PANELFIT

PARTICIPATORY APPROACHES TO A NEW ETHICAL AND LEGAL FRAMEWORK FOR ICT

Guidelines on Data Protection Ethical and Legal Issues in ICT Research and Innovation.

THE GDPR – MAIN TOOLS AND ACTIONS

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039. This document reflects only the author's view and the Agency is not responsible for any use that may be made of the information it contains.

5 Main Tools and Actions

5.1 Creating or Gaining Access to a Dataset

Frederic Tronnier (GUF)

This part of The Guidelines was reviewed by Aurélie Pols (DPO) and Iñigo de Miguel Beriain (UPV/EHU).

This part of The Guidelines has been reviewed and validated by Marko Sijan, Senior Advisor Specialist, (HR DPA)

This section provides guidelines for researchers willing to gain access to an external database or for controllers willing to provide access to their databases in exchange of a compensation. It is built on several fundamental hypothesis:

- Databases are, in general valuable. This value derives from two different sources:
  - The information they contain
  - The structure and organization they are built upon. A well organized, documented and structured database is much more valuable than a chaotic database.
- The data involved are personal data. This is:
  - The data involved are not anonymized data. Anonymous data are not personal data and therefore, they fall outside the scope of the GDPR[1], therefore these data can be sold or bought as any other commodity. We are not focusing now in such a data type;
  - Personal data, regardless of whether they have been pseudonymized or not, are protected by the GDPR and must be processed according to this regulation.
  - Data about deceased people are not considered personal data[2]. It generally, does not fall under the obligations laid out by the GDPR (Recital 27) yet possible local interpretations might apply (see the National Reports complementing these Guidelines). Additionally, it is important to keep in mind that if data is obtained from deceased people and are used to gain information about living relatives (genetic data, for instance) this data might be considered as personal data of the relatives.[3]
- The situation might be totally different if the third party will use the database for research purposes under the umbrella of article 89 of the GDPR or not (see the section about data protection and scientific research). This difference mainly relates to the purpose limitation principle (Article 5(b) of the GDPR).

5.1.1 Value in the structure: Sui generis database rights

A well-structured database holds value. This value derives from the work done by a controller who has made an effort to ordinate the data. **As the creators of a database, researchers are the holders of *sui generis* database rights.** These rights were implemented by Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, which was afterwards amended by the "copyright" directive[4]. They recognize the right to the maker of a database "to prevent

[1]Recital26 of the GDPR for additional information.
[2] See Recital 27 of the GDPR.
[3] National regulation, however, must be considered. There are huge differences between the different Member States. See our D21, Issues and gaps analysis on informed consent in the context in ICT research and Innovation
[4] Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC

extraction and/or re-utilization of the whole or of a substantial part, evaluated qualitatively and/or quantitatively, of the contents of that database."[5] Through sui generis database rights, researchers, acting as controllers, can protect the content of the database, provided that 1) they are able to show that there has been qualitatively and/or quantitatively a substantial investment in either the obtaining, verification or presentation of the contents and 2) researchers are based in the EU or are EU residents.

The right lasts for 15 years once the database is completed but can be continuously renewed for 15 years if substantial investments are made towards the database.

The sui generis database rights can be disclosed and licensed like copyright. Asking for a payment against licensing a database is, thus, perfectly lawful. However, the disclosure of such rights often involves providing access to the database's content to a third party. Therefore, controllers must ensure that they have a legal basis for such processing.

There are other rights that might also protect a database, mainly copyright obligations (possible, maybe not probable) and rights related to data protection. Thus, before accessing a database or disclosing it, a database owner should ensure about whether any of them applies or not.

5.1.2 Paying for access/asking for payment: the legal issues

If we now focus on individual datasets, and not databases, we should not talk about sui generis rights any longer, since the scenario would be totally different. We are now talking about selling/buying data as such. As previously stated, this is only lawful if data are not at all personal data. Thus, researchers who are willing to sell the data gathered should anonymize the datasets before selling them (See "Identification", "Pseudonymization" and "Anonymization", within Part II section "Main Concepts"). This is because anonymous data doesn't fall under the GDPR requirements (as described in the previous section).

If anonymization is not possible, the question that remains is **whether access to personal data could be granted to a third party for commercial purposes or whether a researcher could gain access to such database by paying a fee** – via a license for using the data or sharing the entire database. This issue requires careful consideration of at least the following **factors**:

(1) Selling or buying access to personal data is considered as 'processing' under Art. 4(2) because it is a form of 'dissemination' or making data available to a third party. As with all other types of processing, GDPR requirements must be observed;

(2) The most common legal basis for processing for a purpose other than that for which the personal data has been collected initially is the data subject's consent or a Union or Member State law, which constitutes a necessary and

[5] Article 7(1) of Directive 96/9/EC of the European Parliament And Of The Council of 11 March 1996 on the legal protection of databases. This Directive was

proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1)[6];

(3) If these conditions do not apply (…) the controllers shall, to ascertain whether processing for another purpose is compatible with the purpose for which the personal data was initially collected, **perform a Compatibility Test as described by Article 29 WP[7].** To undergo such as test, the following criteria must be taken into account, inter alia (Art. 6(4)):

i. **Any link** between the purposes for which the personal data have been collected and the purposes of the intended further processing (this is called the 'link factor')

ii. The **context** in which the data have been collected, in particular **regarding the relationship between data subjects and the controller** (the 'context factor')

iii. The **nature** of personal data, in particular whether special categories of personal data are processed, for instance biometrical data (the 'data factor')

iv. The **possible consequences** of the intended further processing for data subjects (the 'consequence factor'), meaning the likelihood and severity of negative consequences that could arise for the data subject through the further processing

v. The existence of appropriate **safeguards**, which may include encryption or pseudonymization (the 'safeguard factor'), meaning how the data could be secured

All these factors are required to evaluate if the purpose of the new processing is compatible with the purpose of the current processing for which the data was initially gathered. The closer the link between the initial purpose and the further processing purpose is, and the lower the possible negative consequences are, the higher is chance that the transmission of the database is lawful. However, many of the factors above can clearly be used to argue against the lawfulness of an unconsented disclosure of a database, which will be explained in the following:

i. If the disclosure is unrelated to the original project (e.g., if your research project is finished and afterwards you conclude that you would like to monetize the data), the **link factor** is not given.

ii. The **context factor** may be interpreted as indicating that the more *foreseeable,* in other words obvious, the further processing purpose (from the data-subjects' perspective), the more likely it is that it will be found compatible with the original purpose and thus *lawful* under Art. 6. If the data subjects have not been informed

[6] See article 6(4) of the GDPR

[7] A29WP, Opinion 03/2013 on purpose limitation Adopted on 2 April 2013 (WP 203). At: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf (Accessed: 27 May 2020)

that the data is to be disclosed to a third party, and data subjects have not consented to this, the context factor will clearly act against the lawfulness of the processing.

iii. The **data factor** can be interpreted as indicating that the more sensitive the data, the more unlikely it will be for the further processing (here, selling) to be found compatible with the original purpose. Said in other words, if the dataset contains special categories of personal data, such as biometric data or data concerning the sexual orientation of the data subject, providing access to third parties can only happen if a legal ground for such processing applies, according to Art. 9 of the GDRP. Art. 9 prohibits the processing of these "special categories" unless specific circumstances, such as the explicit consent to the processing (Art. 9(2)(a)) are met.

iv. The **consequence factor** suggests that the potential impact of sale of the dataset on data-subjects has to be considered in determining whether that sale operation is compatible with the initial purposes for which the data were processed. Usually, companies buy data to enlarge their customer bases. Consequently, they will try contacting data-subjects for their commercial needs. Such interference with the customer's right to privacy is likely to be considered a significant 'impact' which speaks against the lawfulness of the disclosure of a database.

v. The **safeguard factor** requires different considerations. In general, the higher the risks are for the data subjects, the stronger the safeguards need to be. This means that data should be encrypted, protected and pseudonymized as best as possible.

Therefore, before providing access to personal data, the best option is **to obtain the data subjects consent or make sure that a Union or Member State law,** which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23**, applies.** In the absence of any of these circumstances, lawfulness of processing would be unjustifiable.

It also means that questions need to be raised by the parties involved and between them to be able to undergo the compatibility test. Additionally, contracts should support the transfer between the parties to assure each party's legal obligations are met.

Some examples of compatibility processing test

Further processing is possible

A bank has a contract with a client to provide the client with a bank account and a personal loan. At the end of the first year the bank uses the client's personal data to check whether they are eligible for a better type of loan and a savings scheme. It informs the client. The bank can process the data of the client again as the new purposes are compatible with the initial purposes.

Further processing isn't possible

The same bank wants to share the client's data with insurance firms, based on the same contract for a bank account and personal loan. That processing isn't permitted without the explicit consent of the client as the purpose isn't compatible with the original purpose for which the data was processed.[8]

5.1.3 Disclosure of data for research purposes and the purpose limitation principle

If data will be used for research purposes, consent of the data subject is not needed for the disclosure. According to article 5(b) of the GDPR, using the data gathered for research purposes is lawful and compatible with the purposes for which the personal data were initially collected (provided that technical and organizational measures are in place in particular in order to ensure respect for the rights and freedoms of the data subject and that article 89(1) applies) (see "Purpose limitation principle" within Part II section "Principles" of these Guidelines).

Further regulatory previsions do not seem to be necessary, either, even though article 9(2) (j) explicitly mentions the need for processing to be "based on Union or Member State law which shall be proportionate to the aim pursued, 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". Recital 159 and 33 introduce the notion of broad consent for scientific research, meaning that the exact processing must not be fully specified in advance. Data subjects should however be given the option to give consent to specific areas of research and to withdraw consent for other parts of the research objective. (see "Data protection and scientific research" in Part II section "Main Concepts").

5.1.4 Agreements

Even if a controller manages to find a legal basis to provide access to the data to a third party, this does not mean that the guarantees and requirements of the GDPR do not apply to these datasets. Similarly, a researcher who gains access to a database must be aware of the legal implications that their new position (as controller, joint controller or processor) might bring about (see the "Main Actors" section within Part II of these Guidelines). Furthermore, the fairness and transparency requirement will have to be met again. This means that data subjects must be made aware of their rights as to this further processing. All the other principles of the GDPR will have to be complied with in relation to this further processing as well.

[8] Source: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/purpose-data-processing/can-we-use-data-another-purpose_en (addressed 27 May 2020)

In order to clarify the roles to be played by different parties involved in data transfer agreements and ensure that GDPR provisions are adequately implemented, contracts are necessary and advised. These contracts should encompass all the details of the data processing operations, including the subject matter (data to be processed), the duration of the processing, the purpose of the data processing, the nature of the processing, the nature of the data, the categories of data subjects, etc. They should specify how the rights of data subjects will be protected and by whom. Everybody must be fully aware of what roles, responsibilities and rights every party involved has. Needless to say, contracts should also include clauses about security measures, data storage, audit rights, notification of breaches and, in general, all sensitive issues that are covered by the GDPR. These clauses should clarify the different obligations assumed by each signing party.

Standard contracts exist also for the different cases, including, for instance, joint controllership. Researchers providing access to their databases shall include detailed clauses devoted to consent management for further processing as they are the initial controller who passes on the personal data.

Regardless of whether the project is academic or commercial in nature, the controllers must provide to data subjects the same information which is provided when data is collected directly from data subjects, including but not limited to who is the controller and how to contact them, the purposes of the processing and the legal basis for the processing as well as the data subject rights. Additionally, data subjects must be informed from which source the personal data originate and whether it came from publicly accessible sources. The information obligation must be fulfilled within a reasonable period from obtaining the data, but at the latest within one month. Exceptions to this obligation apply (e.g., data subject has already the information). Full details on scope of this obligation and applicable exceptions are provided in Article 14 of the GDPR (see “Right to information” in Part II, section “Data Subject Rights”).

5.1.5 Territorial scope of the data

If the organization is established within the EEA, then the processing of the personal data will fall under the GDPR regime, regardless of whether the data relates to data subjects outside of the EEA or whether they have been collected/processed outside of the EEA or not (Art. 3(1)). Additionally, the GDPR will also apply if the offering of goods and services, as well as the monitoring of behavior takes place within the EEA (Art.3(2)(a) and Art.3(2)(b)), regardless of whether the data controller or processor are located within the EEA. GDPR also applies for data processing of personal data in places where “Member State law applies by virtue of public international law” (Art.3(3)) even if the data controller is not located in the EU.

If data is transferred outside of the EEA, the data subject should also be notified, and this international data transfer should be supported by some mechanism to make it lawful (Art.14(1) (f)) (See “Transfer of Data to Third Parties” in Part II section “Main Tools and Actions”)

DOs

- Before gaining access to a database, a contract between provider and the recipient of the data should define rights and responsibilities of each party involved in the transaction. This includes the definition of whether the purpose of the processing by the recipient is in line with the processing that the data subjects consented to before (compatibility test).
- Collect proof that substantial investments have been made for the creation of your database (not on the creation of data as such). This ensures the sui generis rights of the database which grant you the right to prevent others from using the database or extracting information from it.
- Be sure to have a legal basis for disclosure to third parties. Pass obligations on to recipients of data and make clear stipulations in the contracts between the parties involved.
- If you are considering the commercialization of data, make sure that the datasets do not contain any personal data (otherwise, commercialization would be illegal). You should ask as many experts as possible before commercializing data on your own.
- Consult with a data protection officer (if one has been appointed at your organization) or personal data protection specialists before the start of processing operations.

DON'Ts

- Don't use the paradigm of data ownership – it doesn't fit. Fundamental rights of data subjects cannot be 'sold'.
- Don't think that if you pay database makers to use their databases, you will be excluded from liability in those cases where the provider of the data infringed another right on a previous database. Always critically question the origin of the data you are about to accede, it's part of the due diligence obligations.
- Don't try to collect consent for every possible scenario. Broad consent is acceptable, but it cannot be considered a blank check.

- Do not try to influence or nudge individuals into giving you their personal data. Remember to offer participants a real choice.
- Never assume that the data you collected is uncritical. Don't skip the application of the GDPR because of the pseudonymization of personal data. In most cases it is much easier to re-identify data subjects that you think (e.g., due to advanced technologies which can correlate data from multiple sources and link to a specific person). Only if data is truly anonymized, it is no longer possible to reverse it to personal data.

Checklist

- The parties are well aware of the difference between licensing sui generis rights and buying/selling databases as such.
- The type of data at stake is clearly defined and the controller has ensured whether the GDRP is applicable or not.
- An agreement between the controller and the third party has been signed and it clarifies the roles to be played by each party.
- Adequate safeguards to protect data subjects' rights have been settled and all parties are aware of their obligations.

5.1.6 Further Reading

- A29WP, Opinion 03/2013 on purpose limitation Adopted on 2 April 2013 (WP 203). At: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf
- ICO: Principle (b): Purpose limitation. At: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/purpose-limitation/

5.2 Sharing data

Frederic Tronnier (GUF)

This part of The Guidelines was reviewed by Aurélie Pols (DPO) and Iñigo de Miguel Beriain (UPV/EHU).

This part of The Guidelines has been reviewed and validated by Marko Sijan, Senior Advisor Specialist, (HR DPA)

This part of the Guidelines provides advice for researchers who want to share processed data with other researchers or research organizations after having accomplished your original research task. The sharing of data with other researchers is likely to be considered a form of 'dissemination' or of making data 'available' to other researchers. Accordingly, it would be considered a different (further) processing than the original one, which involved data being 'used' to tackle a research question (see 'Gaining access to a database' in Part II section "Main Tools and Actions").

Proceeding on the assumption that no expressed consent has been obtained by the data subjects (otherwise the lawfulness requirement would be easier to meet under Art. 6(1)(a), there are various scenarios demanding different legal evaluations (See "Identification", "Pseudonymization" and "Anonymization" within Part II section "Main Concepts" of these Guidelines):

(1) If the data have been **pseudonymized** or appropriate safeguards against re-identification have been put in place, it may be easier for the 'sharing' of data to be found legal under Art. 6(4).

(2) Even if the data have **not** been **pseudonymized**, as long as the dissemination of data is considered necessary for scientific or historical research purposes (e.g. it is not meant to satisfy the morbid curiosity of other researchers, but to genuinely assist them in progressing in their field), then the processing is still likely to be considered to be compatible lawful processing operations (Recital 50), although it is still highly advised to obtain consent by the data subjects for the further processing. Recital 159 and 33 introduce the notion of broad consent for scientific research, meaning that the exact processing must not be fully specified in advance. Data subjects should however be given the option to give consent to specific areas of research and to withdraw consent for other parts of the research objective.

In any case, controllers will have to satisfy the **fairness/transparency** principle (see "lawfulness, fairness and transparency" in Patrt II section "Principles" of these Guidelines) again, making the data-subjects aware of their rights as to this further purpose (Art. 14(4)). All the other principles of the GDPR will have to be complied with in relation to this further processing as well.

As with sale of the personal data, be aware that you maybe in a joint controllership with the recipient of the data and that you are still responsible for the database, i.e. liable if infringements are made by the recipient of the data (see "Main Actors" in Part II of

these Guidelines). Therefore, as with all transactions, contracts between you and the recipient of the database are necessary and advised in order to provide all parties with clarity on the legal obligations and rights of every party involved. Contracts should specify the purpose of the recipient with the data as well as how the rights of data subjects will be protected and by whom.

DOs

- Before purchasing access to a database, a contract between provider and the recipient of the data should define rights and responsibilities of every party involved in the transaction. This includes to define whether the purpose of the processing by the recipient is in line with the processing that the data subjects consented to before.
- Treat every data with the same care as for personal data and remember that data may be aggregated with additional data from other sources. Thus, anonymization of personal data is very difficult.
- If you collect consent for sharing data, remember to keep language clear and simple to engage as many people as possible. Make it relevant to people's lives; use real-life, everyday examples where possible. This includes explaining what the data is needed for, what rights the data subjects have and how you protect the data and the data subject's privacy. Make sure to collect individual consent for each different purpose, for which you foresee the need to process the personal data.
- Collect proof that substantial investments have been made for the creation of your database (not on the creation of data as such). This ensures the sui generis rights of the database which grant you the right to prevent others from using the database or extracting information from it.
- Record everything you do and explain reason why.
- Be sure to have a legal basis for disclosure to third parties. Pass obligations on to recipients of data and make clear stipulations.
- If you have questions regarding the commercialization of data, ask as many

experts as possible before commercializing data on your own.

- Inform yourself on the GDPR by reading it. A clear understanding on the basic terms: 'personal data', 'processing', 'data processor', 'data controller' and 'data subject' is necessary but keep in mind that compliance with the GDPR is more than just these terms. Therefore, consult with a data protection officer (if one has been appointed at your organization) or personal data protection specialists before start of processing operations.
- For scientific research, use the EDPS opinion on data protection and scientific research[9]

DON'Ts

- Don't use the paradigm of data ownership – it doesn't fit. Fundamental rights of data subjects cannot be 'sold'.
- Don't think that if you pay database makers to use their database, you will be excluded from liability in those cases where the provider of the data infringed another right on a previous database. Always critically questions the origin of the data you are about to buy.
- Don't try to collect consent for every possible scenario, people will distrust you. However, don't also collect one consent for more than one processing purpose. Also, don't use jargon to hide intent or scare people off.
- Do not warn about economic consequences of withdrawal of consent or refusing giving consent. Remember to offer participants a real choice.
- Never assume that the data you collected is uncritical. Don't skip the application of the GDPR because of the pseudonymization of personal data. In most cases it is much easier to re-identify data subjects that you think (e.g. due to advanced technologies which can correlate data from multiple sources and link to a

[9] EDPS, 2020. A Preliminary Opinion on data protection and scientific research. Available at: https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf

specific person). Only if data is truly anonymized, it is no longer possible to reverse it to personal data.

5.3 DPIA (Data Protection Impact Assessment)

Bud P. Bruegger (ULD)

The final version of this section was validated by Hans Graux, guest lecturer on ICT and privacy protection law at the Tilburg Institute for Law, Technology, and Society (TILT) and at the AP Hogeschool Antwerpen. President of the Vlaamse Toezichtscommissie (Flemish Supervisory Committee), which supervises data protection compliance within Flemish public sector bodies.

In certain cases, the GDPR requires controllers to carry out a Data Protection Impact Assessment (DPIA). The following describes this concept by answering some key questions

The answers are predominantly based either on the GDPR itself and the guidelines provided by the Article 29 Data Protection Working Party on the topic (wp248rev.01)[10] that has been formally endorsed[11] by the European Data Protection Board[12].

Checklist

- Verify whether you need to conduct a DPIA for your processing activity.
  - See *In what cases must I carry out a DPIA?* below.
- Document this verification (no matter whether it was affirmative or not).

[10] wp248rev.01, ARTICLE 29 DATA PROTECTION 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, Adopted on 4 April 2017, As last Revised and Adopted on 4 October 2017, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236 (last visited 14/01/2020).

[11] Endorsement of GDPR WP29 guidelines by the EDPB, https://edpb.europa.eu/news/news/2018/endorsement-gdpr-wp29-guidelines-edpb_en, Brussels, 25 May 2018, Bullet point 6.

[12] https://edpb.europa.eu/

If a DPIA is necessary:

- Start as early as possible (following the principle of Data Protection by Design).
    - See *At what point in time does the DPIA need to be carried out/updated* below.
- Get an overview of what a DPIA is. See below:
    - *What is a DPIA*
    - *What are the purposes of a DPIA*
    - *What is the intended audience of a DPIA report*
    - *Who is responsible for carrying out a DPIA*
    - *What happens if I do not carry it out*
- Use the guidance and templates provided by the competent Data Protection Supervisory Authority (DPA) where possible.
- If not (your DPA does not provide such material or you have to cater to many areas of competence of different DPAs), follow the guidance provided by the Article 29 Working party in wp248rev.01.
    - See *Further Reading* below.
    - See *Is there a standardized method for carrying out a DPIA* for an overview and help in interpreting WP248rev.01.
- Assemble the team necessary to conduct the DPIA.
    - See *Who should be involved in carrying out a DPIA* below.
- Consider ways of facilitating your work.
    - See *What can facilitate carrying out a DPI*A below.

DOs

- Start working on the DPIA as early as possible.
- Emphasize and document the (continuous) process, not just the result (report).
- Use the DPIA as a decision tool for yourself.
- Involve the DPO and all other mandatory parties.
- Focus on technical and organizational measures that lower the risks to an acceptable level.
- Implement a schedule to revise and update the DPIA when required

DON'Ts

- Don't confuse the DPIA with IT security risk management.
- Don't consider the risks to your organization and its assets; consider the risks to data subjects and other natural persons who are affected by your processing.
- Don't understand risk as an undesirable event (such as an attack or a natural disaster); consider your processing as the source of risk, even if everything goes as planned.

Further Reading

- Guidance and Templates possibly provided by your competent Data Protection Supervisory Authority who is the main audience of the DPIA. (What exactly is available depends on where you are located)
- WP248rev.01, ARTICLE 29 DATA PROTECTION 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, Adopted on 4 April 2017, As last Revised and Adopted on 4 October 2017, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236 (last visited 14/01/2020).

5.3.1 What is a DPIA

A DPIA is a **continuous process**[13] that guides and supervises the implementation of a processing activity such that it complies with all data protection requirements and that the impact on natural persons is minimized. This process is documented in the **DPIA report**.

Next figure shows an illustration of the process provided by the Article 29 Working Party[14].

[13] wp248rev.01, page 14, Section III.D.a), 3rd paragraph: "Carrying out a DPIA is a continual process, not a one-time exercise."
[14] wp248rev.01, page 16, Section III.D.3), 2nd paragraph.

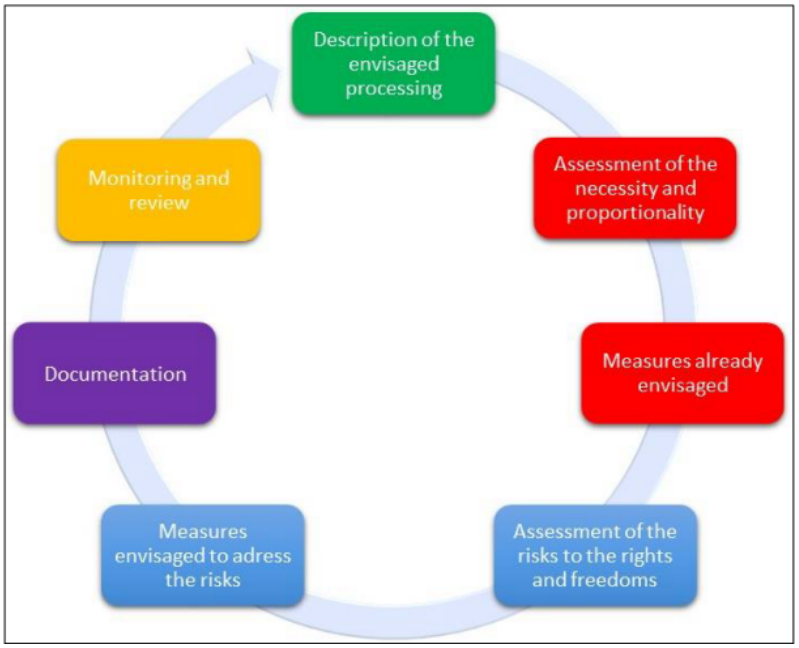


Figure 25: Generic iterative process for carrying out a DPIA according to the Article 29 Working Party.

5.3.2 What are the purposes of a DPIA?

The DPIA has two main purposes[15]:

(i) **building compliance** and
(ii) **demonstrating compliance**.

(i) The former refers to an **internal process** that accompanies the design and operations of a processing activity. By reaching compliance with the requirements of the GDPR, risks posed by the processing activities on data subjects are identified and mitigated. The process of conducting a DPIA installs data protection as a guiding principle that informs decisions[16] in a way to minimize the data protection risks and impact of processing for the affected persons. This affects in particular decisions about the purposes and means of the processing. It makes sure that data protection requirements are taken into account throughout all life cycle phases of the activity and not just as an "afterthought" when all decisions have already been made. In other words, it avoids that personal data can be processed without having identified its risks and impact and without implementing suitable safeguards and mitigation measures.

[15] wp248rev.01, page 4, Section I, 2nd paragraph: "In other words, a DPIA is a process for building and demonstrating compliance."
[16] wp248rev.01, page 14, Section III.D.a), 1st paragraph: "The DPIA should be seen as a tool for helping decision-making concerning the processing."

(ii) The latter refers to the **DPIA report** as a tool of accountability[17] that is used to demonstrate that a given processing activity complies with the GDPR.

5.3.3 What is the intended audience of a DPIA report?

The DPIA report addresses the following audiences:

(i) Persons who will be involved in the processing activities **(typically** of the controller and, optionally, processors)

(ii) including the **Data Protection Officer** (DPO),

(iii) the competent **supervisory authority**, and

(iv) (where possible,) the **public**.

(i) Considering that the DPIA guides decisions by the controller and (optionally) the processor(s), the DPIA report (in various versions and stages of completion) serves as a communication tool for the involved staff. This is of particular importance when considering the possibly interdisciplinary character of the work where for example, one kind of expertise is required to identify the risks and another to find adequate technical mitigation measures. Its role is further important when staff changes and when the processing activity evolves over time.

(ii) Data Protection Officers (DPOs) have responsibilities that refer directly to the DPIA. In particular, they have the task of providing advice where requested on the DPIA and monitor its performance[18].

(iii) A supervisory authority who investigates whether a given processing activity is compliant with the GDPR, may ask to receive a DPIA report (where required) as evidence that the obligation of Article 35 was satisfied – and more generally to assess compliance with the GDPR. In fact, a well-written DPIA report contains all the evidence necessary to demonstrate that the processing activity is indeed compliant.

(iv) Transparency is a key requirement of the GDPR. Accordingly, the Art 29 Working Party recommends considering the publication of at least a redacted version of the DPIA[19].

5.3.4 How is a DPIA different from a security assessment?

Many people are more familiar with IT security than data protection and use security metaphors to also think about data protection. Since this is highly misleading and may

[17] wp248rev.01, page 4, Section I, 2nd paragraph: "DPIAs are important tools for **accountability**, as they help controllers not only to comply with requirements of the GDPR, but also to **demonstrate** that appropriate measures have been taken to **ensure compliance** with the Regulation (see also article 24). [Highlighting added by the authors].

[18] Article 35(1)(c) GDPR

[19] wp248rev.01, page 18, Section III.D.d), 2nd paragraph: "Publishing a DPIA is not a legal requirement of the GDPR, it is the controller´s decision to do so. However, controllers should consider publishing at least parts, such as a summary or a conclusion of their DPIA."

lead to unacceptable DPIAs, this section explains the difference between data protection and security impact assessments.

In the GDPR, data protection and thus compliance is requires the implementation **of technical and organizational measures**[20]. It is somewhat misleading that the *records of processing* which are meant to demonstrate compliance[21], include only information about technical and organizational **security** measures[22]. It is therefore important to note that a DPIA goes beyond just describing measures and that the measures reported in a DPIA (Article 35(7)(d) GDPR) are by no means limited to only security aspects.

From a security point of view, data must be protected against external and internal attacks and undesirable events (such as technical failures). Often, one speaks of protecting data at rest, in transit, and in use. Whether a residual risk is acceptable is decided relative to the organization of the controller. This perspective is not applicable to data protection, even if the wording "protecting the data against attacks" could be understood to imply this.

While data protection also looks at protection against attacks and undesirable events, i.e. security[23], this aspect covers only one[24] of six[25] principles of data protection (see "Integrity and confidentiality" in Part II section "Principles" of these Guidelines). In other words, IT security is a prerequisite for compliant processing but falls far short of full compliance.

When looking beyond security, the main risks to the rights and freedoms of natural persons originate in the processing **as planned**, i.e. even in absence of undesirable events and attacks. Data protection mandates that the negative impacts of processing for affected persons be minimized. A DPIA thus has to demonstrate this by justifying that all operations of processing are indeed **necessary and proportional in relation to the purposes**. This is evidently very different from a security assessment: a processing activity may be highly secure against incidents and attacks, and yet comprise unacceptable risks to the rights and freedoms of individuals.

In security, mitigation measures are mostly technical and prevent attacks or mitigate the effect of undesirable events on the assets of the controller. In data protection, in contrast, organizational measures are equally important and the measures minimize the negative impact on affected persons. Examples for organizational measures include training and awareness campaigns for employees, non-disclosure-agreements, and specific contractual clauses for computing outsourced to processors.

---

[20] Article 24(1) GDPR states that "...the controller shall implement appropriate **technical and organizational measures** to **ensure and** to be able to **demonstrate** that processing is performed **in accordance with this Regulation**." (Highlighting added by the authors).

[21] Recital 82 GDPR states that "**In order to demonstrate compliance** with this Regulation, the controller or processor should **maintain records of processing activities** under its responsibility." (Highlighting added by the authors).

[22] Article 30(1)(g) states that the records of processing activities shall contain, "where possible, a general description of the technical and organizational **security** measures referred to in Article 32(1)". (Highlighting added by authors).

[23] In particular, Article 32 GDPR "Security of processing" is concerned with security.

[24] See Article 5(1)(f) GDPR which lists security as one of the six principles of data protection.

[25] The six principles of data protection are listed in Article 5(1)(a) through (f) GDPR.

In security, the risk of violating the rights and freedoms of only a few persons may have only insignificant effect on an organization's assets and thus be acceptable to a controller. In data protection, the focus is on the affected persons and no matter if only few are affected, the risk may by no means be acceptable to them[26].

While in security, measures are designed to defend against attacks and events, in data protection they minimize the negative impact on the affected persons. This is for example evident in the limitation of the storage period which temporarily limits the possible impact. Similarly, pseudonymization prevents easy identification of data subjects and thus lowers the data subjects' risk. Other measures aim at creating transparency such that data subject are not helplessly subjected to the decisions of controllers, but have the possibility to protect their rights should their rights and freedoms be excessively or illegitimately be infringed. Measures that implement data subject rights then render it possible for data subjects to intervene to protect their rights. These examples of data protection measures illustrate the largely different character compared to measures for security.

5.3.5 Who is responsible for carrying out a DPIA?

"The controller is responsible for ensuring that the DPIA is carried out (Article 35(2)). Carrying out the DPIA may be done by someone else, inside or outside the organization, but the controller remains ultimately accountable for that task."[27] Note that the DPO has to be consulted for a DPIA in an advisory role, but is never responsible.

5.3.6 Who should be involved in carrying out a DPIA?

The following first provides a legal answer rooted in the GDPR and then provides additional guidance on who may have to be involved in the process of an impact assessment.

From a legal point of view, the Article 29 Working Party gives the following authoritative advice:

- "The controller **must** also seek the advice of **the Data Protection Officer** (DPO), where designated (Article 35(2)) and this advice, and the decisions taken by the controller, should be documented within the DPIA. The DPO should also monitor the performance of the DPIA (Article 39(1)(c))."[28]
- "If the processing is wholly or partly performed by a **data processor**, the processor **should** assist the controller in carrying out the DPIA and provide any necessary information (in line with Article 28(3)(f))."[29]

---

[26] The Article 29 Working Party states: "Note: the DPIA under the GDPR is a tool for managing risks to the rights of the data subjects, and thus takes their perspective, as is the case in certain fields (e.g. societal security). Conversely, risk management in other fields (e.g. information security) is focused on the organization.", wp248rev.01, page 17, Section III.D.c), 3rd paragraph.
[27] wp248rev.01, page 14, Section III.D.b), 1st paragraph
[28] wp248rev.01, page 15, Section III.D.b), 1st paragraph, Highlighting by authors.
[29] wp248rev.01, page 15, Section III.D.b), 2nd paragraph, Highlighting by authors.

- "The controller **must** 'seek the views of data subjects or their representatives' (Article 35(9)), 'where appropriate'. "[30] This can take a variety of forms depending on context, including generic studies, involvement of representatives (such as consumer organizations), and surveys. Consent is not a valid form.

Beyond these legally required involvements, the Article 29 Working Party recommends to cover all relevant disciplines (expertise) and responsibilities (decisions)[31]. This can lead to the involvement of both, internal staff and external experts. This may for example include the following:

- The **business unit** that uses the application, instructs affected employees, makes decisions on storage periods, access control, etc.
- The **IT department** that installs and operates the application and certain technical mitigation measures (as for example firewalls or backup systems).
- The **human resource department** who may organize awareness campaigns and training, as well as manage non-disclosure agreements with employees.
- The **legal department** who drafts specific contractual clauses to pass on obligations to processors.
- The **software house** that that provides the application and may offer (security) updates, maintenance, and evolution.

As explicitly stated by the Article 29 Working Party for DPOs, it is recommended to document the interactions with the involved parties, the advice provided, and the decisions made in the DPIA. This is an important aspect of demonstrating compliance according to Article 5(2) GDPR.

5.3.7 In what cases must I carry out a DPIA? Are there lists of processing activities that require a DPIA?

The Article 29 Working Party has provided the most universally applicable guidance for this question[32]. On this basis, many supervisory authorities have issued more specific guidance in their national language, focusing on their national concerns.

The guidance provides a **procedure** for establishing whether a processing activity is "likely to result in a high risk for the rights and freedoms of natural persons", i.e., **whether a DPIA is required**. It consists of **nine criteria** about the processing activity. For each criterion, the controller has to decide (and document) whether it is relevant for the processing activity at hand. The working party's guidance includes examples that illustrate this.

In particular, the nine criteria pertain to the following:

1. Evaluation or scoring;

---

[30] wp248rev.01, page 15, Section III.D.b), 3rd paragraph, Highlighting by authors, quotation marks changed for better readability.
[31] wp248rev.01, page 15, Section III.D.b), second half of page.
[32] See wp248rev.01, Section III.B., pages 8-13. Download link is contained in Footnote 10.

2. Automated decision-making with legal or similar significant effect;
3. Systematic monitoring;
4. Sensitive data or data of a highly personal nature;
5. Data processed on a large scale;
6. Matching or combining datasets;
7. Data concerning vulnerable data subjects;
8. Innovative use or applying new technological or organizational solutions;
9. Prevents data subjects from exercising a right or using a service or a contract;

Based on the assessment of these criteria, the decision is made whether the processing likely results in a high risk: "In most cases, a data controller can consider that **a processing meeting two criteria would require a DPIA** to be carried out."[33] This is only indicative, however, and a controller may decide that:

- a processing meeting only one of these criteria requires a DPIA;[34]
- a processing meeting (at least) two criteria is still not likely to result in a high risk[35].

In the latter case the controller has to **justify** this decision. In any case, to demonstrate compliance (Article 5(2) GDPR), the procedure to determine whether a DPIA is needed **should be documented**.

As additional guidance, (national) supervisory authorities must publish a list of the kind of processing operations which require a DPIA (Article 35(4) GDPR) and may also publish a list of operations where a DPIA is not necessary (Article 35(5) GDPR). These lists are presented to the EDPB, and published at the EU level[36]; in practice these publications can act as an accessible repository of national level DPIA requirements and expectations.

We advise to follow either the national procedure or that provided by the Article 29 Working Party and document it even if it shows that a DPIA is not necessary.

5.3.8 At what point in time does the DPIA need to be carried out/updated?

In any case, if high risk is likely, a DPIA has to be carried out **prior to processing** (Article 35(1) GDPR). This constitutes a safeguard that ensures that processing involving a high risk cannot happen, unless the risks have been identified and sufficiently mitigated.

As stated above (see *What is a DPIA* above), a **DPIA is a continuous process** that provides guidance to the design and implementation of a processing activity. To successfully guide decisions and guarantee compliance with the GDPR, it is evident that

[33] wp248rev.01, Section III.B., page 11, 2nd paragraph, highlighting added by authors.
[34] wp248rev.01, Section III.B., page 11, 3rd paragraph.
[35] wp248rev.01, Section III.B., page 12, 2nd paragraph
[36] See https://edpb.europa.eu/our-work-tools/our-documents/topic/data-protection-impact-assessment-dpia_en

"[t]he DPIA should be **started as early as is practicable in the design of the processing operation** even if some of the processing operations are still unknown. **Updating the DPIA throughout the lifecycle** [of the] project will ensure that data protection and privacy are considered and will encourage the creation of solutions which promote compliance."[37] This approach is evidently required by the obligation of **data protection by design** (Article 25(1) GDPR).

The process of a DPIA is also not completed, once the processing has started. Rather, "[w]here necessary, the controller shall carry out a **review** to assess if processing is performed in accordance with the [DPIA] at least when there is a **change of the risk** represented by processing operations." (Article 35(11) GDPR). There are several factors that may change the risk, including the following:

- The processing activity changes,
- the efficiency of the mitigation measures changes.

In the former case, a change could be caused by a change in the intended usage of the data (new purposes of processing), changes in the scope of data collection and processing, changes in the number of affected person (e.g., due to the success of the activity), a change in the application software (e.g., a new version with additional functionality), a change in the technical infrastructure (e.g., a migration into the cloud), or a change in the legal situation (e.g., a court decision that affects the interpretation of the GDPR).

In the latter case, a change could be caused by the discovery of new vulnerabilities in the mitigation measures (e.g., software vulnerabilities), an increase in threats and capability of attackers (e.g., new methods to re-identify pseudonymous or anonymous data), or an organizational change that threatens the effectiveness of measures (e.g., new staff who is unaware of what can be disclosed).

5.3.9 Is there a standardized method for carrying out a DPIA? Are there outlines, templates or tools in support of carrying out a DPIA?

With DPIAs being a relatively new instrument introduced at the EU level with the GDPR, there is still ample discussion of how exactly a DPIA should be carried out and there exists several different schools of thought. Some national supervisory authorities have issued guidance on the topic, or even specific tools and templates. While a DPIA is primarily evaluated by the competent (i.e., typically national) supervisory authority, the guidance provided here cannot go in the merit of what is available in all member states. Instead, guidance is provided based on the opinion of the Article 29 Data Protection Working Party on the DPIA (wp248rev.01)[38] that has been formally adopted[39] by the

[37] wp248rev.01, page 14, Section III.D.a), 2nd paragraph, highlighting and text in brackets added by authors.

[38] wp248rev.01, ARTICLE 29 DATA PROTECTION 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, Adopted on 4 April 2017, As last Revised and Adopted on 4 October 2017, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236 (last visited 14/01/2020).

European Data Protection Board[40]. According to Article 70(1) GDPR, "The Board shall ensure the consistent application of this Regulation" and is therefore the best source for advice at European level.

The Figure to illustrate the iterative process for carrying out a DPIA that is provided by the Working Party has already been shown in the Figure above (section 5.3.1). It is a cycle containing the following steps:

1) Description of the envisaged processing.
2) Assessment of the necessity and proportionality.
3) Measures already envisaged.
4) Assessment of the risks to the rights and freedoms [of natural persons].
5) Measures envisaged to address the risks.
6) Documentation.
7) Monitoring and review.

The Working Party explains that there is **flexibility** in how a DPIA is structured:

"The GDPR provides data controllers with **flexibility to determine the precise structure and form of the DPIA** in order to allow for this to fit with existing working practices. There are a number of different established processes within the EU and worldwide which take account of the components described in recital 90. However, **whatever its form**, a **DPIA must be a genuine assessment of risks, allowing controllers to take measures to address them**."[41]

The Working Party gives examples of currently known approaches in their Annex I[42]. These include both, **generic national** and **sector-specific** DPIA "frameworks". "The [**Working Party**] **encourages** the development of **sector-specific DPIA frameworks**."[43]

Controllers are thus free to choose the most suitable structure and format for a DPIA, **as long as certain requirements are fulfilled**: "It is up to the data controller to choose a methodology, but this methodology should be compliant with the **criteria provided in Annex 2**."[44] The Working Party "proposes [these] criteria which data controllers can use to assess whether or not a DPIA, or a methodology to carry out a DPIA, is sufficiently comprehensive to comply with the GDPR"[45].

Usually, the different methodologies come with outlines, templates, and/or tools.

---

[39] Endorsement of GDPR WP29 guidelines by the EDPB, https://edpb.europa.eu/news/news/2018/endorsement-gdpr-wp29-guidelines-edpb_en, Brussels, 25 May 2018, Bullet point 6.
[40] https://edpb.europa.eu/
[41] wp248rev.01, page 17, Section III.D.c), 4th paragraph, Highlighting by authors.
[42] Annex I of wp248rev.01, page 21.
[43] wp248rev.01, page 17, Section III.D.c), 6th paragraph, Highlighting by authors.
[44] wp248rev.01, page 17, Section III.D.c), 6th paragraph, Highlighting by authors.
[45] wp248rev.01, page 22, Annex II, 1st paragraph.

The remainder of this section therefore concentrates on these **criteria for an acceptable DPIA** provided by the Working Party.

The criteria mostly reflect the structure and content of Article 35(7) but provide additional detail and interpretation. The following reports the content with some rewording and minor restructuring for clarity[46]:

1. **Systematic description of the processing** *(Article 35(7)(a) GDPR)*
2. **Assessment of necessity and proportionality** *(Article 35(7)(b) and (d) GDPR)*
3. **Management of the risks** to the rights and freedoms of data subjects *(Article 35(7)(c) and (d) GDPR)*
4. **Involvement of interested parties** (*Articles 35(2) and 35(9) GDPR)*

Each of these is discussed in more detail in subsections in the following.

Can I follow the standard approach by ISO?

ISO has issued the international standard **ISO/IEC 29134:2017 "Information technology — Security techniques — Guidelines for privacy impact assessment.**" As usual for ISO standards, the text of the standard is not available publicly but only for paying customers. ISO standards are global in nature and thus cater to a variety concepts of "privacy". It is unlikely that the standard adopts a legal view and impossible that a single standard satisfies the necessarily different legal requirements from different legislations. Should the ISO approach be suitable for a given controller, it is therefore advised that in addition, legal guidance specific to the GDPR is consulted in parallel.

Of general relevance for all these subsections is the second sentence of Recital 90 GDPR. It is reported here with highlighting and structure (bullets) added by the authors:

"That **impact** assessment should include, in particular, the **measures, safeguards** and **mechanisms** envisaged for:

- mitigating that **risk**,
- ensuring the **protection of personal data** and
- **demonstrating compliance** with this Regulation."

In other words:

- The **focus** of the DPIA is on **measures, safeguards,** and **mechanism**.
- These are applied to:

[46] The criteria are provided in a wording is that of evaluation criterion. In this document, the wording is changed to titles that reflect the structure. For example, "a systematic description of the processing is provided" is changed to "systematic description of the processing". Also, the single top-level entry corresponding to both, Article 35(7)(c) and (d) is split into two separate entry.

- **risks**,
- protection of personal data, in other words **compliance** with the GDPR, and
- **demonstration of compliance**.

What is important to notice is that a DPIA is not only focused on identifying, assessing, and mitigating risks, but also with compliance and demonstration of compliance. The latter is particularly evident in letter (b) of Article 35(7) and the according subsection "2. Assessment of necessity and proportionality" that is described below.

5.3.9.1 Systematic description of the processing

Providing further detail to Article 35(7)(a) GDPR, the Working Party breaks down the description of the processing involved into the following elements[47]:

- **Nature**, **scope**, **context** and **purposes** of the processing *(Recital 90 GDPR)*;
- **personal data**, **recipients** and **storage period**;
- **functional description** of the processing operation;
- **technical** and **human resources** employed in the processing (hardware, software, networks, people, paper or paper transmission channels);
- compliance with approved **codes of conduct** *(Article 35(8) GDPR)*.

Important to note regarding the first bullet is that Article 35(7)(a) reads "**purposes** of the processing, including, where applicable, the **legitimate interest pursued by the controller**"

While most of the concepts listed here are likely well understood, the exact meaning of *(i) nature*, *(ii) scope*, and *(iii) context* may be more elusive. Since there is no authoritative interpretation of these terms, the following provides one possible interpretation in the hope it proves helpful.

(i) **Nature**: There may be multiple aspects related to the **nature** of processing, including the following:

- The **processing paradigm**;
- the **infrastructure paradigm**;
- **level of automation**;
- **form of "effect"**;
- the **level of innovation**.

Processing paradigms can range from imperative (i.e., "traditional" applications), over rule-based/declarative (e.g., expert systems), to machine-learning-based artificial intelligence.

[47] Adapted from wp248rev.01, page 22, Annex II.

The ***infrastructure paradigm*** can range from a desktop application over a client-server application, to a cloud-based solution, all showing different levels of distribution.

The ***level of automation*** can range from providing supports to human actors to fully automatic operation without any possibility of human intervention.

The ***form of "effect"*** describes the "output" of the processing. This may range from pure information (in information systems), over the creation of a status (e.g., right to vote) that determines the possible actions of a person, over the management of virtual assets of a person (e.g., a bank account), to cyber-physical systems that directly affect the physical world in which the person lives or the person herself.

The ***level of innovation*** can range from staying within realism where risks and their mitigation are well-understood, to deploying new technologies and methods whose consequences have yet to be found out and that may come with yet unknown side-effects and risks.

(ii) **Scope**: What is inside and outside of the **scope** of the processing activity determines its impact. In data protection, the scope has to be considered relative to the affected persons. This encompasses multiple aspects, including the following:

- Which and how many persons are affected?
- Which aspects of life of these persons are affected?
    - For what duration and with what frequency are these aspects captured?
    - With what precision are these aspects captured?

Which and how many persons are affected evidently determine the impact of the processing activity. Which kind of persons is affected is interesting in regard of whether some of these are **vulnerable** and require special kinds of protection. Apart from the **absolute number** of persons, **relative numbers** pertaining to geographic areas or groups of users.

The ***affected aspects of life*** are closely related to the involved categories of data. Evidently, different aspects of life come with different levels of sensitivity and thus risk. In the GDPR, the **special categories of data** (Article 9) together with data about criminal convictions (Article 10) are identified as particularly sensitive. The impact of the data processing does not only depend on the kinds of aspects are in the scope of the processing, but also what **range of aspects** of an individual are addressed. An isolated aspect usually has a much smaller impact than the processing of a profile that provides a complete picture of a person's life.

The ***temporal scope***, most prominently the **duration** over which these aspects are captured, also determines the impact. This is closely related to storage periods and erasure of data. When a certain type of data is collected more than just once, the **frequency** is also important. This is most evident when considering location data, where a tracking once every few days is largely different from a tracking every few minutes.

The ***precision*** with which aspects of a person's life are captured also determines the impact of the processing activity. This is for example evident when looking at location where knowing the country where a person is located has much less impact than knowing the precise coordinates. Similarly, knowing that a person is of age has much less impact than knowing the date of birth.

(iii) **Context**: Understanding a processing activity and its risks is often impossible without knowing its **context**. Different aspects of context can, among others, be:

- Legal;
- Technical
- Economical;
- Societal.

Part of the ***legal*** context is the **legal basis** for processing according to Article 6 GDPR and possibly Article 9 GDPR. Also relevant here are possible **certifications** according to Article 42 GDPR, approved **Codes of Conduct** according to Article 40 GDPR (see Article 35(8)) and **Binding Corporate Rules** according to Article 47 GDPR. The legal context may also include authoritative **opinions by the European Data Protection Board** according to Article 64 GDPR or court decisions that are relevant to the assessment of impact. Note that the Working Party has listed the codes of conduct in a separate element, likely since it is explicitly required in Article 35(8) GDPR.

There are two aspects that contribute to the ***technical*** context:

- **Other processing activities** by the same or by different controllers that interact with the processing activity, and
- **The state of the art of technology** to defend and attack.

In some cases, it is impossible to assess a processing activity in isolation. This is typically the case with **distributed systems** where different controllers operate different components. A good example is federated identity management where an *identity provider* operates a component that can only be understood when also considering *users* and *relying parties*. Here and in many cases, privacy is often determined by the communication protocols used between components and thus processing activities. This is illustrated by the existence of specifically designed privacy enhancing protocols[48]. If one were to assess the impact without considering the context, these particularly relevant protocols would fall into the gaps between controllers and thus DPIAs.

It is self-evident that the **state of the art of technology** has to be considered to understand the impact of processing. Accordingly, the GDPR mandates to take into account the state of the art in both, Article 32 on the security of processing, and Article 25 on data protection by design and by default (see "Data Protection by Design and by

[48] This is illustrated by the cryptographic technique of p+rivate set intersection (see https://en.wikipedia.org/wiki/Private_set_intersection).

Default" in Part II of these Guidelines, section "Main Concepts"). In security (that is one aspect of data protection), to understand risks, it is crucial to understand the current threat landscape that describes the ease of attack and the availability and efficiency of defensive measures. To minimize the impact of processing on data subjects according to data protection by design, it is crucial to know the available technical possibilities.

The ***societal*** context describes the influence that persons and organizations potentially have on the processing activities. This includes the question of who might be interested in using the processed data for other purposes. This includes aspects of how motivated and resourceful[49] potential players are to do so. It is important to note that the context is not limited to external players but also includes internal staff that might have motive to use data for other purposes.

5.3.9.2 Assessment of necessity and proportionality

Providing further detail to Article 35(7)(b) GDPR, the Working Party breaks down the assessment of necessity and proportionality into several sub-points in two major groups[50]. It is important to note that all these points are concerned with **measures** envisaged **to comply with the GDPR**.[51] For easier understanding, these points are classified here as follows:

Points relating to:

(i) Generic obligations from Chapter 2 GDPR "**Principles**" (see "Main Principles" in Part II of these Guidelines)

(ii) Specific obligations from Chapter 3 GDPR "**Rights of the data subject**" (see "Data Subject Rights" in Part II of these Guidelines)

(iii) Specific obligations from Chapter 4 GDPR "**Controller and processor**"

(iv) Specific obligations from Chapter 5 GDPR "**Transfers of personal data to third countries or international organizations**" (see "Transfers of data to third countries" in Part II section "Main Tools and Actions")

These are described in the following in more detail:

(i) ***Principles***:

The points provided by the Article 29 Working Party in this section closely correspond to the generic principles (a) through (f) of data protection provided in Article 5(1) GDPR with the following differenced:

- The more concrete Article 6 is used instead to cover lawfulness, instead of 5(1)(a) itself.
- Article 5(1)(d) on "accuracy" is omitted, likely since the data subject right to rectification covers the same aspects in a more concrete manner.

[49] Resourceful here includes technical capability and economical capacity, as well as the availability of additional information accessible to a player.
[50] Adapted from wp248rev.01, page 22, Annex II.
[51] See wp248rev.01, page 22, Annex 2, 1st bullet point under "necessity and proportionality are assessed".

- Article 5(1)(f) on security ('integrity and confidentiality') is omitted, likely since it is covered later in "management of the risks to the rights and freedoms of data subjects"

The DPIA is now required for each principle (see "Main Principles" in Part II of these Guidelines). , what **measures** were taken to comply with it. In the following, an incomplete selection of examples for such measures is given:

Measures to demonstrate compliance with "**purpose limitation**" described in Article **5(1)(b)** consist of **specifying** the **explicit purposes** of processing. This description has to be precise and concrete. To demonstrate compliance, it should be **justified** why these purposes are **legitimate** and that the impact on data subjects has been minimized by keeping the purposes **as narrow as necessary**.

An additional important aspect of Article 5(1)(b) is that data shall "not [be] further processed in a manner that is incompatible with those purposes". Since **disclosure** is considered to be processing (see Article 4(2) GDPR), this means that personal data shall only be disclosed to persons and parties **as necessary for and justified by the stated purposes**. Measures that show compliance with this requirement include the documentation of who (employees of the controller and third-party recipients) needs access to the data and processing and how access rights are managed and updated in practice. This complements the measures to mitigate threats of illegitimate access that are part of the section "management of risks" that is described further down.

Measures to guarantee the **lawfulness** of processing consist of **documentation** of the chosen **legal basis** according to Articles 6(1) and possibly 9(2) GDPR.

Where Article **6(1)(a)** "**consent**" is used as a legal basis, the documentation should include how this consent was collected (e.g., a form or a dialog) together with a **justification** how the **requirement** for consent given in **Articles 7 and 8** GDPR are fulfilled. In the case where Article **9(2)(a)** "**explicit consent**" is chosen, a justification how the requirements for this special form of consent are met should be added. The best support for this is provided by the Article 29 Working Party in their "Guidelines on Consent"[52].

Where Article **6(1)(f)** "**legitimate interests** pursued by the controller or by a third party" is chosen, it is very important to note that the legal basis states "**except where** such interests are **overridden by the interests or fundamental rights and freedoms of the data subject** which require protection of personal data, in particular where the data subject is a child." To be sure that the interests of data subject do not override the legitimate interest of the controller, an additional "**balancing test**" (see "Legitimate interest and balancing test" in part II, section "Main Tools and Actions") is required. What such a balancing test is and how to conduct it was described by the Article 29 Working Party in their Opinion WP217[53].

[52] wp259rev.01, ARTICLE 29 DATA PROTECTION WORKING PARTY, Guidelines on Consent under Regulation 2016/679, Adopted on 28 November 2017, As last Revised and Adopted on 10 April 2018, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051 (last visited 29/01/2020)

[53] wp217, ARTICLE 29 DATA PROTECTION WORKING PARTY, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, Adopted on 9 April 2014, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf

Measures to demonstrate compliance with Article 5(1)(c) "**data minimization**" are **justifications** that the collected and processed **personal data** is **adequate**, **relevant** and **limited to what is necessary** to reach the **stated purposes** (see "Data minimization" in Part II section "Principles" of these Guidelines). .

Measures to demonstrate compliance with Article 5(1)(e) "**storage limitation**" (see "Storage limitation" in Part II, section "Principles") consist of documentation that **justifies** that the data is **stored only as long as necessary for the purposes** (and then erased) and that **pseudonymization** and **anonymization** that reduce/eliminate the identifiability of data subjects is **applied as soon as possible** for the purposes (see "Identification", "Pseudonymization" and "Anonymization" within Part II of these Guidelines, section "Main Concepts").

While not explicitly included among the point by the Working Party, a desirable additional measure would be the documentation of **persons** and recipients **to whom the data** are legitimately **disclosed**.

(ii) ***Rights of the data subject***: (see section "Data subject Rights" within Part II)

The points provided by the Article 29 Working Party in this section take up almost the complete set of articles of Chapter 3 "Rights of the data subject". This includes Articles 12-14 GDPR that are mostly concerned with transparency, as well as Articles 15 through 21 which are concerned with specific data subject rights.

Measures to demonstrate compliance with the obligations pertaining to Chapter 3 consist of a documentation of the information that is provided to data subjects and the technical or organizational means available to data subjects to exercise these rights.

Somewhat surprisingly, the Working Party did not include Article 22 GDPR among their points, although "automated individual decision-making, including profiling" obviously bears high risks for data subjects. It is therefore recommended to address the compliance with this article anyhow, if applicable. A suitable measure could be to document how data subject can access the "right to obtain human intervention" that is mentioned in Article 22(3).

(iii) ***Obligations of the controller and processor***:

The points provided by the Article 29 Working Party in this section consist solely of two Articles out of Chapter 4 GDPR "**Controller and processor**", namely Articles 28 and 36.

Article 28 is concerned **processors**. Measures that demonstrate compliance with this article include for example[54] the following:

- Documentation of the **guarantees provided by the processor** "to implement appropriate technical and organizational measures in such a manner that

(last visited 29/01/2020). Note that while this opinion refers to the Data Protection Directive rather than the GDPR, the concepts and methods should equally apply.

[54] The list of examples is not meant to be exhaustive.

processing will meet the requirements of this Regulation" (Article 28(1) GDPR).

- Measures (such as contractual clauses) that **guarantee** that "**processor [do] not engage another processor without prior** specific or general written **authorization** of the controller." (Article 28(2) GDPR).
- Documentation of a "**contract or other legal act**" that governs the processing by the processors. This includes **clauses** that guarantee the **requirements** laid out in Article **28(3)(a) through (h)**.

Article 36 is concerned with "**prior consultation**" of the competent supervisory authority if the residual risk after implementing suitable mitigation measures is still high. The measure to demonstrate compliance with this Article is to document such consultation and its outcome.

Beyond the two Articles of Chapter 3 GDPR that were explicitly listed among the points by the Working Party, additional measures are both possible and desirable. Some examples are the following:

- Measures to demonstrate compliance with Article 25 "**data protection by design and by default**" can include documentation how data protection was integrated already in the conception and design of the processing activity. This can for example consist in data protection requirements that were stated for a custom development or tender, or an analysis of data protection compliance during a selection process (see "Data Protection by Design and by Default" in Part II, section "Main Concepts" of these Guidelines).
- Measures to demonstrate compliance with Articles 33 and 34 on notification and communication pertaining to **data breaches** could consist in the documentation of internal procedures to handles such situations.

(iv) ***Transfers of personal data to third countries or international organizations***:

In this section, the Article 29 Working Party provides a single point that refers to the whole Chapter 5 of the GDPR. Measures to demonstrate compliance in this section document safeguards in place that protect data subjects in the situation where their data is transferred to areas where the GDPR is not directly enforceable. Among the concrete measures are the documentation that there is an adequacy decision by the Commission in place (Article 45 GDPR), the adherence to legally binding corporate rules (Article 47 GDPR), or the use of other legally binding and enforceable instrument (Article 46 GDPR) (see "Transfers of data to third countries" in Part II, section "Main Tools and Actions" of these Guidelines)

5.3.9.3 Management of the risks to the rights and freedoms of data subjects

Article 35(7)(c) mandates the "assessment of the risks to the rights and freedoms of data subjects". Recital 84 further states that the controller carrying out a DPIA should "evaluate, in particular, the origin, nature, particularity and severity of that risk". On this basis, the Article 29 Working Party stresses that such assessment needs to be made from the perspective of the data subject and provides the following approach:

- A list of risks that need to be assessed and
- a series of steps that constitute such an assessment

A DPIA must thus address these steps for each of the risks.

The Working party lists the following risks:

1. illegitimate access [to personal data],
2. undesired modification [of personal data], and
3. disappearance of data.

Evidently, these risks paraphrase the wording of Article 5(1)(f) on the principle of "integrity and confidentiality". It is also consistent with "confidentiality, integrity, availability and resilience of processing systems and services" that is stated in Article 32(1)(b) GDPR. It is also possible to see a direct equivalence to the protection goals used in IT security, namely *confidentiality*, *integrity*, and *availability*.

For the assessment of each risk, the Working Party states the following components:

1. identification of risk sources (in accordance with Recital 90)
2. identify potential impacts of each risk to the rights and freedoms of natural persons
3. identify threats that could lead to these risks
4. estimate the likelihood and severity of the risks (in accordance with Recital 90).

On this basis, considering the estimated likelihood and severity of each risk, appropriate mitigation measures have to be conceived, implemented, and documented in the DPIA (as mandated by Article 35(7)(d) and Recital 90).

Since the principles of "integrity and confidentiality" (see "Integrity and confidentiality" in Part II, section "Principles" of these Guidelines). as well as the listed threats are typical for IT security, the measures documented here are well known from that discipline. The major difference to security is the estimation of severity or impacts that are evaluated relative to the affected persons rather than the organization responsible for the processing. The fact that only this section is concerned with IT security further illustrates the difference that was already addressed above.

5.3.9.4 Involvement of interested parties

According to Article 35(2), "[t]he controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment."

Also, according to Article 35(9), "[w]here appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations."

This section of the DPIA documents that these two requirements were indeed met by the controller. When views of the data subjects or representatives were sought, the documentation should justify why these views should be considered as reasonably

representative of the data subjects concerned. When views were not sought, the documentation should clarify why this was not useful or possible.

5.3.10 What can facilitate carrying out a DPIA?

The following list some ways that could potentially facilitate carrying out a DPIA.

- In some cases where the processing has a **legal basis based in Union or Member State law** (i.e., Article 6(1)(c) or (e) GDPR), a DPIA may have already been carried out by the legislator. In this case, unless a Member State deems a DPIA by every controller necessary, or unless the legislation leaves significant margin of implementation to the controller in a way that affects the risks to data subjects, the **DPIA does not have to be executed** (see Article 35(10) GDPR for detail).
    - An example can be found in the Austrian "Research Organization" legislation[55] that already provides DPIAs[56] for its Articles.
- "There are circumstances under which it may be reasonable and economical for the subject of a data protection impact assessment to be **broader than a single project**" (Recital 90 GDPR). This obviously facilitates the single processing activities that can then refer to the "broad DPIA". This is further confirmed in Article 35(1) that states: "A single assessment may address a set of similar processing operations that present similar high risks." The Article 29 Working Party provides additional guidance[57] here stating that "[a] single DPIA could be used to assess multiple processing operations that are **similar in terms of nature, scope, context, purpose, and risks**." It further states that "**DPIAs aim at systematically studying new situations** that could lead to high risks on the rights and freedoms of natural persons, and **there is no need to carry out a DPIA in cases** (i.e. processing operations performed in a specific context and for a specific purpose) **that have already been studied**." In these cases, it is possible to fall back on the "broad DPIA" or at least delegate major portions of an individual DPIA to it. If a "broad DPIA" is unavailable, there may still be individual DPIAs of similar processing activities that help conducting one oneself.
- The Working Party states that "A DPIA can also be useful for **assessing the data protection impact of a technology product**"[58]. So if a technology provider has already conducted a DPIA, "the data controller deploying the product remains obliged to carry out its own DPIA with regard to the specific

[55] see Bundesgesetz über allgemeine Angelegenheiten gemäß Art. 89 DSGVO und die Forschungsorganisation (Forschungsorganisationsgesetz – FOG)
StF: BGBl. Nr. 341/1981 idF BGBl. Nr. 448/1981 (DFB) (NR: GP XV RV 214 AB 778 S. 81. BR: S. 413.), in German, https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10009514 (last visited 30/01/2020).
[56] See Appendices 4 through 21.
[57] wp248rev.01, page 7, Section III. A., 2nd paragraph, highlighting added by authors.
[58] wp248rev.01, page 8, Section III. A., 2nd paragraph.

implementation, but this can be informed by a DPIA prepared by the product provider."

- The Working Party points out the possibility that a DPIA is facilitated by the existence of a **sector-specific DPIA framework**: "The WP29 encourages the development of sector-specific DPIA frameworks. This is because they can draw on specific sectorial knowledge, meaning the DPIA can address the specifics of a particular type of processing operation (e.g.: particular types of data, corporate assets, potential impacts, threats, measures)."[59]
- Another potential way of facilitating a DPIA is to exploit **systematic approaches** that are used across multiple processing activities. Article 24(2) provides the example of corporate-wide "**data protection policies**". Article 24(3) adds "**approved certification**" (according to Article 42 GDPR) and "**approved codes of conduct**" (according to Article 40 GDPR). The latter is also specifically mentioned in Article 35(8) GDPR.

5.3.11 What happens if I do not carry it out? What are the possible consequences?

"Under the GDPR, non-compliance with DPIA requirements can lead to fines imposed by the competent supervisory authority. Failure to carry out a DPIA when the processing is subject to a DPIA (Article 35(1) and (3)-(4)), carrying out a DPIA in an incorrect way (Article 35(2) and (7) to (9)), or failing to consult the competent supervisory authority where required (Article 36(3)(e)), can result in an administrative fine of up to 10M€, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher."[60]

5.4 Data Management Plan

Tom Lindemann (EUREC)

This part of The Guidelines has been reviewed and validated by Marko Sijan, Senior Advisor Specialist, (HR DPA)

5.4.1 What is a data management plan?

A data management plan (DMP) is a key element of good data management and shows a proactive commitment to scientific integrity.

A DMP covers the entire management lifecycle of all data collected, generated or processed by a research project. Usually, a DMP provides information on:

[59] wp248rev.01, page 17, Section III. D.c)., 2nd last paragraph.
[60] wp248rev.01, page 4, Section I, 3rd paragraph.

- the handling of research data during and after a project, including measures to ensure confidentiality, if applicable;
- which data will be collected, generated and processed;
- which methodology and standards will be applied;
- whether data will be shared;
- how data will be curated and preserved, including after the project;
- ethics and intellectual property concerns.

In other words, a DMP focuses on the collection, organization, use, storage, contextualization, preservation and sharing of data. More precisely, a DMP outlines which resources are allocated to data management; it identifies and assigns responsibility to data controllers and processors; and it sets procedures for protecting, safeguarding and sharing data. Hence, a DMP assigns responsibilities, allocates resources, ensures adequate data protection and safeguarding, and specifies mechanisms for sharing research data.

With regard to opening up research and sharing research data, the FAIR principles[61] serve as particularly important guidelines. The FAIR principles apply to research data (i.e. the data upon which scientific reasoning processes are based/the evidence supporting claims) and describe how research projects can ensure that research data are as open as possible and as closed as necessary.

The latter provision is particularly important with regard to personal data. Data protection requirements supersede the FAIR principles and invalidate them if research data are personal data. In Europe, data protection requirements are derived from the GDPR, relevant national and international legislation, and institutional guidelines. Importantly, the GDPR contains research exemptions which facilitate using and storing data for research purposes. If personal data are anonymized they can be shared, since anonymous data are information which does not relate to an identified or identifiable natural person, and therefore GDPR does not concern the processing of such anonymous information, including for statistical or research purposes (See "Identification, pseudonymization and anonymization" in Part II, section "Concepts" of these Guidelines). Because the relationship between open science and data protection requires clarification in the current regulatory landscape, researchers should pay close attention to ongoing developments.[62]

Over the course of a project, the DMP should be reviewed periodically and updated whenever changes arise, for example due to new data or the addition of further data controllers or processors. Keeping information up to date ensures that the DMP continues to facilitate good scientific practice during the whole project.

[61] According to the FAIR principles research data should be findable, accessible, interoperable and reusable. They are described in an article by Wilkinson et al. that can be accessed here.

[62] This can, for instance, be done by checking the European Data Protection Supervisor's or the European Data Protection Board's website for hints or an opinion on "data protection and scientific research".

5.4.2 Why should I write a DMP?

Although research projects are not legally obliged to adopt DMPs, they should do so for at least three reasons:

- DMPs help researchers to comply with data protection legislation and to follow best practices in opening up research data. In this way, they provide guidance, reduce uncertainty and increase transparency.
- Research funding organizations increasingly make funding conditional on the sharing of research data, in order to support reliable, transparent and cumulative research.
- The guidelines of many research institutions encourage researchers to write DMPs.

5.4.3 Am I legally obliged to have a data management plan?

Although writing a **DMP is not currently a legal requirement** in the European research context, it has become a core element of good scientific practice. Many research funding organizations expect grant recipients to develop a DMP in order to promote sound data management. One reason is that data management is becoming increasingly complex, as ever more data can be processed and the number of multi-centre projects continues to rise. As a result, research projects involving data processing should have a DMP that governs data processing of the whole project. Therefore, as an example of best practice, there should be one DMP per project to which all partners can refer for guidance.

5.4.4 When should I write a data management plan?

DMPs should be written before or at the beginning of a research project, and be reviewed at regular intervals during the project. Adjustments should be made during these reviews, or whenever necessary due to significant changes, such as the use of new data, the use of data for different purposes or the addition of new data controllers or processors. As such, DMPs should be 'living documents' that constantly evolve over the course of a project. Data management, in other words, should be a priority during the entire project.

5.4.5 Who, if anyone, reviews or approves my data management plan?

A DMP does not typically need the approval of a Data Protection Officer (DPO) or an institutional authority. However, the precise obligations that research funding organizations or institutional guidelines impose may vary. As DMPs describe the data management practices of research projects in detail and allocate responsibilities, they often include information on who the relevant DPOs are, especially in projects that process personal data. In such cases, it often makes sense to involve DPOs in the

drafting process. Moreover, DPOs are typically a good source of advice and can often help researchers to adhere to all pertinent legislations and standards of good practice.

Besides, research funding organizations may view DMPs as formal project deliverables that should be submitted, and which subsequently are reviewed by experts who may request changes. Approval mechanisms, consequently, vary depending on circumstances and contractual obligations.

5.4.6 What is the legal standing and coercive force of data management plans?

DMPs are not legally binding. Instead, they provide guidance, increase transparency and help researchers follow relevant legislation, like the GDPR. The coercive force rests primarily in the legal instruments (e.g. data protection law, cybersecurity regulations) and agreed-upon guiding principles (e.g. FAIR data management principles) that the DMP specifies for concrete research projects, but not in DMPs themselves.

Research funding organizations increasingly make the disbursement of funds conditional on proper research data management, which adds 'teeth' to DMPs as an instrument. However, this does not change their formal legal status.

5.4.7 Where can I get help with writing a data management plan?

As good data management has become a core element of good scientific practice, resources helping researchers to develop DMPs have proliferated. For example, DMPs for projects funded by the European Commission under the Horizon 2020 research and innovation program should follow the template provided here and include information explained here. If you submit your proposal to another funder you should check whether they offer guidance or have formulated specific requirements. Other useful templates and guidelines are provided by, among others, the Digital Curation Centre, DMPTool of the University of California (focused on the USA), OpenAIRE, the Go-FAIR initiative, the Research Data Management Organizer and various universities. Before writing a DMP, it is worth checking if your university or research institute has developed a DMP template. Data Protection Officers – in case personal data are concerned – or Research Ethics Committees might also be able to help formulating your DMP.

Helpful YouTube videos are provided by, for example, OpenAIRE (here and here), the New York University Health Sciences Library (here) and UK Data Service (here). Regular webinars and trainings on research data management are offered by the Consortium of European Social Science Data Archives (CESSDA); see here.

However, it is important to emphasize that many of these resources contain little information on which research data should be considered personal data, and to which, therefore, the requirements of open science only apply with major qualifications. We recommend not following the templates and recommendations linked above blindly, but consider your own particular data protection requirements. Your DMP should always outline which data will and which data will not be shared, and explain why sharing the latter data is not possible. Importantly, anonymized personal data can be shared as they are no longer considered personal data. Personal data, on the other hand, cannot be

shared unless a lawful basis permits otherwise. Existing policies, such as the "Privacy Policy" of an institution can be mentioned in the DMP to underline your institution's commitment with the questions concerned.

5.4.8 Who should write a DMP?

Every researcher dealing with data might write a DMP to facilitate their own research, comply with principles of scientific integrity and make potential conflicts and issues with data management visible early on. In a research consortium one person should be responsible, but especially in inter- and transdisciplinary research projects everybody should be involved, to take into account different disciplinary perspectives and needs.

DOs

- Write a DMP before starting a research project
- Review and update your DMP over the course of a research project
- Outline how research data will be handled during and after the end of a project
- Outline what data will be collected, generated and processed
- Outline which methodology and standards will be used
- Specify whether data will be shared
- Observe data protection legislation
- Anonymized data can be shared as they are not personal data
- Outline how data will be curated and preserved, during and after the end of a project
- Consult your DPO in case of doubt
- Monitor ongoing developments in data protection legislation and research data management
- Obey the FAIR principles: findable, accessible, interoperable, reusable

DONT's

- Don't follow recommendations blindly: many general recommendations on research data management do not take data protection requirements sufficiently into account
- Don't share personal data unless you are sure that doing so is lawful
- Don't refrain from writing a DMP, even if you are not required to do so

Checklist

- Does my DMP describe the collection, organization, use, storage, contextualization, preservation and sharing of data clearly?
- Have I allocated sufficient resources to data management?
- Are these resources clearly allocated?
- Are responsibilities clearly and unambiguously assigned?
- Is it clear who the data controllers and data processors are?
- Are procedures for protecting and safeguarding data clearly specified?
- Is it clear which data will be shared, with whom data will be shared, and which data will not be shared?
- Are all data protection requirements met?

5.5 Documentation of Processing Personal Data

Bud P. Bruegger (ULD)

The final version of this section was validated by Hans Graux, guest lecturer on ICT and privacy protection law at the Tilburg Institute for Law, Technology, and Society (TILT) and at the AP Hogeschool Antwerpen. President of the Vlaamse Toezichtscommissie (Flemish Supervisory Committee), which supervises data protection compliance within Flemish public sector bodies.

An organization who is processing personal data (including both, controllers[63] and processors[64]) needs to documents its activities primarily for consumption by the competent Data Protection Supervisory Authorities[65] (DPA). This includes the ***records of processing***[66] that is maintained centrally by the organization across all its processing activities and **additional documentation** that pertains to an individual data processing activity. These are discussed separately in the following. The discussion focusses on the most common case for the intended audience, i.e., that a new processing activity is started within an organization that already has appointed a data protection officer who already keeps records of processing.

[63] See Art. 30(1) GDPR.
[64] See Art. 30(2) GDPR.
[65] See Art. 58(1)(a), 30(4) and 5(2) GDPR.
[66] See Art. 30 GDPR.

5.5.1 Records of Processing

Records of processing can be kept in written or electronic form[67]. So expect to either fill in an organization-specific form or enter your information into some (data protection) management system.

To provide an initial idea, the minimal content of the records of processing for controllers includes the following items[68]:

- the **name** and **contact** details **of the controller**, the controller's **representative** and the **data protection officer**;
- the **purposes** of the processing;
- a description of the **categories of data subjects** and of the **categories of personal data**;
- the **categories of recipients** to whom the personal data have been or will be disclosed;
- where applicable, **transfers of personal data to a third country** (see "Transfer of data to third countries" in Part II, section in the "Main Tools and Actions" of these Guidelines") together with the documentation of suitable safeguards;
- where possible, the envisaged **time limits for erasure of the different categories of data** (see "Storage limitation" in Part II, section "Principles" of these Guidelines");
- where possible, a general description of the **technical and organizational *security* measures** (see "Integrity and confidentiality" in Part II section "Principles" of these Guidelines");.

Your organization may use a different set of items since on one hand, it already is in possession of some of this information (such as the first bullet), and on the other hand, it may require additional information (such as the contact of the person responsible for the single processing activity at hand). It is possible that the legally required record keeping is combined with the management needs of the organization, such as an internal inventory of computing and computing resources.

Your organization may also use multiple systems, e.g. depending on whether it is acting as a controller or as a processor; or distinguishing between permanent data processing activities (such as communication systems and accounting) and temporary ones (such as

[67] See Art. 30(3) GDPR.
[68] See Art. 30(1) GDPR for more detail.

those linked to temporary projects or assignments). The creation and maintenance of records across multiple systems is not prohibited under the GDPR.

Should you have difficulties in providing the requested information, your data protection officer (if your organization has one) may be able to help.

Checklist (records of processing)

- Contact the office/person who is keeping the records of processing for your organization.
  - If necessary, your Data Protection Officer can help establish the contact.
- Inform them early on that you intend to process personal data.
  - Your processing activity needs to be entered in the records before processing starts.
- Follow their instructions of
  - what information you need to provide for the records of processing,
  - when you need to send updates of this information.

5.5.2 Additional documentation pertaining to a single processing activity

In addition to the records of processing that are managed centrally in the organization, the person(s) responsible for a specific processing activity has to maintain additional documentation. For this purpose, it is good practice to set up a **systematic way of collecting the necessary documentation** starting **from the time when you conceive and plan your possessing activity**[69]. This kind of information can be asked for by Data Protection Supervisory Authorities either remotely[70] or during on-premise audits[71]. The necessary action is described in the following DOs:

DOs

- Data protection (like security) is a process, not a final state. Continuously document that process rather than only the final characteristics of the

[69] Art. 25(1) GDPR calls this "the time of the determination of the means for processing".
[70] See Art 58(1)(a) GDPR.
[71] See Art 58(1)(b) GDPR.

processing activity.

- When applying data protection by design[72], the processing activity can be seen as the results of a series of many considerations and decisions. It is these considerations and decisions that should be documented.
- Deciding on a structure and format to systematically collect this information at the point of time when you conceive your processing activity.
- Where the documentation itself contains personal information (see below), make sure to protect is sufficiently and limit its further use to the purpose of demonstrating compliance with the GDPR.

This documentation encompasses at least the following that is first listed in a checklist and then described in more detail thereafter.

5.5.2.1 Assessment whether the processing activity likely results in a high risk to the rights and freedoms of natural persons

In order to determine whether a Data Protection Impact Assessment (DPIA) is required for a processing activity, an assessment has to be made to whether the processing likely results in a high risk. This was described in the section "In what cases must I carry out a DPIA" in "Data Protection Impact Assessment" above. It is based on guidelines by the Article 29 Working party and consists of the Boolean evaluation of nine criteria. It is important to document this particularly as a justification for the case where a DPIA is unnecessary (see "DPIA" in Part II, section "Main Tools and Actions" of these Guidelines).

5.5.2.2 A Data Protection Impact Assessment where the above assessment yields an affirmative result

Where a DPIA is necessary, the DPIA itself is part of the documentation of processing. See Art. 35 GDPR and *Data Protection Impact Assessment* above for detail.

5.5.2.3 Potential consultation of the competent supervisory authority prior to processing

Where the DPIA indicates that the processing would result in a high risk even after mitigation with appropriate technical and organizational measures, the controller shall consult the supervisory authority prior to processing (see Art. 36(1) GDPR). Such consultation must be documented.

[72] See Art. 25 GDPR.

5.5.2.4 Requirements and acceptance tests for the purchase and/or development of the employed software, hardware, and infrastructure

According to Art. 25 GDPR, when determining the means of processing, a controller has to take the following into account:

- The state of the art,
- the cost of implementation,
- the nature, scope, context and purposes of processing, and
- the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing.

Based on this evaluation, the controller implements appropriate technical and organizational measures which are designed to implement data-protection principles, to meet the requirements of the GDPR and to protect the rights of data subjects.

This evaluation and the decisions taken have to be documented in order to comply with the requirement of **data protection by design** (of Art. 25 GDPR). Practically, this can take the form of:

- Data protection **requirements** specified for the purchase (e.g., a tender) or development of software, hardware and infrastructure,
- **acceptance tests** that verify that the chosen software, systems and infrastructure are fit for purpose and provide adequate protection and safeguards.

Such documentation can be an integral part of the DPIA.

5.5.2.5 Implemented technical and organizational measures

The documentation shall also comprise the technical and organizational measures that are implemented to mitigate the data protection risks and safeguard the rights and freedoms of data subjects.

The security measures are also part of the *records of processing* (see Art. 30(1)(g) GDPR); all implemented measures are part of the DPIA (see Art. 35(7)(d) GDPR).

5.5.2.6 Regular testing, assessing and evaluating the effectiveness of technical and organizational measures

The GDPR emphasizes data protection as a process. This is evident in Art. 32(1)(d) that requires regular testing, assessing and evaluating the effectiveness of technical and organizational measures, and Art. 35(11) that requires the controller to carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations. Such recurring testing, assessing and evaluating shall be documented.

5.5.2.7 Requirements and acceptance tests for the selection of processors

According to Art. 28(1) GDPR, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organizational measures. This requires a selection process that shall be documented.

5.5.2.8 Contracts stipulated with processors

According to Art. 28(3) GDPR, the processing by a processor shall be governed by a contract that requires among others the implementation of appropriate measures and safeguards (see points d and e) and the right for inspection and audit by the controller (see point h). Such contacts are part of the documentation.

5.5.2.9 Possible inspections and audits of the processor

When a controller inspects or audits a processor according to Art. 28(3)(h), the actions taken and the outcome shall be documented.

5.5.2.10 Method to collect consent

Valid consent requires the fulfilment of stringent requirements (see Art. 4(11) and 7 GDPR). Where a controller chooses consent as a legal basis for (part of the) processing, the way (e.g., dialog) in which the consent was collected must be documented in order to demonstrate that the requirements were satisfied. Where dialogs change over time, a versioning that records the time of change is necessary.

5.5.2.11 Demonstrations of individual expressions of consent

According to Art. 7(1), the controller shall be able to demonstrate that the data subjects have consented to processing of their personal data. This requirement is discussed in more detail by the *EDPB* in their *Guidelines 05/2020 on consent under Regulation 2016/679*[73]. One possible way to demonstrate consent that they describe is to "retain information on the session in which consent was expressed, together with documentation of the consent workflow at the time of the session, and a copy of the information that was presented to the data subject at that time."[74]

This illustrates that documentation in support of being able to demonstrate consent itself must be considered personal data. It must therefore be adequately protected and its use limited to the purpose of such demonstration.

[73] Section 5.1, pages 21 and 22 in EDPB, Guidelines 05/2020 on consent under Regulation 2016/679, Version 1.0, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf (last visited 11/05/2020).
[74] See at the end of paragraph 108.

5.5.2.12 Information provided to data subjects

Art. 13 and 14 GDPR require the controller to provide adequate information about the processing to data subjects. To demonstrate compliance, the information actually provided shall be documented. Again, a versioning is necessary if the provided information changes over time.

5.5.2.13 Implementation of data subject rights

Articles 15 through 22 mandate the controller to grant data subjects specific right (as for example the right to rectification of inaccurate data, or the right "to be forgotten") (see "Data Subject Rights" in Part II of these Guidelines). In addition, when processing is based on consent, data subjects have the right to withdraw consent at any time (see Art. 7(3) GDPR). To demonstrate compliance, it is necessary to document how these rights are implemented[75]. Again, versioning may be necessary.

5.5.2.14 Actual handling of data subject rights

When data subjects invoke their rights, they shall be processed by the controller without delay. Art. 12(3) and (4) specify maximal acceptable response times. In order to demonstrate correctness and timeliness of the actions taken and response sent, a documentation is necessary. Again, this documentation constitutes personal data and has to be adequately protected.

5.5.2.15 Possible breach notifications to the competent supervisory authority

Art. 33 GDPR requires notification of a personal data breach to the supervisory authority. Such notifications shall become part of the documentation.

5.5.2.16 Possible communication of data breaches to concerned data subject

Art 34 GDPR requires communication of a personal data breach to the data subject under certain conditions. Such communications shall be documented. They likely contain personal data that need protection.

5.5.2.17 Any other communication with the competent supervisory authority

Any communication with a supervisory authority should be documented. Such communication can for example be initiated by the supervisory authority according to Art. 31 GDPR. Communication initiated by the controller according to Art. 36 was already listed above. In addition, data protection officers can also consult supervisory authorities according to Art. 39(1)(e).

[75] The term "implemented" is not intended to imply automation; manual processing, for example by the data protection officer or another designated person, can be perfectly acceptable.

Checklist (additional documentation pertaining to a single processing activity)

The following items must be documented:

- Assessment whether the processing activity likely results in a high risk to the rights and freedoms of natural persons.
- A Data Protection Impact Assessment where the above assessment yields an affirmative result.
- Potential consultation of the competent supervisory authority prior to processing.
- Requirements and acceptance tests for the purchase and/or development of the employed software, hardware, and infrastructure.
- Implemented technical and organizational measures.
- Regular testing, assessing and evaluating the effectiveness of technical and organizational measures
- Requirements and acceptance tests for the selection of processors.
- Contracts stipulated with processors.
- Possible inspections and audits of the processor.
- Method to collect consent.
- Demonstrations of individual expressions of consent.
- Information provided to data subjects.
- Implementation of data subject rights.
- Actual handling of data subject rights.
- Possible breach notifications to the competent supervisory authority.
- Possible communication of data breaches to concerned data subject.
- Any other communication with the competent supervisory authority.

5.6 Legitimate Interest and Balancing Test

Iñigo de Miguel Beriain (UPV/EHU)

Acknowledgements: The author thankfully acknowledges advice, input and feedback on drafts from Bud Bruegger and Harald Zwingelberg.

This part of The Guidelines has been reviewed and validated by Marko Sijan, Senior Advisor Specialist, (HR DPA)

Legitimate interest is one of six legal bases for the processing of personal data stated in Article 6(1) of the GDPR (see "Lawfulness, fairness and transparency" subsection in the "Principles" within Part II of these Guidelines). This legal basis requires that the legitimate interests of the controller or any third parties to whom the data are disclosed prevails over the interests, fundamental rights and freedoms of the data subjects (Article 6(1)(f). To verify that this is indeed the case, controllers can make use of a tool that is called ***balancing test***, which has been recommended by the Article 29 Working Party, for instance[76]. This tool is aimed at ensuring that the legitimate interests of the controller or any third parties to whom the data are disclosed prevails over the interests and fundamental rights and freedoms of the data subjects.

5.6.1 When do fundamental rights and freedoms of the person concerned by the data protection do not take precedence?

Carrying out a balancing test involves considering several key factors that are decisive in determining which interests, freedoms or rights prevail, namely[77]:

- The nature and source of the legitimate interest: whether the data processing is necessary for the exercise of a fundamental right, is otherwise in the public interest, or benefits from recognition in the community concerned. Evaluating the possible prejudice suffered by the controller, by third parties or the broader community if the data processing does not take place is compulsory.
- The **power and status of the two parties** (controller or third party and data subject). For instance, an employer intending to process the data of an employee is in a stronger position than the employee. If the data subjects are minors their interests, rights or freedoms should be overweighed.
- **The nature of the data.** While processing of any personal data should be adequately weighed, processing of special categories of personal data such as racial origin, religious beliefs, generic data or data concerning health, should be given greater weigh.

[76] A29WP, Opinion 06/2014 on the notion of legitimate interests of the controller under Article 7 of Directive 95/46/EC. April 2014, p. 24. At: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf. Accessed 05 January 2020

[77] A29WP, Opinion 06/2014 on the notion of legitimate interests of the controller under Article 7 of Directive 95/46/EC. April 2014, p. 24. At: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf. Accessed 05 January 2020.

- **The impact of the processing on the data subjects.** To this purpose, controllers should consider whether processing might result in a high risk to individuals' rights and freedoms. If this is the case, they must perform a DPIA.
- The data subjects' **reasonable expectations** about what will happen to their data. Controllers should be able to demonstrate that a data subject would expect the processing in light of the particular circumstances applicable. If the purpose and method of processing is not immediately obvious and there is the potential for a range of reasonable opinions about whether people would expect it, controllers may wish to carry out some form of consultation, focus group or market research with individuals to demonstrate expectations and support their position. If there are pre-existing studies in regard to reasonable expectations in a particular context, controllers may be able to draw on these as part of their determination of what individuals may or may not expect.[78]
- The **way data are processed** (large scale, data mining, profiling, disclosure to a large number of people or publication);
- **The additional safeguards** which could limit undue impact on the data subject, such as data minimization (e.g. strict limitations on the collection of data, or immediate deletion of data after use) - technical and organizational measures to ensure that the data cannot be used to take decisions or other actions with respect to individuals ('functional separation') - wide use of anonymization techniques, aggregation of data, privacy-enhancing technologies, privacy by design, privacy and data protection impact assessments; - increased transparency, general and unconditional right to object (opt-out), data portability & related measures to empower data subjects, etc.

5.6.2 The issue of the additional safeguard

The Article 29 Working Party considers that mitigation measures and safeguards, such as organizational or technical measures adopted by the controller for the protection of the data subject data should be included in the balancing test. There is, however, an alternative approach, which considers that article 6(1)(f) asks for a balancing test between two values, the legitimate interests of the controller (or a third party) and the interests, rights and freedoms of the data subject. Mitigation measures and safeguards do not fit well with any of these values. Therefore, they should not be considered. Otherwise, they would overweigh the controllers' side since they would undermine the importance of the possible harm to be caused to the data subject interests, rights and

[78] ICO, How do we apply legitimate interests in practice? At: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/how-do-we-apply-legitimate-interests-in-practice/ Accessed: 15 January 2020

freedoms. Kamara and De Hert have made some convincing statements on this concrete issue, by stating that[79]

> "*including mitigation measures in the assessment would lead to a representation of the actual expected impact of the processing to the data subjects' rights, and would still allow the legitimate interests to prevail. This approach does not 'punish' the controller that takes mitigation measures and safeguards, by not including them in the balancing test. On the contrary it encourages the controller to do so. On the other hand, one should keep in mind that the weight of future safeguards and mitigation measures is always relevant to their realisation and effectiveness. Such measures therefore should be considered, but not play a significant role in determining to which side the scale leans."*

DOs

- Check the nature of the data processed and take extra care about special categories of personal data (especially if data subjects are children)
- Consider the reasonable expectations of the data subjects
- Perform a DPIA if circumstances recommend it

DON'Ts

- Don't process special categories of personal data if it is not absolutely necessary to reach the pursued interest
- Don't process the data if the balancing test is inconclusive
- Don't hesitate to introduce adequate safeguards to minimize prejudice to data subjects interests, rights and freedoms

Checklist

- The controllers have made sure that the individual's interests do not override legitimate interests of the controller or third parties.
- The controllers use data subject's data in ways they would reasonably expect.
- The controllers are not using data subject's data in a very intrusive way or in a

[79] Kamara, Irene and De Hert, Paul, "Understanding the balancing act behind the legitimate interest of the controller ground: a pragmatic approach, Brussels Privacy Hub, Working paper, vol. 4, nº 12, 2018, p.17. At: https://brusselsprivacyhub.eu/BPH-Working-Paper-VOL4-N12.pdf Accessed: 17 January 2020

way which could cause them harm, unless they have a particularly good reason.

- The controllers do not process special categories of personal data, or, if they do, they have taken care that adequate technical and organizational safeguards are implemented in processing.
- The controllers have considered safeguards to reduce the impact where possible.
- The controllers have considered whether they need to conduct a DPIA.

5.6.3 **Further Reading**

- Additional examples of balancing test were provided by the Article 29WP and can be found in their Opinion 06/2014 on the notion of legitimate interests of the controller under Article 7 of Directive 95/46/EC
- A29WP, Opinion 06/2014 on the notion of legitimate interests of the controller under Article 7 of Directive 95/46/EC. April 2014, p. 24. At: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf
- EDPS, Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit, 11 april 2017, at: https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en.pdf. Accessed 5 May 2020
- ICO, How do we apply legitimate interests in practice? At: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/how-do-we-apply-legitimate-interests-in-practice/
- ICO, What is the 'legitimate interests' basis? https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/. Accessed 05 May 2020.
- Kamara, Irene and De Hert, Paul, "Understanding the balancing act behind the legitimate interest of the controller ground: a pragmatic approach, Brussels Privacy Hub, Working paper, vol. 4, nº 12, 2018, p.17. At: https://brusselsprivacyhub.eu/BPH-Working-Paper-VOL4-N12.pdf

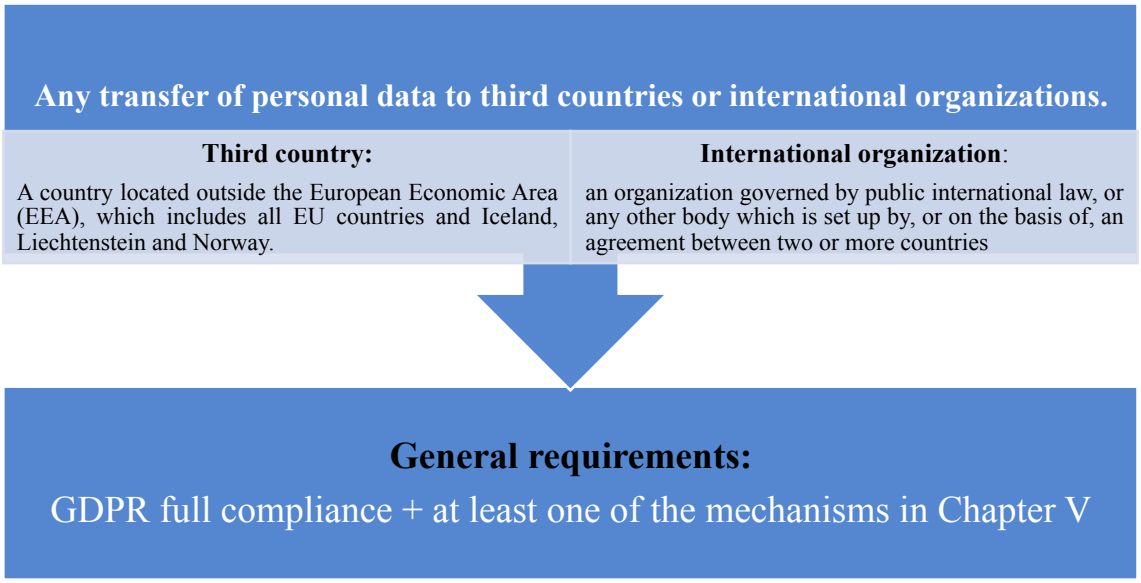
5.7 Transfer of Data to Third Countries

Mikel Recuero Linares (UPV/EHU)

This part of The Guidelines has been reviewed and validated by Marko Sijan, Senior Advisor Specialist, (HR DPA)

The GDPR does not expressly define what is meant by a transfer of data to third countries or international organizations (hereinafter 'international transfer'). However, the regime for international transfers is explicitly laid down in Article 44 to 50 of the Regulation. Therefore, the definition of international transfer has to be inferred by assessing each concept individually, which will result in the following definition:

The processing operation whereby a controller or a processor within the EEA ('data exporter') transfers (or gives access to) personal data to a controller or processor outside the EEA ('data importer') or an international organization.



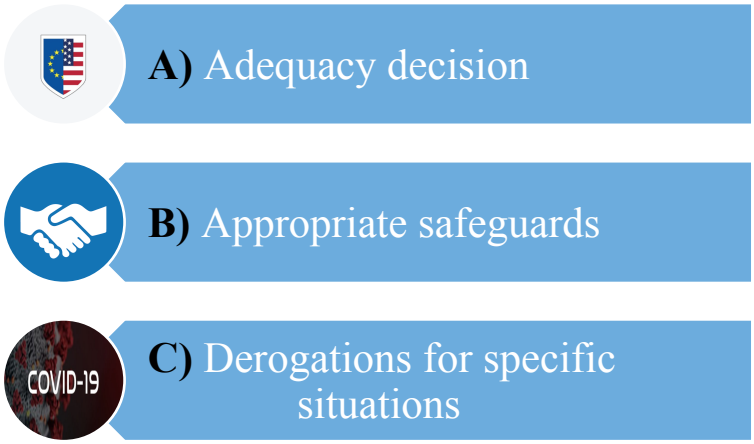
These transfers are perfectly acceptable and often necessary, but they should not undermine the level of protection of the concerned individuals given in the EU or granted by the GDPR. Therefore, transfers to third countries or international organizations should be done in full compliance with Chapter V of the GDPR.

5.7.1 Requirements

Transfers of personal data to third countries and international organizations may only be carried out:

i. **Where the controller or processor has complied with the other provisions of the GDPR[80].** Prior to carrying out the international transfer, provisions and requirements under the GDPR must also be complied with. In addition to the specific rules of Chapter V applicable to data transfers, the data importer and the data exporter will have to comply with "the other provisions of this Regulation" (e.g. general principles, legal basis, derogations for the processing of sensitive data, etc.).

ii. **Where specific conditions laid down relating to the transfers of personal data are complied with by the controller or processor**. This can be carried out, mainly, through three instruments, in this exact order:



iii. These principles and requirements will not only apply to the first data transfer, but also to onward transfers to other controllers or processors in the same or another third country or international organization[81].

A) Transfers on the basis of an adequacy decision

Firstly, a transfer can only be carried out where it is covered by an adequacy decision. This decision is a ruling by the European Commission that the legal framework in place in that country, territory, sector or international organization provides 'adequate' protection for individuals' rights and freedoms for their personal data[82]. An "adequacy decision" is an implementing act by the Commission[83] adopted in accordance with an examination procedure[84] and subject to a periodic review.

The adoption of an adequacy decision involves:

- a proposal from the European Commission;
- an opinion of the European Data Protection Board ("EDPB");

[80] See Article 44 of the GDPR "Any transfer of personal data (…) shall take place only if, subject to the other provisions of this Regulation (…)".
[81] See Article 44 *in fine* of the GDPR.
[82] Article 45(1) of the GDPR.
[83] Article 45(3) of the GDPR.
[84] Article 93(2) of the GDPR.

- an approval from representatives of EU countries; and
- The adoption of the decision by the European Commissioners.

The aim of this decision is therefore to assess whether a country, territory, sector or international organization provides an 'adequate' level of protection for individuals' rights and freedoms (see "Data Subject Rights" in Part II of these Guidelines). Moreover, Article 45(2) of the GDPR lists the elements that the Commission shall, in particular, take into account when assessing the adequacy of the level of protection in a third country or international organization.

The benefits of relying on adequacy decisions for carrying out international transfers are obvious. The decision will have EU-wide effect[85] and no specific authorization will be required[86]. However, this mechanism also poses several shortcomings:

- **There are very few countries with valid adequacy decisions in force[87].**
- **The adequacy decisions in force do not necessarily apply to and / or cover all processing operations and sectors.**
- **The case law of the Court of Justice of the European Union has significantly diminished the robustness and trust of these tools.** Specific reference should be made to its Schrems I[88] and II[89] judgments, which, among other issues, annulled the 'Safe Harbor' and 'Privacy Shield' decisions, respectively:
  - The word 'adequate' must be understood as requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed in the EU[90], even though the means to which that third country has recourse may differ from those employed within the EU[91].
  - The national supervisory authorities are vested with the power to check whether a transfer of personal data from its own Member State to a third country complies with European data protection rules[92]. However, as a rule, as long as the Commission's decision is not declared invalid by the CJEU, the Member States and the supervisory authorities cannot adopt measures

[85] Recital 103 of the GDPR.
[86] Article 45(1) *in fine* of the GDPR.
[87] After the further annulment of the Privacy Shield by the CJEU, there are currently only decisions in force with: Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland and Uruguay.
[88] Court of Justice of the European Union. Judgment of 6 October 2015, Maximillian Schrems v Data Protection Commissioner (C-362/14, Schrems I).
[89] Court of Justice of the European Union. Judgment of 16 July 2020, Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems, (C-311/18, Schrems II)
[90] Court of Justice of the European Union. Judgment of 6 October 2015, Maximillian Schrems v Data Protection Commissioner (C-362/14, Schrems I). Parag. 73.
[91] Ibid. parag. 74.
[92] Ibid. parag. 47.

contrary to that decision[93]. This cannot prevent persons whose personal data has been or could be transferred to a third country from lodging a claim[94].

- Legislation permitting public authorities to have access on a generalized basis to the content of electronic communications must be regarded as compromising the essence of the fundamental rights of European data subjects[95]. Likewise, legislation not providing any possibility for individuals to pursue legal remedies in order to have access to personal data relating to them, or to obtain the rectification or erasure of the data does not respect the essence of the fundamental right to effective judicial protection[96].

B) Transfers subject to appropriate safeguards

In the absence of 'adequacy decision' a controller or processor may transfer personal data to a third country or an international organization only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subjects' rights and effective legal remedies for data subjects are available[97]. That is to say, if there is no 'adequacy decision' about the country, territory or sector to which the transfer is to be made, the controller or processor may choose between the mechanisms set out in Article 46 of the GDPR in order to provide 'appropriate safeguards'.

In the application of the mechanisms in Article 45 there is no need to observe a specific order. It is possible to choose the mechanisms according to the particular needs or the purpose of the processing. However, the GDPR classifies these mechanisms according to whether or not they require any specific authorization from a supervisory authority:

i. **Mechanisms that do not require any specific authorization from a supervisory authority[98]:**

   a) Legally binding and enforceable instruments between public authorities or bodies. E.g. administrative arrangements which include enforceable and effective individual rights

   b) Binding Corporate Rules (BCR). These are commonly used for data transfers within multinational companies. BCRs are an internal code of conduct operating within a multinational group, which applies to restricted transfers of personal data from the group's EEA entities to non-EEA group entities. There are many documents about the BCRs adopted by the European Data Protection Board and the former WP29[99]

[93] Ibid. parag. 52.
[94] Ibid. parag. 53 and 66.
[95] CJEU Judgment of 16 July 2020, Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems, (C-311/18, Schrems II) Parag. 185.
[96] Ibid. parag. 197 and 198.
[97] Art. 46 of the GDPR.
[98] Under art. 46.2 of the GDPR.
[99] EC. Binding Corporate Rules (BCR). At: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en Accessed 12 May 2020.

c) Standard Contractual Clauses (SCC) adopted by the Commission. Also known as model clauses. They contain contractual obligations on the data exporter and the data importer and rights for the individuals. Therefore, they must be signed between both data exporter (EAA country) and the data importer (outside EAA country or international organization). The European Commission adopted SCC models for controllers and for processors[100].

d) An approved code of conduct. The transfer could be carried out if the receiver has signed up to a code of conduct which has been previously approved by a supervisory authority. The code of conduct must include minimum content and requirements in accordance with Article 40 of the GDPR (i.e. appropriate safeguards to protect the rights of individuals). The EDPB has adopted a set of guidelines on codes of conduct.[101] No approved codes are yet in use. However, many institutions and organizations are developing codes (e.g.the BBMRI-ERIC is developing a Code of Conduct for Health Research).[102]

e) An approved certification. The transfer could be carried out if the receiver has a certification, under a scheme approved by a supervisory authority. The certification mechanism must include minimum content and requirements in accordance with Article 40 of the GDPR (i.e. appropriate safeguards to protect the rights of individuals). The EDPB has adopted a set of guidelines on certification mechanisms[103]. No approved certification mechanisms are yet in use.

ii. Mechanisms that require authorization from the competent supervisory authority:

a) Contractual clauses authorized by a supervisory authority. Even if the model clauses adopted by the European Commission are not used, other models of SCC may be adopted if they are previously and individually approved by the competent supervisory authority.

b) Provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights, e.g., a document such as a memorandum of understanding.

---

[100] Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council. C/2021/3972. OJ L 199, 7.6.2021, p. 31–61. Available at: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj

[101] EDPB. Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679 Version 2.0 4 June 2019. At: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201901_v2.0_codesofconduct_en.pdf Accessed 12 May 2020

[102] BBMRI-ERIC, Code of conduct for health research: taking up speed & calling for your input, At: https://www.bbmri-eric.eu/news-events/code-of-conduct-for-health-research/ Accessed 12 May 2020

[103] EDPB. Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation Version 3.0 4 June 2019. At: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_en.pdf. Accessed: 12 May 2020.

Nevertheless, the case law stemming from the Schrems II ruling of the Court of Justice of the European Union has led to important consequences for the Standard Contractual Clauses and the rest of mechanisms for transferring data to third countries on the basis of appropriate safeguards. Firstly, because data subjects whose personal data are being transferred to a third country pursuant to Standard Contractual Clauses (or other mechanisms) should be afforded, as in the context of an adequacy decision, a level of protection essentially equivalent to that guaranteed within the European Union[104]. Secondly, because this may require, depending on the prevailing position in a particular third country, the adoption of supplementary measures by the controller in order to ensure compliance with that level of protection[105]. As a result, if the data exporter established in the EU is not able to take appropriate supplementary measures, they are required to suspend or prohibit the transfer of personal data "in the event of the breach of such clauses or if it is impossible to honor them"[106].

C) Derogations for specific situations

Finally, where the transfer is not covered by an adequacy decision, nor an appropriate safeguard mechanism, it shall only be carried out if it is covered by any of the exceptional derogations or situations set out in Article 49 of the GDPR[107]:

i. Where the data subject has explicitly consented to the proposed transfer.

ii. Where the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request.

iii. Where the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person.

iv. Where the transfer is necessary for important reasons of public interest.

v. Where the transfer is necessary for the establishment, exercise or defense of legal claims.

vi. Where the transfer is necessary in order to protect the vital interests of the data subject or of other persons, when the data subject is physically or legally incapable of giving consent.

vii. Where the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest.

---

[104] Court of Justice of the European Union. Judgment of 16 July 2020, *Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems*, (C-311/18, *Schrems II*). Parag. 96.
[105] Ibid. Parag. 132 and 125.
[106] Ibid. Parag. 134 and 135.
[107] More information about art. 49 derogations and exceptions can be found in the EDPB, Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679 Adopted on 25 May 2018, At: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf Accessed: 14 May 2020

5.7.2 **Further Reading**

Article 29 Data Protection Working Party. Recommendation on the approval of the Processor Binding Corporate Rules form. https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51307

Article29 Data Protection Working Party. Recommendation on the Standard Application for Approval of Controller Binding Corporate Rules for the Transfer of Personal Data. https://edpb.europa.eu/sites/edpb/files/files/file2/wp264_art29_wp_bcr-c_application_form.pdf

Court of Justice of the European Union. Judgment of 16 July 2020, *Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems*, (C-311/18, *Schrems II*).

Court of Justice of the European Union. Judgment of 6 October 2015, Maximillian Schrems v Data Protection Commissioner (C-362/14, Schrems I).

European Commission. Binding Corporate Rules (BCR). https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en

European Commission. Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council. C/2021/3972. OJ L 199, 7.6.2021, p. 31–61. Available at: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj

European Commission. Rules on international data transfers. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/rules-international-data-transfers_en

European Data Protection Board (EDPB). Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_en.pdf

European Data Protection Board (EDPB). Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201901_v2.0_codesofconduct_en.pdf

European Data Protection Board (EDPB). Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf