EUROPEAN ARCHIVES GROUP

GUIDANCE
ON DATA PROTECTION FOR ARCHIVE SERVICES

EAG guidelines on the implementation of the General Data Protection Regulation in the archive sector

These guidelines are intended to help archive services in Europe apply the General Data Protection Regulation. They are a work in progress, subject to improvement and enrichment, thanks to your experience and comments. These guidelines may also be amended on the basis of future jurisprudence and of opinions and guidelines issued by the European Data Protection Board.

The European Archives Group warmly welcomes your comments. Comments can be sent to the following e-mail address: SG-EAG-GUIDELINES@ec.europa.eu.

LEGAL DISCLAIMER

This document is not intended to provide, and does not constitute or comprise, legal advice on any particular matter and is provided for general information purposes only. You should not act or refrain from acting on the basis of any material contained therein, without seeking appropriate legal or other professional advice.

Title: Guidance on data protection for archive services. EAG guidelines on the implementation of the General Data Protection Regulation in the archive sector
Author: © European Archives Group
Date: October 2018

TABLE OF CONTENTS

ACRONYMS AND ABBREVIATIONS USED IN THESE GUIDELINES

DIRECTIVE 95/46/EC: 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

DPA: Data Protection Authority

DPO: Data Protection Officer

EAG: European Archives Group

EDPB: European Data Protection Board

GDPR: General Data protection Regulation, i.e. the *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)*

I. INTRODUCTION

1. **Audience:** these guidelines are addressed to public and private institutions that hold archives, i.e. records that have been selected for permanent preservation. They are not only addressed to National Archives or to State Archives but also to Regional and Municipal Archives, museums, libraries, foundations and other public and private entities that preserve archives.

2. **Goal:** these guidelines are intended to provide basic information and practical guidance to archivists regarding the specific challenges for the application of the General Data Protection Regulation (GDPR) in the archival sector.

3. **Scope.** Just like any other public and private entity, archive services process personal data regarding their own personnel. These Guidelines do not provide guidance for processing of personal data by an archive service in its role as an employer. Nor do these Guidelines provide guidance for the processing of personal data of users, of donors, of contractors, and so on and so forth. National Data Protection Authorities and national governments, the European Commission, the European Data Protection Board and other actors are already providing guidance on such matters (see the Appendix: *Where to look for further guidance*). These Guidelines focus exclusively on the processing of personal data contained in archival fonds.

4. The **GDPR: the same rules across the EU (but with exemptions for the archives sector).** An EU regulation is a binding legislative act which must be applied in its entirety across the Union. The EU decided to adopt a regulation – instead of another directive – to replace the previous data protection legislation (EU Directive 95/46/EC[1]) in order to have more uniform norms across all Member States. However, the GDPR leaves some room for Member States to introduce exemptions in specific areas. One of them is for "archiving purposes in the public interest"; another one is for historical research. Archivists have to see if their national lawmakers have made use of the opportunity that the GDPR provides to issue such exemptions.

5. **Data minimisation vs permanent preservation**. A key principle of the GDPR is data minimisation. It is actually not new: Directive 95/46/EC was already predicated on this principle. Personal data should be collected and processed only if it is really necessary to do so and should be "kept in a form which permits identification of data subjects" (i.e. the person to whom the data relate) only as long as it is necessary in order to achieve the purpose for which the personal data was collected (art. 5(1) points (b) and (e)). If no exceptions to this principle were allowed, in the future we would no longer have archives containing personal data. But EU lawmakers did introduce some exemptions to this rule. They acknowledged that archives are necessary to enforce fundamental rights. In fact, the GDPR states that "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". However, this is subject to the condition that appropriate measures are

[1] *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*.

taken "in order to safeguard the rights and freedoms of the data subject" (art. 5(1) point (e)).

6. **Processing personal data only when it is really necessary to do so is nothing new for archivists**. One of the key archival functions is the selection of documents for permanent preservation. Only a very small percentage of the documents created or received by the State and other public administrations, or by private entities in the course of their activity, ends up in archival institutions. Archivists select for permanent preservation only documents that are necessary to enforce citizens' rights and for historical research. Archival institutions should publish the general criteria that they apply for the selection of documents for permanent preservation and should be able to explain why they decided to retain specific archival fonds containing personal data.

7. **Storing personal data is not the same as providing access**: In all EU Member States national legislation sets rules regarding access to documents kept in public archives. The closure period for documents containing personal data changes from one country to the next and according to the nature of the personal data. In Italy, personal data that reveal racial or ethnic origin, religious and political opinions, membership of parties, trade unions, are closed for 40 years, while those disclosing health and sex life are closed for 70 years; and records that can reveal the identity of a mother who wanted to give birth anonymously are closed for 100 years. The closure period can be even longer; for example, in Romania, medical records and civil status registers are closed for 100 years after their creation, while documents regarding the private life of an individual are closed for 40 years after the data subject's death. Citizens can trust archive services: they will not disclose their personal data unduly.

8. **The GDPR does not change the closing period of documents containing personal information**. The Regulation includes provisions regarding the right of data subjects to access the data that concern them. It does not include rules regarding access to archives by the general public. The closing periods of documents containing personal data will remain the same.

9. **The GDPR does not modify freedom of information laws**. The Charter of Fundamental Rights of the European Union[2] considers both the protection of personal data and freedom of expression and information (which includes freedom to receive and impart information) as fundamental rights. The GDPR does not modify freedom of information laws. It states that "Personal data in documents held by a public authority or a public body should be able to be publicly disclosed by that authority or body if the disclosure is provided for by Union or Member State law to which the public authority or public body is subject." (recital 154).

10. **The GDPR does not modify freedom of expression laws.** Users of archives include, among others, journalists, academics and other researchers from all walks of life who will, in many cases, publish their findings. The GDPR does not change press laws and other rules concerning freedom of expression. It states that: "Member States shall by law reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary

[2] 2000/C364/01

expression" (art. 85). Member States may provide certain exemptions or derogations to provisions of the GDPR for this purpose (art. 85).

11. **These guidelines are not a code of conduct**. The GDPR encourages "the drawing up of codes of conduct intended to contribute to the proper application" of the Regulation (art. 40.1). It furthermore provides that "Associations and other bodies representing categories of controllers or processors may prepare codes of conduct." (art. 40(2)) and dictates a specific procedure for the approval of codes of conduct by the national Data Protection Authority (if the code has only a national scope) or by the European Data Protection Board and by the EU Commission (if the code will apply in different EU Member States).

    The present Guidelines were drafted by the European Archives Group (EAG), a European Commission expert group composed of representatives from National Archives and Directorates-General of Archives of EU Member States. The Guidelines did not go through the approval procedure provided by art. 40 of the GDPR for codes of conduct. They should be considered a policy document.

II. GENERAL PRINCIPLES

1. GENERAL PRINCIPLES RELATING TO PROCESSING OF PERSONAL DATA (ART. 5)

Archivists should be aware of some general principles regarding the processing of personal data laid out in art. 5 of the GDPR, which states:

> 1. Personal data shall be:
>
> (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
>
> (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');
>
> (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
>
> (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
>
> (e) 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; 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) 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 ('storage limitation');
>
> (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').
>
> 2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

These principles have many practical consequences for archive services and should therefore always be kept in mind. Archivists are familiar with ensuring the principle of 'confidentiality' as it is standard practice in archive services to protect confidential information from unauthorised access. Some of the implications of such principles are nevertheless less obvious. For example:

- the principle of 'transparency' means – among other things – that archive services have to publish clear, user-friendly information on their mission, and in particular why and how they process personal data, and how data subjects can access them.
- the principle of 'integrity' means – among other things – that archival malpractice that leads to the loss of documents containing personal data constitutes not only a

violation of archival professional principles and archival laws, but also a violation of the GDPR.

2. LAWFULNESS OF PROCESSING (ART. 6)

Under the GDPR the processing of personal data is legitimate only if at least one of the specific circumstances listed in art. 6 applies, including: "the data subject has given consent to the processing of his or her personal data"; "processing is necessary for the performance of a contract to which the data subject is party"; the "processing is necessary for compliance with a legal obligation to which the controller is subject", etc. Of special interest to archivists is the condition laid out at (1) point (e)), that processing of personal data is legitimate if it "is necessary for the performance of a task carried out in the public interest".

The GDPR leaves it to EU law or national law to determine which kind of activities are considered as being "in the public interest". National law can include provisions that define the processing of archives by a given institution, or the processing of certain categories of archives to be "a task carried out in the public interest".

3. THE GDPR PROTECTS ONLY PERSONAL DATA OF LIVING PERSONS (BUT NATIONAL LAW CAN PROTECT ALSO THE DATA OF DECEASED PERSONS)

The GDPR protects personal data of living persons. It does not apply to the personal data of deceased persons. However, archivists should consider that national laws may do so. The GDPR in fact stipulates that "Member States may provide for rules regarding the processing of personal data of deceased persons" (recital 27).

How can archivists know whether a data subject is deceased? In most cases they cannot. However, they can reasonably assume that persons born more than one hundred years ago are no longer alive. For example an archivist processing personal files of soldiers who fought in Word War I can assume that they are no longer alive and that the GDPR does not therefore apply to those files. Many other cases will, however, not be so clear cut. Archivists will have to make case-by-case assessments of the possibility that archival fonds under their care contain personal data of living individuals.

III. WHAT IS "ARCHIVING PURPOSES IN THE PUBLIC INTEREST"?

4. DIFFERENT RULES FOR DIFFERENT ARCHIVES ("ARCHIVING PURPOSES IN THE PUBLIC INTEREST" UNDER RECITAL 158)

The GDPR allows for a number of exemptions in favour of "archiving purposes in the public interest". Recital 158 explains the meaning of this expression.

> "Public authorities or public or private bodies that *hold records of public interest* should be services which, pursuant to Union or Member State law, 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." (emphasis added)

Which archive services fall under this definition? As one can see, it is not the nature of archives, but the mission of the institution that holds them that determines whether the exemption can be applied. It is safe to say that National Archives and other historical Archives run by the State or by other public bodies, carry out "archiving purposes in the public interest" according to the GDPR definition, as do the Historical Archives of the European Union.

In accordance with Member State law, other institutions preserving archives can also fall under this definition. For example, national law might dictate that a specific body has the mission of acquiring, preserving and making available to researchers the personal papers of writers; or it could create a museum on the history of science that includes among its tasks the acquisition and preservation of the personal papers of scientists. Member State law might create an institute for the history of a past authoritarian regime, whose mission includes the preservation of documentary heritage concerning the victims of political repression.

It is important to consider that when the GDPR refers to "national law" it does not mean only pieces of law approved by national parliaments. Recital 41 in fact stipulates that "Where this Regulation refers to a legal basis or a legislative measure, this does not necessarily require a legislative act adopted by a parliament". The legal instrument that can assign to an entity the legal obligation to acquire, preserve, arrange and communicate archives can change from one country to another, in accordance with different constitutional systems. For example, it could be a national law, a regional law, a ministerial decree, and so on and so forth. At any rate, archivists should consider that an archive service or another cultural institution which has the statutory mission of acquiring, preserving and providing access to archives for general public interest, would fall under the definition of recital 158.

Not all the entities that preserve archives have a legal obligation to acquire them and thus not all of them fall under the definition of recital 158. In many cases, however, such entities have a clear cultural mission and preserve archives for the purpose of historical research. The GDPR allows for exemptions for processing of personal data for historical research, which are laid out throughout the Regulation and in particular in article. 89.

Finally, archivists should be aware that exemptions in favour of "archiving purposes in the public interest" concern only the processing of personal data included in the archival fonds that archive services keep. All of the other personal data processing carried out by archive services fall under the same rules that apply to any other public or private entity. In other words, when archive services process the personal data of users, or of students who participate in educational activities, or of participants to conferences and so on, they do not enjoy of any exemption to the rules.

5. SAFEGUARDS AND DEROGATIONS RELATING TO PROCESSING FOR ARCHIVING PURPOSES IN THE PUBLIC INTEREST, SCIENTIFIC OR HISTORICAL RESEARCH PURPOSES OR STATISTICAL PURPOSES (ART. 89)

Throughout the GDPR one can find many references to archives and historical research. Several articles that set out duties or prohibitions for the controller, in fact allow for exemptions when the processing is necessary for archiving purposes in the public interest, scientific or historical research purposes.

Moreover, the GDPR includes an article specifically dedicated to "processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes" (art. 89). The first paragraph of this article lays down rules that are common for both processing of personal data "for archiving purposes in the public interest" and for processing for "scientific or historical research purposes or statistical purposes".

> 1. 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.

Article 89 further states that

> 2. Where personal data are processed for scientific or historical research purposes or statistical purposes, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18 and 21 (…)
>
> 3. Where personal data are processed for archiving purposes in the public interest, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18, 19, 20 and 21 (…)

In both cases, the above mentioned derogations are possible

> (…) subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.

The principle of data minimisation and the obligation of taking appropriate safeguards in order to protect data subjects' rights are therefore common to both "processing for archiving purposes in the public interest" and processing for "scientific or historical research purposes or statistical purposes". But the concrete application of these principles will be different in the different areas.

When doing medical research it is important to preserve the correlation of different medical data regarding a given patient but the identity of the patient is irrelevant. In this case, pseudonymisation of medical records would be an appropriate measure. However, an archive service that holds records in the public interest has to preserve the integrity of medical records selected for permanent preservation in the interest of the data subjects. For example, in recent times some countries were able to pay compensation to persons who had been subjected to compulsory sterilisation decades ago because the integrity of the medical records was guaranteed. European history provides for many other instances in which the integral preservation of documents containing personal data has been instrumental in restoring the rights of data subjects.

Enforcing the right to the truth and the right to remedy and reparation for victims of gross violations of human rights requires the integral preservation of archives

Victims of Fascist and Nazi persecutions or of the Nazi use of slave labour could be identified and indemnified because archives containing personal data had been preserved. The integral preservation of archives has been equally instrumental in returning confiscated properties after the fall of Communism. The GDPR encourages the integral preservation of archives documenting human rights violations. Recital 158 in fact states:

> "Member States should also be authorized to provide for the further processing of personal data for archiving purposes, for example with a view to providing specific information related to the political behaviour under former totalitarian state regimes, genocide, crimes against humanity, in particular the Holocaust, or war crimes."

When they take decision about retention or disposal of records containing personal data, archivists should remember that personal data protection needs to be balanced against the right to justice, the right to the truth and the right to remedy and reparation for victims of gross violations of human rights.

Acknowledging that processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes requires different kinds of measures in order to enforce the principle of data minimisation, the GDPR does not always require pseudonymisation but only when "those purposes can be fulfilled in that manner".

Archivists enforce the principle of data minimisation differently than scientists and statisticians. Firstly, they select records that contain personal data for permanent preservation only when it is really necessary to do so pursuant to the mission that the law assigns to their archive service. They furthermore enforce laws concerning access to archives, excluding access to documents that contain personal data for as long as their

national law requires. Statutory restrictions on access to archives differ from one country to another and for certain kinds of personal data the closure period can be as long as 120 years.

When documents that contain personal data become accessible, but there is still a chance that the data subject is alive, archivists abstain from any processing that could result in harm to the dignity of the data subject. They always keep art. 1 of the Charter of Fundamental Rights of the European Union in mind: "Human dignity is inviolable. It must be respected and protected." A concrete enactment of this principle is to abstain from publishing online archival documents or finding aids whose diffusion could harm the dignity of data subjects.

Archive services might also make use of pseudonymisation, but if practiced by archive services, pseudonymisation should be fully reversible and should be done in a way that does not endanger the evidential value of records. In case of personal data preserved for archiving purposes in the public interest, archive services should store unaltered original data in a protected storage facility and make a pseudonymised copy of personal data for access by researchers, if such purposes can be fulfilled in that manner.

Does the GDPR allow for the preservation of business archives containing personal data?

Some private companies preserve century-old archives including personal data, which are troves of information for historians. Will historians of the future be able to access similar archival sources? In other words, is the preservation of business archives containing personal data possible under the GDPR? There is no a simple answer to such a question.

Records created by private bodies can be processed for archiving purposes in the public interest just like those created by public bodies. Such processing, however, qualifies as "archiving purposes in the public interest" only if it is performed by a public or private body that has "a legal obligation to acquire, preserve, appraise, arrange, describe, communicate, promote, disseminate and provide access to records of enduring value for general public interest." (recital 158) What "legal obligation" means, differs in civil law countries and in common law countries.

Bodies that have a historical research mission, but do not have a legal obligation to acquire and process archives, can process business archives containing personal data for historical research purposes. Both the principle of "purpose limitation" and that of "storage limitation" (art. 5(1), points b) and e)) allow in fact for derogations not only for archiving purposes in the public interest, but also for historical research purposes. Such derogations are subject to implementation of appropriate measures in order to safeguard the rights and freedoms of the data subject. The interpretation of such provisions will become progressively clearer, as long as DPAs and the EDPB issue decisions and guidelines.

IV. DATA SUBJECTS' RIGHTS

6. THE HEART OF THE MATTER: GRANTING INDIVIDUALS CONTROL OVER THEIR PERSONAL DATA

One of the main goals of the GDPR is to grant individuals control over their personal data. For this reason, it provides them with a comprehensive set of rights regarding their own personal data (the right to know which data are processed and why, the right to access, to erase and to transfer them, etc.), which allow only limited exemptions. Archiving purposes in the public interest is a ground for derogation from most of data subjects' rights. In two cases – the right to information (art. 14) and the "right to be forgotten" (art 17) – the GDPR directly introduces derogations for archiving purposes in the public interest. In other cases, it allows member States to do so. As already mentioned, in fact, art. 89 allows member states to provide derogations from the rights referred to in articles 15, 16, 18, 19, 20 and 21. This means that archivists in different EU countries might have to obey to different laws, regarding some data subjects' rights.

In all such cases, exemptions are not absolute, but subject to the safeguards provided by art. 89(1), i.e. technical and organizational measures aimed at enforcing the principle of data minimisation, and the protection of the data subject's rights and freedoms. Moreover, archive services should allow data subjects to have the widest possible control over their data. This principle has special relevance when archive services preserve the personal papers of living individuals, who donated, sold or deposited them in archive services; or when archive services preserve oral interviews collected during oral history projects. Archive services, however, cannot accommodate data subjects' requests, if that would imply violating the archive services' statutory mission of preserving the integrity of archives and of arranging, describing and making them available to the public.

7. INFORMATION TO BE PROVIDED WHERE PERSONAL DATA HAVE NOT BEEN OBTAINED FROM THE DATA SUBJECT (ART. 14)

The GDPR states that the controller has to provide data subjects with certain information regarding the processing that he or she carries out. This is applicable even if the controller did not obtain the personal data directly from the data subject, as set out in article 14. This is generally the situation of archive services which process documents containing personal information that they did not collect, but were collected by the entity that created the archive.

However, the GDPR allows for some exemptions, and one concerns archives. Article 14 states in fact that the obligation to provide information to data subjects where personal data were not obtained from the data subject does not apply when it would be "impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes". In such cases, art. 14 explicitly encourages controllers to make the information about the processing publicly available.

When archive services acquire, arrange, describe, preserve and make available to researchers archival fonds containing personal data regarding an indefinite number of

persons, to the extent that informing data subjects about such processing would be "impossible or would involve a disproportionate effort", the best line of action seems to make information about such processing available on the web site of the archival service, so that the general public can learn about it.

In some cases, a more focused effort to inform data subjects might be undertaken. For example, if an archive service acquires the archive of an association, a political party or a trade union, that processed personal data only of its associates, it might agree with them to use their information channels (newsletters, websites, mailing lists, etc.) in order to inform their associates about the processing that the archive service will perform.

Art. 14 includes a detailed list of the pieces of information that controllers should provide to data subjects when personal data have not been obtained from them. In a nutshell, archive services should explain in terms easily understandable by someone who knows nothing about archives, what kind of data processing they perform and why, and what is the legal basis for that. Moreover, they should inform data subjects how they can access their data and also explain that archival fonds are accessible to users, subject to the statutory limitations on access to records containing personal information. Finally, if data subjects contact archive services to ask for information about the kind of processing they perform, archivists should be prepared to provide data subjects with all possible information about that.

8. RIGHT OF ACCESS BY THE DATA SUBJECT (ART. 15)

As a rule, data subjects have a right to obtain confirmation from the controller whether or not personal data concerning him or her are being processed. Moreover, data subjects also have the right to know the purposes of the processing, the categories of personal data concerned and other information regarding the processing of their personal data.

Archive services process large amounts of personal data that have been collected by other entities. When these entities transfer their records to an archive service, they should transfer finding aids as well to allow archive services to know, among other things, which personal data the transferred records contain. It nevertheless frequently happens that archive services receive transfers without detailed finding aids but with only a generic transmission list. As a consequence, archivists cannot know which personal data are included in the transferred records. Moreover, archive services often receive archives that have lost their original order and require a careful work of arrangement to restore it.

These conditions create objective difficulties in enforcing some of the rights of data subjects' provided by the GDPR. The GDPR acknowledges this and, as already mentioned, article 89 provides that Union law or member states law may introduce derogations from the rights of data subjects.

Archivists should therefore verify if national law introduced derogations from the data subjects' right of access provided by article 15 of the GDPR. Such derogations protect archivists from liability if they are unable to fully comply to requests from data subjects for information about the processing of their personal data by an archive service. However, these derogations do not exempt archivists from doing their best to comply with such requests from data subjects.

If a data subject approaches an Archive service in order to access his/her personal data, archivists should provide all possible assistance by explaining how to do research in the archives, indicating the archival fonds most likely to contain personal data and by explaining how to consult finding aids and submit requests to consult files. If the data subject has specific difficulties in doing research due to old age, level of literacy or a physical impediment, archive services will provide special assistance, to the extent of the possible, taking into account constraints such as the number of staff.

9. RIGHT TO RECTIFICATION (ART. 16)

Art. 16 of the GDPR stipulates that data subjects have the right to have their personal data rectified if they are inaccurate and completed if they are incomplete. The controller has to comply with data subject's requests "without undue delay".

Archive services must guarantee the integrity of archives in order to retain the evidential value of documents. This is necessary to protect the rights of data subjects. For example, police files of repressive regimes typically include derogatory information about political opponents. Maintaining the integrity of such files is necessary to allow data subjects to request indemnification for the discrimination they suffered at the hands of the repressive regime.

The GDPR allows to reconcile the responsibility of archive services to maintain the integrity of documents, and the right of data subjects to have incomplete personal data completed. Rectification can be achieved by "providing a supplementary statement". Moreover, as already mentioned, article 89 provides that Union or Member State law may introduce derogations from the rights of data subjects' provided by article 16.

Archive services shall facilitate the exercise of a data subject's right to have their data updated, rectified or supplemented by "providing a supplementary statement" and ensure that the data are kept in a way allowing the original source material to remain separate and distinct from any such supplementary information.

10. RIGHT TO ERASURE ('RIGHT TO BE FORGOTTEN') (ART. 17)

The "right to be forgotten" within the EU was first stated in the 2014 landmark decision by the Court of Justice of the European Union in the Google Spain case. The Court ordered Google Spain to remove two reports on insolvencies from search results regarding a Spanish citizen, Mario Costeja González. The reports had been legitimately published by a newspaper in 1998 and continued to appear prominently when searching Costeja's name. The Court's decision left intact both the analogue and digital archives of the newspaper. It applies only to the result when searching Costeja's name with Google (the reports remain retrievable when using other search terms). Following the Court decision, persons can request that personal data relating to them (if they are inadequate, irrelevant or no longer relevant) are delinked from search engines so that such data will no longer appear if one searches their name.

The decision by the EU Court of Justice in the Google Spain case was grounded on Directive 95/46/EC which did not explicitly include a "right to be forgotten". By contrast,

the GDPR uses this expression in the title of article 17 "Right to erasure ('right to be forgotten')".

Under the GDPR, the right to be forgotten does not refer to delinking but to the actual erasure of the personal data. Article 17 grants in fact data subject the right to obtain from the controller the erasure of personal data concerning him or her without undue delay.

This right can apply where "the personal data are no longer necessary in relation to the purposes for which they were collected" or where "the data subject withdraws consent" on their processing, as well in some other circumstances. At the same time the right to be forgotten is subject to different restrictions, and it shall not apply if processing is necessary for archiving purposes in the public interest, if erasure "is likely to render impossible or seriously impair the achievement of the objectives of that processing" (art. 17(3)).

Recital 158 explains that public authorities and other bodies that hold records in the public interest are services that have "the legal obligation" to process archives selected for permanent preservation. The erasure of personal data included in archive documents would thus make it impossible for these services to carry out the mission that the law assigns to them. The right of erasure in article 17 of the GDPR therefore does not apply to documents selected for permanent preservation by archive services that fall under the definition of recital 158.

At the same time, archivists should remember that the right to be forgotten as stated by the EU Court of Justice (i.e. not erasure, but delisting of personal data) can be enforced by archive services without prejudice to their mission. Delinking or delisting, or in other ways preventing the use of search engines to search for names in documents does not in fact affect the integrity of archive documents nor does it endanger their permanent preservation. Moreover, archive services can prevent name search of an online document, while keeping it retrievable by using search keys different from personal names.

In the first place, archive services must abstain from posting online archival documents or finding aids that contain personal data which could jeopardize the dignity of data subjects. Moreover, whenever they post archival documents or finding aids that contain personal data of living individuals online, they have to consider – according to the nature of the personal data – whether it would be appropriate to post them in a restricted-access area of their websites which is out of the reach of search engines. On a case-by-case basis, archivists will assess how to best balance their legal obligation to "describe, communicate, promote, disseminate and provide access to records of enduring value for general public interest" (recital 158) with the principle of data minimisation (art. 5), which requires them to limit the processing of personal data to what is necessary.

11. RIGHT TO RESTRICTION OF PROCESSING (ART. 18) AND RIGHT TO OBJECT (ART. 21)

The GDPR grants data subjects both the right to obtain from the controller restriction of processing and the right to object to processing of personal data concerning him or her. What are the differences between such rights and what are their practical implications relevant for archive services?

Such rights share the same ultimate goal of granting individuals control over the processing of their personal data, but apply in different circumstances, and have different

consequences. What most matter to archivists, national law can introduce derogations from both such rights, in case of processing of personal data for archiving purposes in the public interest (art. 89(3)).

Under specific circumstances listed in art. 18(1), data subjects have the right to obtain the *restriction* of processing of their personal data. Of key relevance for archive services is that the restriction of processing does not prevent the storage of personal data (art. 18(2)). The preservation of archival documents, thus, cannot be the hampered by restriction.

Moreover, data subjects have the right to *object* to the processing of personal data concerning themselves, even if the processing "is necessary for the performance of a task carried out in the public interest". In that case, "the controller shall no longer process the personal data" (art. 21(1)). However, the controller can continue processing personal data, if he can demonstrate "compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject" (art. 21(1)). This provision might apply to the processing of archives in the public interest, but archivists should not take it for granted. It is advisable for them to keep informed on how Courts interpret this provision.

In the first place, archivists should verify if their national lawmakers made use of the possibility to introduce derogations from the rights to restriction of processing (art. 18) and to object (art. 21) and, in this case, if national law indicated which are the appropriate safeguards to the rights and freedoms of data subjects that archive services should take. If national law does not suggest the appropriate safeguards, archive services will consider, on a case-by-case basis, how to best enforce the principles relating to processing of personal data listed in art. 5 of the Regulation.

Finally, archivists should consider that

> Where personal data are processed for scientific or historical research purposes or statistical purposes pursuant to Article 89(1), the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest. (art. 21(6))

This provision might be relevant for archivists who work in museums or other cultural institutes or organizations that preserve archives for reasons of public interest, but do not carry out "archiving purposes in the public interest" according to the definition of recital 158.

12. NOTIFICATION OBLIGATION REGARDING RECTIFICATION OR ERASURE OF PERSONAL DATA OR RESTRICTION OF PROCESSING (ART. 19)

The GDPR dictates that "The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out (…) to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort." (art. 19). As already mentioned, national law can introduce derogations from the rights of rectification or erasure or restriction of processing, in case of processing of personal data for archival purposes in the public interest. It is therefore unlikely that personal data included in archival fonds preserved by archive services will be the object of rectification or erasure or restriction of processing.

Moreover, national law can introduce a derogation from the obligation of notification as well, if personal data are processed for archival purposes in the public interest (art. 89(3)). Finally, archivists should consider that a data controller should comply with the obligation dictated by art. 19, "unless this proves impossible or involves disproportionate effort" and this might be very much the case for archive services.

13. RIGHT TO DATA PORTABILITY (ART. 20)

The GDPR grants data subjects "the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format" (art. 20(1)). Moreover, "the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible." (art. 20(2)) Archive services do not receive the personal data included in the archival fonds they hold directly from the data subject, except in the case of personal papers. Most of the archival fonds processed today by archive services are in analogue format, so transmitting the personal data they include to the data subjects in a "machine-readable format" would, by and large, not be "technically feasible".

Finally, archivists should be aware that national law can introduce derogations from the right of data portability if personal data are processed for archival purposes in the public interest (art. 89(3)).

V. PROCESSING CATEGORIES OF DATA THAT REQUIRE SPECIAL SAFEGUARDS

14. PROCESSING OF SPECIAL CATEGORIES OF PERSONAL DATA

The GDPR provides special protection to certain categories of personal data, the processing of which could create significant risks to the fundamental rights and freedoms of data subjects. It forbids the

> Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation (art. 9(1))

However, the GDPR allows for some derogations from this provision. The prohibition to processing of such sensitive data does not apply in cases where "processing is necessary for archiving purposes in the public interest" and for historical research. Such processing must be based on law and must be "proportionate to the aim pursued". Moreover, it must "respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject." (art. 9(2) point (j))

For the most part, the provisions of article 9 are not new. Directive 95/46/EC already prohibited the processing of special categories of personal data, with some exemptions. The GDPR enlarged the categories of personal data deserving special protection, by adding "genetic data, biometric data for the purpose of uniquely identifying a natural person" to the list appearing in art. 9.

In accordance with national law in EU Member States, documents that contain special categories of personal data are excluded from access for extended periods, ranging from a few decades to a century or more. Archivists therefore already have a long and successful experience in applying laws that restrict access to special categories of personal data.

15. PROCESSING OF PERSONAL DATA RELATING TO CRIMINAL CONVICTIONS AND OFFENCES (ART. 10)

The GDPR sets very strict rules regarding the processing of personal data relating to criminal convictions and offences and does not allow for any exemptions. Processing of such a kind of personal data can "be carried out only under the control of official authority or when the processing is authorised by Union or Member State law". The law must provide for "appropriate safeguards for the rights and freedoms of data subjects" (art. 10).

In EU Member States, national laws dictate that after a certain number of years – generally 20 or 30 years – court decisions, court files and prison records selected for permanent preservation are transferred to the National Archives or to other archival institutions. These archive services therefore process large amounts of data relating to

criminal convictions: they select them, transfer them to their repositories, arrange and describe them and make them available to researchers. This kind of processing is fully compliant with the GDPR because it is dictated by law and carried out by official authorities with appropriate safeguards for the rights and freedoms of data subjects. For example, if national law restricts access to court files for a given number of years, archivists carefully enforce such restrictions. If they publish on line freely-accessible documents relating to criminal convictions, and there is a chance that the data subjects are still alive, archive services can take measures such as posting such documents on a restricted-access area of their websites, or redacting names, pursuant the paramount principle of respecting and protecting the dignity of individuals.

If a public or private body (e.g. a university, foundation or civil society organisation) holds legal archives or copies of court files and court decisions or otherwise collects, preserves and makes available to researchers documents containing personal data relating to criminal convictions and offences (for example: an academic centre specialized in the study of terrorism or a community archive set up by anti-mafia activists), it should contact its national DPA to seek instructions about the appropriate safeguards for the rights and freedoms of the data subjects concerned.

VI. DATA SECURITY

16. DATA PROTECTION BY DESIGN AND BY DEFAULT (ARTICLE 25): WHAT DOES IT MEAN IN THE ARCHIVES?

Article 25 dictates that when they are planning the means for processing personal data, controllers have to "implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles". This is what the GDPR refers to as "data protection *by design*".

One of the fundamental data-protection principles is data minimisation. In fact, Article 25 further requires that controllers "implement appropriate technical and organisational measures for ensuring that, *by default*, only personal data which are necessary for each specific purpose of the processing are processed." (emphasis added)

Article 25 will apply particularly to the development of new information systems. In the archives, this may involve, for example:

- Creating a digital repository;
- Creating a data bank concerning birth records or other fonds containing personal information
- Creating an information system to manage the reading-room services
- Creating tools for on-line access

Archive services have to keep article 25 in mind when they plan the different kind of activities that typically archive services perform, i.e appraisal, arrangement and description, providing access to archives and communicating them.

Appraisal: Archive services adopt an appraisal policy that limits the permanent preservation of records containing personal data to what is really necessary, according to their mission. They put into practice Article 25 by carefully drafting retention plans that define which kind of files containing personal data have to be selected for permanent preservation. For archive services, retention plans are tools to demonstrate compliance with Article 25.

Arrangement and description: Archive services enforce the principle of personal data minimisation when they create finding aids. When they arrange and describe an archival fonds that includes personal data of living individuals concerning health, sex life, political opinions and other special categories of data, or data relating to criminal convictions, archive services must create a finding aid that shows real names, in order to be able to respond to possible requests of access by data subjects, and comply with other data subjects' rights. At the same time, for online research (in case their national law allows access to such records) archive services might create a version of the finding aid in which real names are replaced by pseudonyms, if their mission to provide access to archives can be fulfilled in this manner. Software for archival description that allows the creation of two different versions of a finding aid (one with real names and one with pseudonyms) is a tool for compliance with art. 25.

Providing access to archives: Archive services are obliged to ensure that access to records is managed appropriately and that correct organisational and technical safeguards are in place. Archive services have a long history of managing and facilitating access to records

and archives, through organisational controls such as the application for a reader's ticket, checking that the requested files are cleared for public inspection and limiting the number of files presented in the reading room.

In the electronic environment, the issues of access will be compounded due to the scale, variety and complexity of electronic records. In many cases large data cannot be manually checked and verified prior to access so safeguards and controls will have to be increasingly automated.

Supervising activities and collaboration with creators of archives. Within the EU, the nature of the relations between the entities that create the archives and archive services change from one country to the other, and according to public sector and private sector. In some cases State Archives have supervising or monitoring or counselling authority, in others they do not.

Relevant to archive services is the design of new systems by public bodies whose records may be transferred to the archive services in the future. The challenge may be with regard to the design of new information systems that endeavour to comply with GDPR, where the archiving in the public interest is not included in the initial planning stage. It is important, therefore, that archive services are involved in system design and planning, to ensure that at the appropriate time the records are able to be exported from the system or replicated for ingest and transfer to an archive service. Ideally, the information system should automatically take into account the final destination of the documents.

17. SECURITY OF PERSONAL DATA (ARTICLE 32-34)

SECURITY OF PROCESSING

A key principle of the GPDR is that "the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk" (Article 32). This is the 'security principle'.

Doing this requires the controller and the processor to consider risk analysis, organisational policies, and physical and technical measures. They also have to take into account additional requirements about the security of the processing.

The controller and the processor can consider the state of the art and costs of implementation when deciding what measures to take, but these measures must be appropriate both to the circumstances and the risk posed by the processing.

The measures must ensure the 'confidentiality, integrity and availability' of the systems and services and the personal data that are processed within them. The measures must also enable the controller and the processor to restore access and availability to personal data in a timely manner in the event of a physical or technical incident.

The controller and the processor also need to ensure that they have appropriate processes in place to test the effectiveness of their measures, and undertake any required improvements.

RISK MANAGEMENT TECHNIQUES

The GDPR does not define the security measures that the controller and the processor should have in place. It requires them to have a level of security that is ‘appropriate’ to the risks presented by their processing. Before deciding what measures are appropriate, they need to assess their information risk through a formal risk management methodology.

PERSONAL DATA BREACHES

The GPDR creates a system of notification of personal data breaches (article 33). This notion of breach means "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data" (Article 4(12)). This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

When the personal data breach is likely to result in a risk to the rights and freedoms of natural persons, the controller shall notify the personal data breach to the supervisory authority competent as soon as possible and, if possible, not later than 72 hours.

The processor shall notify the controller without undue delay after becoming aware of a personal data breach (Article 33(2)).

The content of the notification is provided by the Article 33(3) of the GPDR.

SECURING THE PROCESSING OF PERSONAL DATA IN THE ARCHIVES AND SECURING FROM UNAUTHORISED ACCESS THE PERSONAL DATA HELD IN THE ARCHIVES

Archivists are responsible for the security of personal data in their care and, in accordance with existing professional practices, safeguard their integrity and authenticity and protect them from unauthorised access, alteration, loss, damage or destruction.

Records should be stored securely so that confidentiality is maintained at all times. Access should be provided only to those who have a need to know that can be satisfied within the law. Archival arrangements and provenance should not be compromised through the separation of personal and non-personal records.

The level of security should be appropriate and proportionate to the nature of the data and the harm that could arise from a breach in security. It must reflect professional standards and the utilisation of risk management techniques to assess the nature, level and impact of risks and the appropriate measures to be taken to protect the data.

Practical security measures to be considered include installing physical security devices such as intruder alarms, restricting access to secure areas, keeping a record of visitors and supervising their activities as far as possible. Electronic data should be secured, e.g. by means of software protection against viruses and Trojans, and password-controlled access for authorised users only. Personal data should be transmitted securely: encryption tools should be used for secure transmission of electronic personal data.

While archive services exist to preserve and provide access to documents, they must not disclose documents containing personal data unless they can reconcile the requirements of research, whether historical or for evidence, with the rights and fundamental freedoms of data subjects.

WHAT ARCHIVISTS MIGHT DO/SHOULD DO IN CASE OF A DATA BREACH?

In the event of a serious breach arising from the processing – be it storage, access, communication… – of documents, archive services must consider whether the breach is likely to cause significant damage to the interests of living data subjects. If so, notification of the breach should be considered under the terms of article 34(3) point (c) of the Regulation, and given to the supervisory authority.

Art. 34(1) states "When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay". However, in case this would involve 'disproportionate effort' – which of course could be so when a breach with regard to a large archival series containing thousands of personal data would occur – art. 34(1) point (c) offers the alternative of "a public communication or similar measure whereby the data subjects are informed in an equally effective manner". This could be, for example, a notice on the website or a communication via a mailing list.

Security breaches should be recorded and investigated and staff should be encouraged to report and respond to security incidents.

18. DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION (ARTICLES 35-36)

The GDPR requires controllers to carry out a data protection impact assessment (DPIA) prior to the processing, when the processing "is likely to result in a high risk to the rights and freedoms of natural persons" (Article 35(1)). "DPIAs are important tools for accountability, as they help controllers not only to comply with requirements of the GDPR, but also to demonstrate" compliance with the Regulation[3].

WHAT IS A DATA PROTECTION IMPACT ASSESSMENT (DPIA)?

The aim of a DPIA is to identify and to assess the risk that could arise for the individual (as citizen, client, patient, etc.) from a new type of processing. The Article 29 Working Party defined DPIA as: "a process designed to describe the processing, assess its necessity and proportionality and help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data by assessing them and determining the measures to address them."[4]

WHEN IS (OR IS NOT) A DATA PROTECTION IMPACT ASSESSMENT REQUIRED?

When new technologies for processing personal data or a new kind of processing operation is introduced, as a first step a risk assessment has to be carried out. If the nature of the data or the way of processing is likely to create a high risk for data subjects, a DPIA is required.

A DPIA is not necessary when the processing is *not* likely to create risks for data subjects, and when it is similar to previous processing activities for which a DPIA has already been

[3] Article 29 Working Party, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*, wp248 rev.01, 13 Oct. 2017.

[4] Ibidem.

carried out. The GDPR makes clear, in fact, that "A single assessment may address a set of similar processing operations that present similar high risks." (Article 35(1))

The Data Protection Authorities are expected to publish a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment and also of those which are not.

WHAT DOES "HIGH RISK" MEAN?

The GDPR does not define exactly what kind of processing could entail a high risk. It provides however a few examples, including one that might very well concern archive services, namely the processing on a large scale of personal data relating to criminal convictions or of sensitive personal data (i.e. data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, and data concerning health or a person's sex life or sexual orientation) (Article 35(3) point (b)). Moreover, when assessing whether the processing could result in a high risk for the rights and freedoms of data subjects, archive services should consider whether the personal data refer to vulnerable data subjects, such as for example mentally ill persons (recital 75).

WHEN DO ARCHIVE SERVICES HAVE TO CARRY OUT DPIAS?

Where archive services decide to digitise material or create digital finding aids to personal data, for use on site or online, a DPIA may be necessary. This will certainly be the case if they are going to process archival fonds containing sensitive personal data, such as medical files, criminal courts' case files, or the personal files of prisons' inmates.

The DPIA will ensure that the archive service has considered the data protection and privacy aspects of the proposed project or work and can satisfy or demonstrate to a Data Protection Authority that such concerns were addressed or factored into the design or implementation.

WHAT HAS TO BE DONE?

In the course of the data protection impact assessment, the planned processing operation and the legitimate interest of the operation has to be described in a systematic way. As a next step the proportionality and the necessity of the envisaged operation has to be evaluated. Then the risks for the rights and freedoms of the data subject have to be assessed followed by a detailed plan of the measures that will be taken to manage the risks. When the processing operation is running it has to be monitored on a regular basis and the DPIA has to be adapted when changes occur.

Some Data Protection Authorities published tools to help controllers to carry out a DPIA. See for example the free software produced by the French DPA: https://www.cnil.fr/en/cnil-releases-free-software-pia-tool-help-data-controllers-carry-out-data-protection-impact.

WHEN DOES THE SUPERVISORY AUTHORITY HAVE TO BE INFORMED?

The supervisory authority (i.e. the Data Protection Authority) has to be consulted if the data protection impact assessment indicates that processing "would present a high risk in the absence of measures taken by the controller to mitigate the risk" (art.36). If the supervisory authority considers that the planned processing does not conform with the

Regulation or the envisaged measures to mitigate the risk are not sufficient, it has to provide written advice to the controller.

VII. MEASURES FOR TRANSPARENCY AND PROMOTING COMPLIANCE

19. RECORDS OF PROCESSING ACTIVITIES (ARTICLE 30)

Article 30(1) states: 'Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility.'

The record of processing activities – also often referred to as '(data) processing register' – is a very useful means to support an analysis of the implications of any processing whether existing or planned. The record facilitates the factual assessment of the risk of the processing activities performed by a controller or processor on individuals' rights, and the identification and implementation of appropriate security measures to safeguard personal data – both key components of the principle of accountability contained in the GDPR.

This record must be in writing (including in electronic form), clear and intelligible. Since 'processing activities' within the context of the GDPR concern operations performed on personal data relating to an identified or identifiable natural person, only activities regarding personal data are concerned.

The obligation to keep a record of processing activities does not apply to organisations endowed with less than 250 employees unless they find themselves in the position of either carrying out processing likely to result in a risk (not just a high risk) to the rights of the data subjects, or if they are processing personal data on a non-occasional basis, or if they tend to be processing special categories of data under Article 9(1) (i.e. data concerning health, sex life, ethnic origins, political opinions and other kinds of sensitive information) or data relating to criminal convictions under Article 10.
If one of these circumstances applies – which in fact is the case for most, not to say all archival institutions – an organisation is obliged to maintain the record of processing activities.

Organisations and their representatives must provide this record to the Data Protection Authority (DPA) upon request.

WHICH INFORMATION SHOULD THE RECORD OF PROCESSING ACTIVITIES HOLD:

The record must contain specific information about every processing activity carried out:

- the **name and contact data** of:
    - the archive service, or its representative;
    - if necessary other organisations with whom the archive service established in common the purposes and means of the processing;
    - the Data Protection Officer (DPO) if the archive service has appointed one;

- The **purposes** for which the archive service processes personal information.

  Similarly to 'Historical research' which already has been recognised as a 'purpose' in the past, 'archiving (purposes) in the public interest' should be

sufficient as a goal. It is not clear whether or not the addition 'of public interest' must be added to motivate the information.

- A description of the **categories of persons** of which the archive service processes data.

  For example: students, conscripts, defendants, patients…

- A description of the **categories of personal data**. Also identify so-called 'sensitive' data such as information about health and judicial information.

  For example: professional activities, financial transactions, judicial information about criminal convictions and sentences, data from which political opinions can be derived, …

- The **date on which the data must be deleted** (if known).

  Attention: From the point of view of archive services, it is of particular importance to point out to archives' creators that 'retention period' must not be confused with 'disposal' of information, and that they should act in conformity with the Law on Archives and as stipulated in the archival disposal schedules. Data archived in the public interest must indeed never be destroyed.

- The **categories of recipients** to whom the archive service provides personal data.

  Please note that we are speaking of "recipient categories": that is to say, for example 'universities and research institutions', 'individual researchers'…

- Does the archive service share data with a **foreign country or an international organisation outside the EU**? Then it must indicate this in the record.

- The general description of the **technical and organisational measures** taken in order to secure the personal data the archive service is processing: description of the technology, applications, and software used for data processing, that is to say which type of 'data protection by design or by default' has been used.

Organisations should consider this record as an internal tool to help implement the GDPR. The record can contain any additional information that is considered of importance by the data protection officer (DPO) in function of the activities carried out, for example indication of legal basis for data processing or an overview of all breaches regarding personal data.

PROCESSING BY SUBCONTRACTORS

Please note: If an archive service mandates other parties to process personal data on its behalf, a 'data processing agreement' with these organisations must be signed. By concluding such an agreement, the archive service ensures that the third party does not use or process the personal data for its own individual goals.

Only processing agents who can fully guarantee that they abide by legal requirements should be appointed. Archive services deciding to outsource processing activities to third party providers remain fully responsible for abiding by the stipulations of the GDPR.

SOME MODELS OF RECORD OF PROCESSING ACTIVITIES ARE AVAILABLE ONLINE, FOR INSTANCE:

The model offered by the Belgian DPA, which is available in French and Dutch: https://www.privacycommission.be/fr/canevas-de-registre-des-activites-de-traitement

The French DPA published two model registers, one more complex and one more simple: https://www.cnil.fr/fr/rgpd-et-tpepme-un-nouveau-modele-de-registre-plus-simple-et-plus-didactique

The European Data Protection Supervisor (i.e. the EU's independent Data Protection Authority) published a "Register template" https://edps.europa.eu/data-protection/our-work/publications/other-documents/register-template-0_en

Member states might create a record of processing activities application, whose use is mandatory for public services. Belgium is a case in point.

20. DATA PROTECTION OFFICER (ARTICLE 37): DO ARCHIVES NEED TO APPOINT ONE?

The Data Protection Officer (DPO) assists the controller or the processor in all issues relating to the protection of personal data. Its main tasks are:

- to inform and advise the controller and the employees who carry out processing of their obligations under the GDPR and national data protection norms;
- to monitor compliance with the GDPR
- to provide advice as regards the data protection impact assessment (DPIA)
- to cooperate with the supervisory authority;

The GDPR introduced an obligation to appoint a DPO for public authorities and for private entities that carry out certain types of processing activities. All public authorities must have a DPO but this does not mean that each archive service in the public sector needs to appoint one. In many cases their parent institution might appoint a DPO whose responsibilities extend to the archive service. For example, a municipality might have a DPO responsible for monitoring compliance with the GDPR and counselling all the offices of the municipality, including the Municipal Archives.

Private sector entities must appoint a DPO if:

- Their core activity requires regular and systematic monitoring of data subjects on a large scale.
- Their core activity consists in the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation, or personal data relating to criminal convictions and offences.

It is very unlikely that foundations, museums, libraries, cultural associations, and other private sector bodies that hold archives carry out "regular and systematic monitoring of data subjects on a large scale". By contrast, it is entirely possible that their core activity consists in the processing of sensitive personal data.

There are, in fact, foundations, community archives and other private-sector bodies specialized in processing the archives produced by NGOs and human rights organisations in the course of their activities, which might include, for example, personal data revealing the racial or ethnic origin of persons victim of acts of intolerance. As already mentioned, there are academic centres specialised in the study of terrorism or community archives set up by anti-mafia activists that process personal data relating to criminal convictions and offences. There might be community archives that hold archives produced by feminist organisations that assisted women victims of violence and which include all sorts of highly sensitive personal data.

In all cases of this sort, private bodies processing archives should appoint a DPO. "The data protection officer may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract." (Article 37.6) Small entities might share the same DPO with other similar entities. It is very advisable for small bodies processing archives for "archiving purposes in the public interest" or for research purposes, to share the same DPO with other similar bodies so that the DPO can develop an expertise in the particular kind of personal-data processing that they carry out.

ANNEXES

GLOSSARY

Archive: The GDPR does not define the term "archive". Throughout these guidelines, "archive" is used to refer to the whole of the documents created and received by a person, family, or organisation, public or private, in the conduct of their affairs, and selected for permanent preservation. In some European languages, the same term is used to refer both to current records, and to records selected for permanent preservation. In this text, the term archive is used only to refer to records selected for permanent preservation.

Article 29 Working Party: Working group created in accordance with art. 29 of EU Directive 95/46. The working group was composed of representatives of the Data Protection Authorities in the Member States, the European Data Protection Supervisor and a representative of the EU Commission. The working group ceased to exist on May 25, 2018 when it was replaced by the European Data Protection Board (EDPB).

Controller: "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data" (GDPR, art. 4)

Data subject: the person whose personal data are processed.

Data Protection Authority (DPA): see Supervisory Authority

Data Protection Officer (DPO): The DPO assists the controller or the processor in all issues relating to the protection of personal data. The GDPR introduced an obligation to appoint a DPO for public authorities and for private entities that carry out certain types of processing activities.

European Data Protection Board (EDPB): the GDPR replaced the Article 29 Working Party with the EDPB. Unlike its predecessor, the EDPB has the status of an EU body with legal personality and is provided with an independent secretariat. It has extensive powers to determine disputes between national supervisory authorities and to give advice and guidance on key concepts of the GDPR. It is composed of the DPAs of the Member States and the European Data Protection Supervisor. The Commission has the right to participate in its meetings.

European Data Protection Supervisor (EDPS): The EDPS is an independent EU body responsible for monitoring the application of data protection rules within European Institutions and for investigating complaints.

Personal data: "any information relating to an identified or identifiable natural person ('data subject'); 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." (GDPR, art. 4)

Archivists should keep in mind that the GDPR protects only the personal data of living persons. However, national law may also provide for the protection of personal data of deceased persons.

Processing: "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction." (GDPR, art. 4)

Archivists should take into account that activities such as selecting documents containing personal data for permanent preservation, transferring them to an archive institution, arranging them, describing them, and making them available to users are all activities that are considered "processing of personal data" under the GDPR.

Personal data breach: "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed" (GDPR, art. 4).

This definition is of paramount relevance for archivists. It implies that if personal data have been selected for permanent preservation and enter into the custody of an archive institution, archivists must protect their integrity. Among the principles relating to processing of personal data, the Regulation incudes in fact "integrity and confidentiality" (art. 5). Accidental loss or alteration of such records would violate not only archival ethics but also the GDPR. The same is true if archivists allow unauthorised disclosure of, or access to personal data.

Processor: "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller" (GDPR, art. 4).

Pseudonymisation: "the 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." (GDPR, art. 4).

It is important to note that the GDPR suggests the possibility of pseudonymisation of personal data preserved for archiving purposes in the public interest or for historical research purposes and does not mention "anonymisation". Unlike anonymisation, pseudonymisation preserves the correlation of different data relating to a person as well as the relation between different data records. Pseudonymised personal data maintain their nature of personal data, and are therefore subject to the provisions of the Regulation.

Special categories of personal data: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, data

concerning health or data concerning a natural person's sex life or sexual orientation; genetic data, and biometric data where processed to uniquely identify an individual (GDPR, art. 9). Such kinds of data are often referred to as “sensitive personal data”.

Supervisory Authority: Art. 51 of the GDPR stipulates that Each Member State shall provide for one or more independent public authorities, which will be responsible for monitoring the application of the Regulation. Such authorities have different names in different countries (for example, in Finland “Office of the Data Protection Ombudsman”, in France “Commission Nationale de l'Informatique et des Libertés”, in Ireland “Data Protection Commissioner”, in Italy “Garante per la protezione dei dati personali”), and are commonly known as “Data Protection Authorities” (DPAs).

WHERE TO LOOK FOR FURTHER GUIDANCE

- The European Commission has a section on its website "Data protection. Rules for the protection of personal data inside and outside the EU" https://ec.europa.eu/info/law/law-topic/data-protection_en where it has published some FAQs on the GDPR, e.g. What is personal data? What constitutes data processing? What are Data Protection Authorities (DPAs)?, etc.). The information is intended for readers who have no prior knowledge on the GDPR. Currently, it is only available in English.

- *Handbook on European data protection law*, 2018 edition – http://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law.
  The handbook has been prepared by the EU Agency for Fundamental Rights (FRA), with the Council of Europe (together with the Registry of the European Court of Human Rights) and the European Data Protection Supervisor. It outlines both the European Union (EU) and the Council of Europe (CoE) data protection law and includes selected case law of the European Court of Human Rights (ECtHR) and the Court of Justice of the European Union (CJEU).

- The European Data Protection Board (EDPB) is going to publish guidelines, recommendations and best practises. It will thus be useful to keep an eye on its website https://edpb.europa.eu/edpb_en, which is in all of the EU languages (although, for the moment, several documents are available only in English). On its first day of existence, the EDPB endorsed the guidelines produced by its predecessor, the Article 29 Working Party.

- The Article 29 Working Party (which ceased to exist on May 25, 2018) published nine guidelines and other documents on the implementation of the GDPR, aimed at contributing to a uniform interpretation and implementation by the different DPAs and governments throughout the EU. The European Data Protection Board (EDPB) endorsed all of such documents and made them available on its website https://edpb.europa.eu/edpb_en

  – *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679* (wp251rev.01), 13-02-2018

  – *Guidelines on Consent under Regulation 2016/679* (wp259), 24-01-2018, [adopted, but still to be finalized]

  – *Guidelines on Data Protection Impact Assessment (DPIA) on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679* (wp248rev.01) 13-10-2017

  – *Guidelines on Data Protection Officers ('DPOs')* (wp243rev.01), 30-10-2017

  – *Guidelines on Personal data breach notification under Regulation 2016/679* (wp250rev.01), 13-02-2018

- *Guidelines on the application and setting of administrative fines* (wp253). Now including available language versions, 13-02-2018

- *Guidelines on the Lead Supervisory Authority* (wp244rev.01), 31-10-2017

- *Guidelines on the right to "data portability"* (wp242rev.01), 27-10-2017

- *Guidelines on Transparency under Regulation 2016/679* (wp260), 24-01-2018 [adopted, but still to be finalized]

- *Position paper on the derogations from the obligation to maintain records of processing activities pursuant to Article 30(5) GDPR*, 19–04-2018.

- The Data Protection Authorities of EU Member States publish information material such as pamphlets, info sheets, infographics, translations of Article 29 Working Party Guidelines, to explain their new rights to citizens, and to help public administrations and small and medium-sized enterprises to comply with the GDPR. Check the website of your DPA! Its coordinates can be found on https://ec.europa.eu/justice/article-29/structure/data-protection-authorities/index_en.htm.

- The European Data Protection Supervisor (EDPS) has a *Glossary* (in English, French and German) with over 70 entries on its website: https://edps.europa.eu/data-protection/data-protection/glossary_en. It has moreover published a free-access Reference Library (https://edps.europa.eu/data-protection/data-protection/reference-library_en) and other informative materials, mostly intended to guide EU institutions in the implementation of the GDPR, but which can be helpful for national public and private bodies as well.

- The National Archives of the UK, in conjunction with government archiving policy leads and the Archives and Records Association, has prepared a *Guide to archiving personal data*, and made it is freely available on its website. It can be a useful reading also for archivists from other member states, providing that they keep in mind that this *Guide* is specific to the British legal system.
  http://www.nationalarchives.gov.uk/information-management/legislation/data-protection/