 March 2019, Section 16 (1)

[36] Act No. 110/2019 Coll. Act of 12 March 2019, Section 16 (2)

[37] Act No. 110/2019 Coll. Act of 12 March 2019, Section 16 (3)

[38] https://www.whitecase.com/insight-our-thinking/gdpr-guide-national-implementation-czech-republic#q5 (Consulted on 2 August 2022).

Slovakia

In the Slovak personal data protection act, processing of personal data for archiving in the public interest and historical research is governed by chapter 4 section 78, dealing with specific situations of lawful processing of personal data. The first general principle is that when personal data are processed for archiving in the public interest and historical research, the controller and the processor have the obligation to put in place 'reasonable safeguards' to protect the rights of the data subject[39]. These safeguards should be technical and organizational measures to implement data minimization and pseudonymization[40]. Moreover, section 78 makes it possible to restrict a series of rights of the data subject (right of access, rectification, restriction and right to object to personal data processing) if these rights 'are likely to render impossible or seriously impair the achievement of such purposes.' This restriction has to be made by a special regulation and safeguards have to be foreseen[41]. As for archiving in the public interest, the same rule applies, but the rights of the data subject that can be restricted also concern notification of rectification, erasure or restriction of personal data processing and data portability[42]. The Slovak law on personal data protection also allows to derogate from the principle of storage limitation: personal data can be stored for a longer period of time if they are used exclusively for archiving in the public interest or for historical research purposes, if adequate safeguards as referred to in section 78 are provided[43]. Section 16 of the Slovak law on data protection makes an exception to the principle that special categories of personal data (art. 9 GDPR) may not be processed. With adequate safeguards in place, processing is allowed for archiving in the public interest and for historical research purposes[44]. However, for processing of personal data relating to criminal convictions or offence (art. 10 GDPR) a special regulation with adequate safeguards is necessary[45]. So, for these personal data, the implementation of adequate safeguards is not left to the discretion of the controller, but is imposed by a specific legislation and not by the data protection law. Under Slovak law, if personal data are not obtained directly from the data subject, the controller has the obligation to inform the data subject. This obligation does not apply if personal data are processed for archiving in the public interest or for historical research purposes and if giving information to the data subject would prove impossible or require a disproportioned effort. If the obligation to give information to the data subject would 'render impossible or seriously impair' the objective of the processing of personal data, the controller can derogate on the condition that appropriate safeguards are put in place[46].

United Kingdom

The UK Data Protection Act has in schedule 2 part 6 derogations on art 89 GDPR for research, statistics and archiving. For historical research it is possible to derogate from articles 15 (1-3), 16, 18(1) and 21(1) of the GDPR if the application of these articles would make the achievement of the research purpose impossible or seriously hinder and on the condition that appropriate safeguards are put in place. Research must moreover be in the

[39] Act of 29 November 2017 on personal data protection and amending and supplementing certain Acts, section 78 (8)

[40] Act of 29 November 2017, section 78 (8)

[41] Act of 29 November 2017, section 78 (9)

[42] Act of 29 November 2017, section 78 (10)

[43] Act of 29 November 2017, section 10

[44] Act of 29 November 2017, section 16 (k)

[45] Act of 29 November 2017, section 17.

[46] Act of 29 November 2017, section 21 (5 b)

public interest. As for art 15 (1-3) of the GDPR (right of access), the derogation is only possible if the results of the research are not made available in a way that makes identification of the data subject possible[47]. For archiving in the public interest, derogation from articles 15 (1-3), 16, 18 (1), 19, 20 (1), 21 (1) of the GDPR is possible if the exercise of the rights of the data subjects defined in these articles would seriously hinder the objective of archiving in the public interest or make it impossible. Adequate safeguards as defined in article 89 GDPR are necessary[48]. Section 19 of the UK Data Protection Act details the procedure to be followed. The first step is to prove why it is not possible to use anonymized data, then as a general rule, pseudonymization should be used. Only if that is not possible to achieve the research or archiving objective, personal data can be used on the condition that processing does not harm data subjects. For processing safeguards and security measures have to be foreseen[49].

Hungary

The Hungarian privacy act does not give much detail on the implementation of art 89 GDPR. In general, controllers and processors must take, where appropriate, technical and organizational measures, more in particular pseudonymisation, to protect the rights of the data subjects[50]. Section 5 that determines the legal basis and general conditions for processing states that if sensitive data are processed, appropriate technical and organizational measures have to be implemented in order to make sure that only people for whom it is absolutely necessary that they process personal data are in a position to access these sensitive data. Individuals or institutions who do research are allowed to disclose personal data, if necessary to present the results of 'scientific research on historical events'[51].

Lithuania

As already indicated in the general overview of the relevant legislations, the Lithuanian national data protection law has no provisions tailored to historical research and archiving in the public interest. In Lithuania an alternative technique is used. The State Data Protection Inspectorate has issued a list of data processing operations subject to the requirement to perform a data protection assessment[52]. These operations include historical research for which special categories of personal data are processed without the consent of the data subject or if personal data processing is based on matching or combining databases.

[47] Data Protection Act 2018, Schedule 2, Part 6, 27.

[48] Data Protection Act 2018, Schedule 2, Part 6, 28.

[49]Information Commissioner's Office, *Guide to the General Data Protection Regulation* (https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-are-the-conditions-for-processing/#conditions10)

[50] Act CXII of 2011, on the right to informational self-determination and on the freedom of information, section 25/A.

[51] Act CXII of 2011, section 5.

[52] ' State Data Protection Inspectorate: List of data processing operations subject to the requirement to perform data protection impact assessment' 19 03 2019, https://vdai.lrv.lt/en/news/list-of-data-processing-operations-subject-to-the-requirement-to-perform-data-protection-impact-assessment (consulted 6 July 2022).

2.2.2 Legislations with more elaborate safeguards

Germany

In **Germany**, art 89 GDPR is implemented by § 27 and 28 of the federal data protection act (*Bundesdatenschutzgesetz* - BDSG). § 27 refers to historical research and 28 to archiving in the public interest.

§ 27 makes a careful balance between the rights of the data subject and the needs of research. Consent of the data subject remains the norm : however if obtaining this consent is necessary for the research objective and the interest of the controller (the researcher) to process the personal data 'significantly outweighs' the rights of the data subject, consent is not necessary. Moreover, the controller has to put in place appropriate and *specific* measures to protect the interests of the data subject. These measures should be in line with § 22 (2) second sentence of the BDSG and as a consequence 'Take into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing'. Art 22 (2) sums up different possibilities as appointing a data protection officer or restriction on access, but it is up to the controller to evaluate which measures are sufficient as a safeguard. § 27 makes it possible to limit some of the rights of the data subject, but only to the extent that these rights 'are likely to make impossible or seriously impair the achievement of the research or statistical purposes and the limitation is necessary for the fulfilment of the research or statistical purposes.' As for the right of access of the data subject (art 15 GDPR), this limitation is only allowed if provision of access would need a 'disproportionate effort'.

Next to this general principle of balancing of interest to define which safeguards are appropriate, section three of § 27 puts forward anonymization as a safeguard. Personal data used for research purposes should be anonymized from the moment that anonymization is possible, considering the purpose of the research. A more specific safeguard is put into place for publication of personal data. In the hypothesis of publication, the rights of the data subject slightly outweigh the interest of the research. The principle is that for publication, the consent of the data subject is needed. There is an exception : publication is allowed without the consent of the data-subject if publication is 'indispensable' to present the results 'on events in contemporary history'[53]. Here again, the balancing of interests is to be made by the researcher. The provision on publication of personal data takes into account the needs of historical research since reference is made to 'events in contemporary *history'.*

The exception for archiving in the public interest is detailed in § 28 of the federal data protection act. The principles are quite similar to § 27 : processing of personal data is allowed if appropriate and specific measures in line with § 22 are put in place. The right of access (art 15 GDPR) is limited to archive records indexed by name or if there is no information available allowing the record with the personal data to be found 'with reasonable administrative effort'. As in the Netherlands, the German law also opens, under certain circumstances, the possibility for data-subjects to exercise their right of rectification (art. 16 GDPR), by adding a counterstatement to the personal dataset[54].

In the German legal context, next to the federal data protection act archival laws need to be considered as well. The GDPR explicitly applies only to the data of living persons (recitals 27 and 158). The GDPR therefore applies to archival materials that contain data of living

[53] Bundesdatenschutzgesetz vom 30. Juni 2017, § 27 and § 22 (Consulted on 8 August 2022).

[54] Bundesdatenschutzgesetz vom 30. Juni 2017, § 28 and 22.

persons. The GDPR also provides that member states may adopt further rules on the processing of personal data of deceased persons. Such regulations already existed in Germany before the entry into force of the GDPR in the form of the federal and state archive laws and they continue to exist in addition to the GDPR. In this context, the protection of personal records is based on the general and post-mortem right of privacy as a fundamental constitutional right (Article 1 (1) GG; Article 2 (1) GG)[55]. According to the German legal understanding, the legal protection of privacy does not end with death, but continues beyond it. The duration of the protection of privacy is not precisely defined, but "fades" in the course of time. The archival laws take this into account through special protection periods for personal archival records.

Almost all archive laws at the level of the *Länder* provide for a protection period of 10 years after the death of the person concerned. Only the archive law of Saxony-Anhalt, which was last updated in 2020, provides for an even stricter period of 30 years after death. If the date of death is not known, the archive laws provide for a period of 90, 100 or 110 years after birth. If neither information on the date of death nor the date of birth is available, most archive laws provide for a retention period of 60 years after the creation of the records. An exception is the Berlin archival law, which specifies 70 years. The archive laws of Baden-Württemberg, Bavaria and Lower Saxony do not specify any further regulations for this case.

In the case of archive records that are subject to federal or state secrecy regulations, there are even longer periods of protection. These are usually archival records that are subject to tax secrecy, social secrecy, banking secrecy or similar. The Federal Archives Act provides for a protection period of 60 years after creation. Some of the state archive laws provide for different protection periods, although these always refer only to secrecy regulations under state law: 30 years after creation in Berlin, Brandenburg and Schleswig-Holstein; 50 years after creation in Lower Saxony. Thuringia provides for a protection period of 30 years after the death or 130 years after the birth of the person concerned or 90 years after the closure of the records for personal archive records that are subject to secrecy regulations of the state.

The archives can shorten protection periods upon request, i.e. submit documents for use despite an existing protection period. Such a shortening of the retention period is always an exceptional permission in the individual case, which cannot be transferred arbitrarily to other purposes of use. The archive must examine the application for a shortening of the retention period and, in each case, weigh the personal rights and legitimate interests of the person(s) concerned against the legitimate interests of the applicant user(s). However, the archive laws provide several criteria for shortening the protection period. A reduction of the protection period is always possible if the person(s) concerned consent to the use. Some archive laws also explicitly regulate the shortening of the retention period on the basis of the consent of relatives or legal successors. In many cases, and due to the historical circumstances of the Holocaust, it will hardly be possible to obtain such consent.

The archive laws therefore provide for the possibility of shortening the protection period for scientific research. In this case, it must always be examined on a case-by-case basis whether the use of the blocked archival records is necessary and indispensable for the achievement of the research purpose. A reduction of the protection period can also be granted if the public interest in achieving the scientific research objective considerably outweighs the interests of the persons concerned that are worthy of protection.

Some of the more recent archival laws also explicitly permit reductions in the retention period if the use serves to protect the legitimate interests of the persons concerned - these include, for example, rehabilitation, restitution, and clarification of the fates of missing or dead

[55] Grundgesetz für die Bundesrepublik Deutschland art 1 and 2. http://www.gesetze-im-internet.de/englisch_gg/ (Consulted on 8 August 2022).

persons, especially from the Nazi era, the period of Soviet occupation, and the German Democratic Republic. These arrangements are consistent with Recital 158 of the GDPR, which provides that member states should be allowed "to further process personal data for archival purposes, for example, with a view to providing specific information related to political behavior under former totalitarian regimes, genocide, crimes against humanity, in particular the Holocaust, and war crimes." So, it can be said that in Germany, recital 158 is not implemented in personal data protection law, but implicitly in some archival laws.

For all reductions in the term of protection, the hurdle for permission to merely inspect records is usually lower than for permission to publish data, a principle which is consistent with § 27 of the German Federal Data Protection Act . The archive can attach conditions to the use of the records in order to ensure that the interests of the person(s) concerned worthy of protection are safeguarded. Such conditions are usually anonymization or pseudonymization. Such conditions represent technical and organizational measures to safeguard the rights of the data subjects within the meaning of Art. 89 GDPR.

Austria[56]

The Austrian Data Protection Act has special provisions for processing of personal data for historical research and archiving in the public interest, but these provisions can only be applied on the condition that specific statutory regulations exist.

The Austrian legislator has distinguished two different constellations for the processing of personal data for historical research or for archiving in the public interest. If processing in this context does not have results on identifiable persons as its objective, the controller is allowed to use any data that is publicly available or the controller uses only pseudonymized data on the condition that the controller is not in a position to retrieve the identity of the data subject. A general condition is that it should not be possible to use the processed personal data to draw conclusions concerning specific natural or even legal persons, e.g. by combining datasets.

If processing of personal data for historical research or for archiving in the public interest generates results on identifiable persons, personal data may only be processed with the consent of the person concerned, if there is a special legal regulation or with the approval of the data protection authority. The authorization to the data protection authority is to be asked by the person responsible for the research. Three criteria are mentioned to grant authorization: it is impossible to obtain consent from the data subject since the data subject is inaccessible or obtaining authorization would require a disproportionate effort; the processing must serve the public interest; and finally the professional qualification of the person who asks for the authorization must be demonstrated. It appears that the public interest of research is not only connected to the funding source (a public institution) but in general that research connected to the National Socialist era serves the public interest.

If research implies processing of special categories of personal data, provisions have to be taken to make sure that the data can only be used by persons for which a legal duty of confidentiality applies or who are otherwise reliable in this regard. The data protection authority has the possibility to make the approval dependent on the fulfillment of conditions and requirements, to the extent that this is necessary to protect the interests of the data subjects, in particular if special categories of personal data are processed.

[56] https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-datenverarbeitung-wisschenschaft-statistik.html

Pseudonymization is used as a safeguard as well. As a general rule, during processing personal data have to be pseudonymized if this method is sufficient for the research purpose. Personal data should be eliminated when these data are no longer necessary for the research purpose. Regarding access to personal data kept in archives, provisions in archival law apply and the data protection authority is not in a position to give an authorization.

Greece

In Greece, art 89 of the GDPR is implemented in article 29 (archiving in the public interest), article 30 (historical research) and article 48 of Law n° 4624. Article 48 states the general principle that processing of personal data is allowed for archiving in the public interest and for historical research on the condition that this processing is in the public interest and that safeguards are taken, mentioning anonymization, as soon as possible, and preventing unauthorized access to personal data using spatial and organizational means[57].The rules for archiving in the public interest and for historical research are fairly similar. As for archiving in the public interest, article 29 makes it possible to derogate from article 9 (1) of the GDPR and process special categories of personal data for archiving in the public interest on the condition that 'suitable and specific measures' are taken to protect the 'legitimate interests' of the data subject. Article 29 lists these possible measures : restriction of access rights, pseudonymization and even encryption of personal data or appointing a data protection officer. Article 29 allows to derogate from articles 15, 16, 18 (1, a, b and d), 20 and 21 GDPR if exercising of the rights of the data subject defined in these articles renders impossible or seriously impairs the objectives of archiving in the public interest[58]. The possible measures to be taken by a controller who is using special categories of personal data for historical research purposes listed in article 30 are the same as in article 29. However, article 30 imposes some additional obligations. Special categories of personal data must be anonymized as soon as possible taking into account the achievement of the research objective. Until then, 'characteristics that can be used to match individual details associated with personal or real situations of an identified or identifiable person' have to be kept separately and these characteristics can only be used in combination with individual details if this is necessary for the research objective. As far as publication is concerned, personal data which have been used for the research purpose can only be published with the written consent of the data subject or if publication is necessary for the presentation of the research results and on the condition that personal data have been pseudonymized. For historical research purposes, derogation is possible, on the same conditions as for archiving in the public interest, of art 15, 16, 18 and 21 of the GDPR.[59].

Belgium

In Belgium, the safeguards to be implemented according to art 89 of the GDPR to derogate from the general rules of the GDPR when personal data are processed for (historical) research and archiving in the public interest are implemented in title 4 (art 186-208) of the

[57] Law nr 4624. Hellenic Data Protection Authority (HDPA), measures for implementing Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, art 48.

[58] Law nr 4624. Hellenic Data Protection Authority (HDPA), measures for implementing Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, art 29.

[59] Law nr 4624. Hellenic Data Protection Authority (HDPA), measures for implementing Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, art. 30.

law of 30 July 2018 on the protection of natural persons pertaining to processing of personal data (hereafter the Belgian personal data protection law - BPDPL)[60].

Archiving in the public interest and (historical) research are basically covered by the same rules. However, as far as research is concerned, a distinction is to be made between personal data collected directly with the data subject on the one hand and personal data collected via further processing, e.g. personal data from an archive which are used for research purposes, on the other hand. If personal data are collected via further processing, normally an agreement has to be concluded with the controller of the initial processing, but this rule does not apply if according to European or national law the controller has a mandate to process personal data for archiving in the public interest or for (historical) research purposes. This means that an agreement is not necessary when personal data from an archive are processed. Another exception is when the personal data are processed which have already been made public (art. 194 BPDPL). We will focus on further processing, the most relevant case for EHRI.

The Belgian legislation provides for general and specific safeguards.

1. General safeguards[61]

According to article 190 BPDPL, the controller must appoint a data protection officer if the processing of personal data might imply a high risk as defined in article 35 of the GDPR. According to article 191 BPDPL, prior to the processing of personal data, the controller has to fill out the data processing register with specific information on the processing as an explanation and justification of the use of personal data or pseudonymized data and in addition, if special categories of personal data (art 9.1 GDPR) are processed, the personal data impact assessment (art. 35 GDPR).

2. Specific safeguards[62]

The BPDPL makes in article 188 a distinction between three types of processing of personal data : collection, communication, dissemination. Communication of personal data means communication to an identified third party (e.g. a researcher with a reader card in a reading room), while dissemination means communication to a non-identified third party; so basically publication.

a) For collection, the ‘cascade’- principle should be mentioned. One of the main safeguards in the BPDPL is anonymization / pseudonymization. In article 197 a procedure is defined which can be labelled as a ‘cascade-principle’. If the research objective in the phase of collection of personal data can be obtained by anonymization, the controller has to use anonymization for the processing of personal data; if not, pseudonymization is to be used for the processing of personal data. Only if the research aim cannot be reached with pseudonymized data, original data can be used. The BPDPL moreover details the procedures to be followed for anonymization and pseudonymization (art 198-204) and the role of the data protection officer in this respect.
b) According to article 205 of the BPDPL, dissemination of non-pseudonymized personal data is not allowed, unless the data-subject has given his/her consent, the personal

[60] ‘Loi relative à la protection des personnes physiques à l’égard des traitements de données à caractère personnel, art 186-208.

[61] ‘Loi relative à la protection des personnes physiques à l’égard des traitements de données à caractère personnel, art 190, 191, 35,

[62] ‘Loi relative à la protection des personnes physiques à l’égard des traitements de données à caractère personnel, art 188, 194, 197-205

data have been made public by the data-subject itself, the personal data have a close relation to the public or historical character of the data-subject or to the public or historical character of the facts in which the data-subject has been involved. However, special categories of personal data (art. 9.1) cannot be disseminated in a pseudonymized form. The regime for communication laid down in article 207 is slightly different, to the extent that special categories of personal data (art. 9.1 GDPR) and data pertaining to penal procedure (art. 10 GDPR) can only be reproduced by handwriting by the identified third party (eg an researcher in a reading room of an archive).

If a code of conduct, validated by the data protection authority exists, the articles pertaining to the collection of personal data do not apply. The same goes for communication according to article 207 (art . 187 and 208 BPDPL)[63].

In general, the Belgian legislator places the responsibility for the implementation of the safeguards asked for in art 89 GDPR, primarily with the controller, who has to meet some specific requirements as keeping a data processing register and in some cases the appointment of a data protection officer or making a data impact assessment. Anonymization and pseudonymization can be considered as the main safeguards in the Belgian law, which makes a distinction between collection, communication and dissemination for which different safeguards have been put in place. A validated code of conduct is also considered as an adequate safeguard, which moreover exempts from certain legal obligations.

France

The French *Loi Informatique et libertés* sets in articles 78 and 79 general principles for the implementation of article 89 of the GDPR. According to the first paragraph of article 78, articles 15, 16 and 18 to 21 of the GDPR do not apply when personal data are processed for archiving in the public interest by a public archiving service and if exercising of these rights makes it impossible or seriously hinders the objective of archiving in the public interest. Moreover, safeguards have to be put in place. These safeguards are not laid down in the *Loi Informatique et libertés* but in the code on patrimony and other laws and regulations pertaining to public archives and by respecting the norms on electronic archiving. So basically, the guarantees are implemented by archival law. The safeguards which are a condition to derogate fully or partly from articles 15, 16, 18 and 21 of the GDPR for archiving in the public interest and for historical research purposes are not determined by the *Loi Informatique et libertés*, but by a Decree based on a reasoned opinion of the Data Protection Authority[64]. In France the Data Protection Authority has a say in the way that personal data can be processed for historical research purposes on the level of general principles.

The Decree defining the safeguards is Decree 2019-536 of 29 May 2019. As the *Loi Informatique et libertés*, this decree is not specific for historical research purposes or archiving in the public interest, but has a general reach. Article 116 of the Decree implements art 78 of the *Loi Informatique et libertés* and elaborates in more detail on what are considered as adequate safeguards. Article 116 is a derogation to the general rules of the GDPR, but interprets these derogations in a limitative way: the derogation can only be used if

[63] 'Loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, art. 187, 208.

[64] *Loi Informatique et libertés,* art 78.(Consulted on 8 August 2022).

respecting the general rules would make it impossible or would seriously hinder the objective of archiving in the public interest or historical research.

Article 116 defines two safeguards in two stages of processing: the conservation of the results of the processing of personal data and the dissemination (*diffusion*) of the data. As for the conservation, the controller must make sure that the data can only be accessed or modified by an authorized person and as a consequence access must be limited. These authorized persons moreover must respect the rules of deontology which apply in their sector of activity[65]. The underlying principle of this safeguard can be compared with the code of conduct, which is referred to in article 40 of the GDPR and which is seen as means to contribute to the correct implementation of the GDPR taking into account the specificity of different sectors[66]. Moreover, the persons authorized to access the results of the processing of personal data must respect the objective for which the personal data have initially been collected and must comply with the safeguards defined in art 116. Implicitly, the paragraph of art 116 on the conservation of the results of the processing of personal data allows that these results are kept and do not have to be destroyed.

Paragraph 3 of article 116 limits the dissemination of the results of processed personal data. The principle is that these data have to be anonymized before dissemination. There are two exceptions : dissemination is allowed if the interest of a third party prevails over the interests or the rights and freedoms of the data subject. For research purposes, the dissemination is allowed but only if this is 'absolutely necessary' for the presentation of the research results. In that case the decision is to be taken by the researcher. Moreover, the researcher should make sure that the data disseminated are 'adequate, pertinent and limited to what is necessary for the purposes for which the data have been processed'[67]. For documents from public archives containing personal data, for which access is only possible after a certain period of time, an authorization to disseminate the personal data is needed from the archival administration with the agreement of the authority which has produced the archives. This goes for instance for court files or files of the civil registry: in that case, access is as a general rule only possible 75 years after the most recent document in the file or alternatively, 25 years after the death of the person concerned if that date is shorter[68].

Article 79 of the *Loi Informatique et libertés* provides for an exception to the obligation of art 14 GDPR to inform the data subject when data are processed which are not collected directly with the data subject, for instance from an archive. In that case, there is no obligation to inform the data subject when the data are processed for archiving in the public interest or for historical research purposes[69].

Italy

Title VII of the Italian personal data protection code implements art 89 of the GDPR. Chapter II deals more specifically with archiving in the public interest and historical research. Section 101 sets the general principle, which can be considered as limitation of processing of

[65] Décret no 2019-536 du 29 mai 2019 pris pour l'application de la loi no 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Art 116. (Consulted on 8 August 2022).

[66] 'Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016, art 40.

[67] Décret no 2019-536 du 29 mai 2019, art 116 (3)

[68] *Ibidem,* art 116 (3) Code du patrimoine art L. 213-3 www.legifrance.gouv.fr/download/file/pdf/LEGITEXT000006074236.pdf/LEGI (Consulted on 8 August 2022).

[69] *Loi Informatique et libertés,* art 79

personal data or more precisely, documents containing personal data. This processing is only allowed in the context of archiving in the public interest or for historical research, if this processing is 'relevant and indispensable' for these purposes. Dissemination of such data is only allowed for achieving the purposes of archiving in the public interest or historical research. There is an exception to this principle of limitation of dissemination however: dissemination is allowed if the personal data relate to 'circumstances or events' which have been made public by the data subject itself or 'on account of the latter's public conduct'[70].

Next to this general principle, more specific provisions are foreseen for archiving in the public interest and for historical research. As for archiving in the public interest, the safeguard focusses on access policy. Access policy is regulated by decree, n° 42 of 22 January 2004, which is the Code of Cultural and Landscape Heritage and covers next to State archives, also historical archives of public bodies and private archives declared to be of especially substantial historical interest.

More in general, the personal data protection code refers to codes of conduct as a safeguard for historical research as well as for archiving in the public interest. Section 102 tasks the data protection authority with encouraging the adoption of codes of conduct for historical research and archiving in the public interest by public and private entities, as scientific societies or professional associations and to some extent delegates the elaboration of appropriate safeguards to the professionals in the field. Section 102 describes the general principles these safeguards should comply with. First, the rules in the code of conduct should be fair and not discriminate between users. Second, these rules should also cover communication and dissemination of personal data, for which reference is made next to the GDPR, to the personal data protection code and to the rules pertaining to journalistic expression[71].

This implies that according to art 89, as a general rule, data minimisation should be implemented. Processing of personal data for journalistic purposes and other intellectual work is covered by sections 136 - 139 of the personal data protection code. Section 136 implements art 85 of the GDPR, which deals with the specific situation of processing of personal data and freedom of expression and information. Section 136 c assimilates processing of personal data ' that are aimed exclusively at publishing or circulating, also occasionally, articles, essays and other intellectual works also in terms of academic, artistic or literary expression' with processing of personal data for journalistic expression. So, it can be assumed that section 136 c applies when results of historical research are published. Section 137 defines the principles to be complied with if section 136 is invoked. Special categories of personal data as defined in article 9 GDPR and personal data relating to criminal convictions and offences as defined in article10 GDPR may be processed without the data subject's consent on the condition that a code of conduct is adopted by the National Council of the Press Association and is complied with. If the code of conduct is not respected, the data protection authority can prohibit processing. Moreover, the data protection authority will define in cooperation with National Council of the Press Association, the 'measures and arrangements' to protect the data subjects, measures and arrangements to be implemented by the National Council of the Press Association[72]. Section 139 is slightly

[70] Personal data protection code. Containing provisions to adapt the national legislation to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, section 101. (Consulted on 8 August 2022).

[71] Personal data protection code. Containing provisions to adapt the national legislation to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, section 102.

[72] Personal data protection code. Containing provisions to adapt the national legislation to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, section 139

ambiguous to the extent that the heading of this section only refers to journalistic activities and to a code of conduct drafted by the National Council of the Press Association, whereas section 136 assimilates academic publications with journalistic purposes and mentions in its heading both journalistic purposes and other intellectual work. The most logic interpretation seems that for publication of research findings the code of conduct for journalism should serve as a guideline or good practice, even if it can be assumed that, generally speaking, academics are not affiliated to a Press Association.

According to section 102 2 b, specific provisions have to be put in place for disclosing data on health, sexual life and family related measures. For these categories of personal data, it must be specified in a code of conduct in which cases the data subject or an interested party has to be informed before dissemination of the data. Codes of conduct should also have arrangements of processing of personal data for archiving in the public interest or for historical research based on private archives. These arrangements should not only cover access, but also the safeguards when personal data are communicated or disseminated[73].

So for archives not covered by decree n° 42 of 22 January 2004, a code of conduct should provide for an equivalent level of personal data protection as laid down in decree n° 42. Chapter III of this decree regulates consultation of archival documents and confidentiality. Consultation of public archives (defined as: 'the archives of the State and in the historical archives of the Regions, of other territorial government bodies as well as those of any other public body and institution') is in principle free, with some exceptions, however. One of the exceptions are documents containing 'sensitive information' and 'information relative to measures of a penal nature expressly indicated in the laws on the use of personal data'. These documents can be consulted only 40 years after their date or 70 years when the document contains information pertaining to the health situation, 'sexual experience' or 'private family relations'[74]. It is possible to consult these documents before the expiry date, for historical research purposes but only after the authorization of the Ministry of the Interior, after consultation of the director competent for the State Archives (or the archival superintendent for regional archives) and the Commission on questions pertaining to the consultation of confidential archival documents. Even if an authorization for consultation is granted, the documents may not be disseminated and remain confidential[75].As for current archives of bodies of the State, regions or other territorial entities, these bodies are tasked with establishing regulations for consultation of their current and deposited archives[76].

Decree n° 42 contains an article 126 on the protection of personal data with provisions granting additional and specific rights to a data subject. According to paragraph 1, when a data subject has exercised his/her rights pertaining to the use of the personal data the archives can be consulted in combination with the documentation referring to the exercise of the rights of the data subject[77]. Paragraph 2 gives the data subject the possibility to request for a 'freeze' of those personal data which are not 'of great interest to the public', if the use of these data would lead to a 'concrete danger' to harm the 'dignity, privacy or personal dignity' of the individual to which the personal data refer[78]. The provisions of paragraphs 1 and 2 can be considered as personal guarantees for a data subject. The third paragraph provides for a safeguard with a general reach ; when archival documents with personal data are used for

[73] Personal data protection code. Containing provisions to adapt the national legislation to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, section 102

[74] Legislative Decree no. 42 of 22 January 2004 Code of the Cultural and Landscape Heritage. Article 123. (Consulted on 8 August 2022)

[75] Legislative Decree n° 42 Article 123.

[76] Legislative Decree n° 42 Article 124.

[77] Legislative Decree n° 42 Article 126.

[78] Legislative Decree n° 42 Article 126.

historical research purposes, the regulations of codes or conduct established under the 'laws on the use or personal data' are to be complied with[79]. So even if a specific regime of personal data protection is in force for archiving in the public interest, codes of conduct, which have a central position in the Italian personal data protection law, still have to be complied with. As for private archives, article 127 of Legislative decree n° 42 provides for similar rules as for public archives for personal data protection[80].

A code of conduct for archiving in the public interest and historical research was issued by the Italian data protection authority on 19th of December 2018[81]. Basically, this code confirms the principles laid down in the personal data protection code and Decree n° 42 sets or details these principles for processing personal data for archiving in the public interest and for historical research. The code for instance details the conditions and the procedure to be followed by a researcher to have access to archival documents containing personal data before the term of 40 or 70 years. The code of conduct applies for archivists as well as for researchers, but makes clear that the way that personal data are used by a researcher is his/her own responsibility. The code of conduct also deals with specific types of sources as oral testimonies, where the code of conduct imposes that the interviewee has given his/her (oral) consent and that when oral testimonies are kept in an archive, the interviewer should add a written document to the testimony with the aim of the interview and the consent of the interviewees[82].

2.3 Concluding remarks

This overview makes clear that there is much variety in the way that art 89 of the GDPR is implemented in national law. There is much variety in the level of detail of the safeguards to be taken into account by a researcher. Some national laws remain rather general and do not add much detail to the principles set out in art 89 of the GDPR. This is the case in Hungary, Poland, Lithuania, Romania, Slovakia, the Czech Republic, the Netherlands and the UK. In these cases it is often just referred to the principle of data minimization by applying pseudonymization or anonymization without further detail. In other cases, however, such as in the Czech Republic, suggestions for technical/organizational means to protect personal data are given. In the other countries under research safeguards are developed in more detail, meaning that a researcher has to comply with more rules and obligations. Again, the safeguards to be taken into account differ. Techniques used are the appointment of data protection officer, a data impact assessment, codes of conduct, retention periods for access to documents to access personal data and specific procedures to derogate. Less common are codes of conduct and the authorization of the data protection authority.

In many legislations with more specific provisions, a distinction is made between collection of personal data on the one hand and dissemination of research results on the other hand. Generally speaking, there are more restrictions for dissemination, which is logical since the risk for the data subject are higher when research results are published.

[79] Ibidem.

[80] Legislative Decree n° 42 Article 127.

[81] Regole deontologiche per il trattamento a fini di archiviazione nel pubblico interesse o per scopi di ricerca storica pubblicate ai sensi dell'art. 20, comma 4, del d.lgs. 10
agosto 2018, n. 101 - 19 dicembre 2018 [9069661]'
https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9069661 (Consulted on 25 July 2022).

[82] Regolo deontologiche per il trattamento a fini di archiviazione, art. 8 and 9.

Processing of personal data for research purposes is a balancing act, where the needs of the research have to outweigh the rights of the data subject. As a general rule, the rights of the data subject can only be limited if this appears to render impossible, seriously impair or demand a disproportionate effort to attain the research objective. One of the innovations of the GDPR as compared to the Directive 95/46/EC is that archiving in the public interest and historical research is explicitly mentioned as a legal ground for processing personal data, while the Directive 95/46/EC only referred to research in general. In some countries the national legislator has taken into account the specificity of historical research by setting rules that are better tailored to the specificity of historical research as compared to research in general, which was in the past often implicitly seen as research in the social sciences and regulated accordingly. In some countries such as in Italy or in Belgium, specific provisions enable to mention personal data in publications if these are closely related to historical events in which the data subject was involved. This approach makes it easier for a researcher to strike the balance between the needs of the research and the interests of the data subject. This balance is mostly to be made by the researcher and it is ultimately the researcher who is responsible. To the extent that the legislation sets more concrete principles and rules, this balancing exercise is easier for the researcher and tends to give more legal certainty. However, specific rules might also tend to limit the possibilities of a researcher to process personal data in a way that best meets the needs of the research. In most legislations, research as a concept is not defined, but in some legislations the condition to derogate from the general rules for personal data protection is that research should serve the public interest.

From the perspective of international Holocaust research, the GDPR has not led to uniformity, meaning that researchers still have to comply with different rules and procedures in different countries. Moreover, the archival work has to comply not only with the GDPR and privacy laws, but in some countries also with specific archival law, which has a different logic in each country and therefore it will be harder to promote uniformity amongst European countries. On the other hand, it can be said that in certain cases the needs of historical research in general are taken into consideration in national rules implementing the GDPR, which can be explained by the fact that the GDPR explicitly mentions historical research and archiving in the public interest as a legal ground to derogate from general principles of the GDPR.

Please see also the annex to this document that provides a *Comparative table of national legislation implementing article 89 GDPR.*

3 Personal data protection in collection holding institutions

In order to understand the practical implications of the GDPR and the implementing national laws for historical research and archiving in the public interest for the access to Holocaust-related archives, WP 3 organized a survey directed at the collection holding institutions in the EHRI-3 consortium.

The survey asked for an assessment of the implementing laws in each country, for the procedures put in place by the collection holding institutions to comply with the GDPR and implementing national legislation and for current debates on the impact of the GDPR on Holocaust research and access to archives. Eight institutions based in five different countries answered the survey.

The survey shows that different procedures are put in place to comply with the GDPR and national data protection legislation, but collection holding institutions stress that personal data protection measures were already in place before the GDPR and implementing national legislation. Institutions often require a person who wants access to archives containing personal data to fill in research declaration/research sheets. This research declaration explains the purpose of the research and sometimes the methodology used in order to enable the archivist to assess the request to access the archives containing personal data. Research declarations/sheets often briefly explain the rules for personal data protection and clearly state that it is the responsibility of the researcher to comply with personal data protection rules laid down in the GDPR, national law or archival law. Moreover, specific restrictions on the use of the personal data collected can be imposed.

Some collection holding institutions have a more gradual approach, depending on the type of personal data the researcher wants to use and the research design. In that configuration, for personal data in general a research declaration would be sufficient whereas for accessing special categories of personal data an authorization is needed, explaining in detail the research design, the reasons why asking the authorization of the data subject is impossible or would require a disproportionate effort and the guarantees that will be implemented to protect the rights and freedoms of the data subject. Moreover, the researcher has to guarantee that they will not divulgate information that would infringe on privacy rights or harm persons or third parties.

Next to research declarations, some institutions are under the obligation to appoint a data protection officer and to adopt procedures for collecting and processing personal data. Sometimes, the data protection officer also answers individual questions regarding personal data protection. For large scale projects, some institutions refer to the national data protection authority.

From the survey with the collection holding institutions, it appears that research is in general not interpreted in a restrictive way and thus not necessarily limited to research in an institutional context. There are cases where the data subject has explicitly decided that his/her personal data in a personal archive cannot be processed, in that hypothesis, the authorization to use the data for research purposes is not given. Some institutions have a pro-active approach in the sense that they use, e.g. for special groups as children during the Holocaust period, techniques of pseudonymization to create datasets for research purposes.

Codes of conduct, which are in the GDPR considered as an instruments for compliance appear to be more the exception than the rule. Sometimes, collection holding institutions have developed codes of conduct themselves which are considered as a means to enforce the GDPR.

4 Conclusion

A comparison between the different national laws shows that there is a variety in the safeguards that legislators have chosen to implement article 89 of the GDPR. From that perspective the expectation that one might have that a regulation would lead to more uniformity as compared to a Directive has not quite been met. This is probably also not too big a surprise since legal systems, traditions and cultures differ and privacy law is part of the legal system as a whole. Moreover, if mechanisms for personal data protection which were in place before the GDPR was introduced were considered to be adequate over time and to the extent that they do not conflict with the GDPR, a legislator might prefer to continue these mechanisms rather than to introduce a new scheme and familiarize those who are bound by it.

The data and privacy policy elaborated by EHRI since its beginning in 2010 needs no fundamental change, since as it already follows the Dutch national law (EHRI's controller – NIOD-KNAW- is based in the Netherlands) which has, as the national legislator and according to art 89 of the GDPR, implemented the necessary safeguards needed for historical research. The overview of the legislation does not indicate that there are differences in the national legislation implementing the GDPR which would prohibit the transfer of collection descriptions to the EHRI-portal. The data and privacy-policy of EHRI was based in the past on a risk assessment, which is in line with one of the general principles of the GDPR, and we will continue to review the data and privacy policies in accordance with these principles.

The comparison of national laws shows that there are different ways to comply with art 89, some more restrictive than others, but all are acceptable from a legal point of view. With the possible partial exception of Germany (in that case in an indirect way), no single EU-member state has implemented the 'Holocaust-exception' of recital 158 of the GDPR in national privacy law. If this were to be considered in the future, it would be advisable to consider the various solutions worked out by national legislators, opting for a common arrangement that ensures that the rights of data subjects are safeguarded, but in a way that impedes Holocaust research as little as necessary. From that perspective, pseudonymization which is one of the guarantees used in many national laws, should be avoided when it comes to access to Holocaust-related archives. Where possible, EHRI will work with relevant stakeholders such as the International Holocaust Remembrance Alliance (IHRA) to support the promotion of convergence implementing art 89 with the aim to ensure that access to data relevant to Holocaust research is enabled rather than restricted while safeguarding the rights of data subjects.

5 Annex: Comparative table of national legislation implementing article 89 GDPR

	National privacy law with limited specific provisions	National privacy law with more elaborate provisions	Archival law with privacy provisions	Distinction between processing and publication	Code of conduct (implemented or not)	Role for the data protection authority	Appoint a data protection officer	Retention period as a guarantee
Austria		x	x			x		
Belgium		x		x	x		x (in some cases)	
Czech Republic	x						x (in some cases)	
France		x	x	x	x (implicitly – rules of deontology)	x		x
Germany		x	x	x			x (in some cases)	x
Greece		x		x		x	x (in some cases)	
Hungary	x			x				
Israel	x		x	x				
Italy		x	x	x	x	x		x
Lithuania	x					x		
The Nether-lands	x		x					
Poland	x						x	
Romania	x							
Slovakia	x							
United Kingdom	x							

Note: many national privacy laws integrate pseudonimyzation as safeguards for the rights and freedoms of the data subjects. Since pseudonymization is a general principle of art 89 GDPR, it is not included in this table.