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 ACTORS

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.

3 Main Actors

Frédéric Tronnier (GUF)

This section aims to explain the main actors, that is, the roles that may be assigned to individuals, organizations or other entities in the GDPR. Art. 4(7-10) define several of these actors while others are defined later on in the GDPR[1]. Here, these actors will be defined in order to clarify the different tasks, rights and responsibilities that each actor possesses. In order to work with personal data and to comply with the GDPR it is necessary to understand the role that one takes when working with personal data. A brief summary on the main actors is made in table 1. Within the main body of this document, practical examples are provided in order to illustrate the interplay between the different categories of actors.

[1] For more detailed information on the main actors: controller, processor and joint controllers, we refer to the EDPS guidelines on these actors. EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725. Available under: https://edps.europa.eu/sites/edp/files/publication/19-11-07_edps_guidelines_on_controller_processor_and_jc_reg_2018_1725_en.pdf (Last visited: 03.12.2020)
And Guidelines 07/2020 on the concepts of controller and processor in the GDPR. Available under: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf (Last visited: 03.12.2020)

Actor	**Data Subject**	**Controller**	**Processor**	**Joint Controllers**	**Recipient**	**Third Party**	**Data Protection Officer**	**Supervisory Authority**
GDPR	**Art.4(1)**	**Art.4(7)**	**Art.4(8)**	**Art.26**	**Art.4(9)**	**Art.4(10)**	**Art.37**	**Art.51**
Short description	A natural person that can directly or indirectly be identified through personal data.	Any entity that determines the purposes and means of the processing of personal data.	Handles the processing of personal data on behalf of the controller. Does not determine the purposes of this processing.	Two or more controllers that are jointly determining the purposes and means of processing of personal data.	Any entity to which personal data is disclosed to, with the exception of public authorities that receive personal data in accordance with the law.	Any other entity other than controller, processor, data subject or persons authorized to process personal data.	Natural person that acts independently within an organization to ensure the correct application of the GDPR	Independent public authority established by the EU member states. Also called Data Protection Authorities (DPAs).
Tasks	No tasks specified in the GDPR. Data subjects can enforce their rights stated in Art.12-23 GDPR.	Is in control of the data and decides what is done with it. Usually wants to achieve a goal with the data.	Processes the data under the instructions of the controller.	The tasks are the same as those of a (single) controller but are performed by all joint controllers	Has no active part. A recipient is defined only by its access to personal data.	Has no active part.	Ensures that the rights of data subjects are protected Handles and addresses	Responsible for monitoring and enforcing the correct application of the GDPR.

				together.			complaints.	Promotes awareness on issues of data processing. Handles complaints of data subjects.
Rights / Responsibili-ties	Equipped with many rights such as the right to rectification, erasure, restriction of processing, right to object and right of access.	Needs to ensure compliance with the GDPR in the processing of the data and be able to demonstrate that processing of personal data is performed in accordance with the GDPR. Needs to implement appropriate technical and	Acts under the instruction of the controller with a certain degree of freedom of choosing the most suitable methods for the processing. Guarantees that the processing meets the requirements of the GDPR.	Joint controllers need to determine their respective responsibilities for compliance with the data processing Need to provide a contact point for data subjects.	No rights and responsibilities. Will become a controller for any processing that is carried out for its own purposes.	Receives personal data. Will become a controller for any processing that is carried out for its own purposes.	Acts independently with an own budget and resources Should not be in a conflict of interest, therefore not a processor or controller.	Enforce application of the GDPR. Can issue warnings and reprimands, or ban or limit the processing of personal data by other entities.

		organizational measures for this.						

Table 1. Short summary on the main actors in the GDP

3.1 Data Subjects

3.1.1 Who are these actors?

The data subject is indirectly introduced in Art.4(1) GDPR as "an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person". A data subject is therefore a, living, individual that is identified through personal data. Deceased persons and legal entities are not defined as data subjects.

The GDPR aims to protect data subjects by getting them back in control of personal data that relates to them, by providing data subjects with rights that they can then exercise.

3.1.2 What are their rights and responsibilities?

Data subjects are provided with a large number of rights under Art.14-23 GDPR. Data subjects for instance have the right of access, meaning that they can demand from the controller to know whether personal data is processed, what categories of personal data are used, what the personal data is processed for and who the recipients of the personal data are. Data subjects furthermore have the right of erasure and rectification, meaning that they can demand that personal data relating to them is to be rectified or deleted. Data subjects also have the right of data portability, that is they can receive the personal data from the controller in a structured format and are then free to provide another controller with the data. According to Art.12 and Art.13 GDPR, controllers have to provide data subjects with personal data relating to them if data subjects request this. The personal data can be provided in writing or electronically, as well as orally if the identity of the data subject could be confirmed through other means. With regards to responsibilities, a controller might refuse to act on such a request for data, or charge a reasonable fee, if such requests for personal data are found to be unfounded or excessive.

If data subjects feel that their rights have been infringed upon by a controller or processor or as a result of processing of personal data, they can lodge a complaint with a supervisory authority (Art.77 GDPR). They can also have the have the right to an effective judicial remedy (Art.77 GDPR) in such a situation. If data subjects have suffered (non)material damage through the infringement of their rights given through the GDPR, they are able to be compensated by the controller or processor for the damage that they suffered. Data subjects are also able to mandate not-for-profit organizations or bodies to take these actions on their behalf, according to Art.80 GDPR.

Example 1:

Individual I is a user of a social network provider S. S gathers personal data such as home address, name, age and gender of I in order to provide I with the intended service.

As I is not sure what data S has gathered exactly, I requests access to the data using the right of access under Art.15 GDPR. Seeing that some of the data is factually incorrect, I requests the rectification of this inaccurate personal data under Art.16 GDPR.

3.2 Controllers

3.2.1 Who are these actors?

The controller can be any *"natural or legal person, public authority or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data (...)"* [2]. This shows that any entity who disposes of personal data for various reasons is considered a controller, be it, for instance, to conduct scientific research based on personal data or for marketing or business purposes. The controller has influence over the processing of personal data, through the execution of the processing or the ability to decide on the processing. In order to determine whether an entity is a controller, the following questions may be asked:

- Who makes decisions about data processing?
- Who has the power to stop the data processing?
- Why is the processing taking place?
- Who initiated the processing?
- Who benefits from the processing?[3]

The definition also includes the possibility that the controller does not act alone, but that there are multiple controllers, jointly controlling processing of personal data. The section on Joint Controllership explains this in more detail.

3.2.2 What are their tasks?

The controller determines the means and purposes of data processing. This means that the controller is in control of processing of personal data and the actor that actually decides what will be done with personal data. Usually, the controller aims to achieve a goal, e.g., a research project and objective or a business process*, for which the processing of data is necessary.

3.2.3 What are their rights and responsibilities?

The controllers need to ensure compliance with data protection regulation, such as the GDPR. In other words, the controllers are responsible for what happens with the personal data, how are they processed and whether the processing is compliant with the GDPR or not. In practice, this means that controllers have to introduce measures and safeguards aimed at respecting the application of the GDPR and demonstrating such policies. Indeed, Art.24 GDPR defines the responsibility of the controller to

[2] Art. 4(7) GDPR

[3] See EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725, p.7 based on Case C-210/16 Wirtschaftsakademie Schleswig-Holstein ECLI:EU:C:2018:388, para. 40 and Opinion of Advocate General Bot in case C-210/16, Wirtschaftsakademie, paras. 64 and 65.

"implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary."[4]

These technical and organizational measures are explained in more detail in the section "Principles" f this document. The controller needs to be able to demonstrate that the data processing principles, such as data minimization, storage limitation and transparency are implemented and guaranteed. This is referenced in Art.5(2) GDPR as the accountability of the controller. It is therefore essential that the controller is able demonstrate and document (Art.30(2) GDPR) that these principles are fulfilled. 56 Research projects should be conducted and implemented with the principles of privacy-by-design and privacy-by-default (Art.25 GDPR) in mind. Accountability hereby means that not only that "… the project proposal has to satisfy a given check list of conditions, but as the research methodology itself has to be ethical-legal compliant by design"7. Practical examples include the involvement of an interdisciplinary team, a legal-ethical expert appointed as DPO, IT-infrastructure that satisfies the CIA triad and the recording and regulating of data flow within and between the research team and other entities.8

The controller can instruct and appoint other entities that conduct processing on their behalf, titled the processor. It is the duty of the controller to use only processors that can provide sufficient guarantees that they implemented appropriate technical and organizational measures for the GDPR-compliant processing of the data. Such measures need to be taken and demonstrated in order to secure the processing and to protect data subjects' rights.[9] Naturally, researchers that act as controllers are therefore obliged to only use trustworthy processors that can demonstrate their compliance with the regulation.

If the data subject rights have been infringed, that is, personal data have been processed unlawfully, resulting in material or non-material damage, these data subjects can exercise their rights given under Art.16 – 23 GDPR (see section on Data Subject Rights). To this end, the controller is the "ultimate point of reference"[10] that the data subjects can contact to exercise their rights. Art. 82(1) GDPR states that under such circumstances data subjects have the right to receive compensation from the controller (or processor) for the damage. Additionally, controllers are liable for damage if they infringe upon the GDPR (Art. 82(2)). Recital 146 states that data subjects are to receive

---

[4] See Art.24(1) GDPR

[5] EDPS, "A preliminary Opinion on data protection and scientific research, 6 January 2020, p.17.

[6] EDPS, "Guidelines 07/2020 on the concepts of controller and processor in the GDPR", 2 September 2020, p. 8.

[7] D. Amram, "Building up the "*Accountable Ulysses" model*. The impact pf GDPR and national implementations, ethics, and health-data research: Comparative remarks"*, Computer Law and Security Review*, July 2020, Vol. 37, p. 2.

[8] Ibid, p. 6. The author of this article identifies additional features to consider to achieve an "acceptable level of compliance".

[9] EDPS, "Guidelines 07/2020 on the concepts of controller and processor in the GDPR", September 2020, p.4.

[10] See https://edps.europa.eu/sites/edp/files/publication/19-11-07_edps_guidelines_on_controller_processor_and_jc_reg_2018_1725_en.pdf p.13

effective and full compensation for the damages they have received and that "concept of damage should be broadly interpreted in the light of the case-law of the Court of Justice in a manner which fully reflects the objectives of this Regulation".

Checklist: You are likely to be a controller if you answer one of the following statements with "yes"

- You are gathering or using personal data for your own personal or research purposes.
- Even though another entity process personal data, you determine why those data should be processed.
- You decided what categories of personal data to gather exactly and from whom.
- Personal data you are planning to process are about your employees.
- You selected another entity, e.g., a different company or research organization, to process or analyze personal data for you.
- You are empowered to end up with processing of personal data

3.3 Joint Controllers

3.3.1 Who are these actors?

Joint Controllers are two or more controllers that are jointly determining the purposes and means of the processing of personal data. For such a joint controllership, specific rules are introduced in the GDPR to govern the relationship between the joint controllers.

3.3.2 What are their tasks?

The tasks are the same as those of a (single) controller but are performed by all joint controllers together.

3.3.3 When does a joint controllership occur?

A joint controllership occurs when a specific processing of data occurs whereby multiple controllers jointly determine the means and purpose of the processing. This means that multiple controllers decide together on the processing. Here, the EDPB distinguishes between **common decisions** and **converging decisions**.

- **Common decision**: Joint controllers decide together with a common intention on the means and purposes of the procession.
- **Converging decision**: **"***Decisions can be considered as converging on purposes and means if they complement each other and are necessary for the processing to take place in such manner that they have a tangible impact on the determination of the purposes and means of the processing."* [11] That means that the processing by each controller is linked to the processing of the other controller and would not be possible without it.

Joint controllership can also arise if one entity does not have access to personal data. Regarding the means of the processing, not every joint controller has to determine *all* means *all* the time. Different controllers can use different means at different stages in the processing of personal data. The same holds true for the purposes of the data. While a joint controllership occurs when the personal data is processed for the same purpose for all controllers, it can also occur if the purposes of different controllers are closely linked to each other or complementary. That means if the processing benefits all controllers and all controllers have agreed on the purposes and means, a joint controllership is formed.

However, the notion of joint controllership needs careful consideration and must be decided on a case-by-case basis. A clear overview on the relationship between all involved parties, as well as the flow of data is elementary to determine whether or not a joint controllership is taking place. The EDBP provides multiple examples in their guidelines on this issue. [12]

3.3.4 What are their rights and responsibilities?

The rights and responsibilities for joint controllers are defined in Art. 26(1-2) GDPR. Here, the joint controllers

> *"shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in* ***Articles 13*** *and* ***14****, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject. The arrangement may designate a contact point for data subjects"*

In order to do so, standard contracts between the joint controllers should be used to clearly determine which controller has exactly which responsibilities and tasks to perform. This includes to determine the purposes of the processing as well as the means

[11] EDPB. Guidelines 07/2020 on the concepts of controller and processor in the GDPR. Version 1. Adopted on 02 September 2020. Available under: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf p. 18. Last accessed 30.10.2020.

[12] Ibid. P.18ff for multiple examples for and against a joint controllership.

of the processing.[13] The data subjects should be provided with the contact information of one of the controllers to make it easier for them to determine who exactly to contact for issues regarding the processing of data. Additionally, the allocation of responsibilities and the essential results of the arrangement (the contract) between the joint controllers should be made available to the data subjects. For instance, a privacy notice for the data subject should include as an identification of the joint controllers and their tasks and responsibilities with the processing of data.

This clear allocation of responsibility and liability is stated in Recital 79 GDPR as a necessary condition for joint controllers. However, Art. 26(3) adds that the data subjects can address issues and exercise their rights against any of the joint controllers.[14]

Example 1:

Universities A, B and C decide to conduct a joint research project together. For this project, each university feeds personal data into a database that was provided by one of the universities for the joint research project. A, B and C then process the personal data in this database for their joint research project as they decided beforehand on the purposes and means for the processing. This means that in this research project, data is gathered in order to achieve a previously specified objective. The data is then analyzed using a specific, previously determined software solution. In this scenario, A, B and C are joint controllers as they determined the means and purposes of the processing together. Thus, all universities should determine, through contractual agreements, the rights, responsabilities of each party with respect to the data processing in a transparent manner.[15] Additionally, data subjects should always be sure which party they can and should contact in case that they have questions or if they would like to exercise their rights stipulated in the GDPR.

If a university A processes personal data in the database for another purpose than different of the joint research project, that university A becomes a separate controller for that particular purpose.

Example 2:

Company A is the parent company of a group of companies B, C and D. To store research data, the subsidiaries use a database hosted and provided by the parent company A.
Each company B, C and D can only access personal data that they themselves have fed into the database. Each company also processes the data for its own purposes only. In this scenario, no joint controllership exists. Companies B, C and D are separate controllers as they determine the purposes of their processing of the data. Company A is

[13] Ibid. p.3

[14] For more information on joint controllership see the guidelines of the EDPS: EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725, p.22ff

[15] For more information on Joint Controllership, see: EDPS, "EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725", November 2019, p. 16ff

seen as a processor as it provides a means of processing, the storing of personal data in their database.

3.4 Processors

3.4.1 Who are these actors?

A processor is defined under Art. 4(8) GDPR as a *"natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller"*. This demonstrates that a wide variety of entities can be considered a processor provided it is a **separate entity than the controller** and that the processing **is taking place on behalf of the controller**. Controllers may also process personal data themselves, of course. However, they will remain as controllers should they not only process personal data but determine the means and purposes of the processing as well.

3.4.2 What are their tasks?

The processor is processing personal data on behalf of the controller. The processor has to implement appropriate organizational and technical measures to ensure data protection. The processing itself can be both, a specific and detailed task or a more general processing. A controller therefore can also decide to only delegate a specific part of the processing to an external processor, and conduct parts of the processing itself.

The processing of personal data happens under the instructions of the controller. Therefore, personal data should not be processed in different manner than the one agreed upon with the controller.

A processor may appoint sub-processors but will need written consent by the controller for this. The sub-processor(s) should process the data on the same terms as the original processor.

3.4.3 What are their rights and responsibilities?

The processor acts under the instruction and terms of the controller. The processor is however allowed to use and choose, to a certain degree, the technical and organizational means that are deemed most suitable for the processing. This **level of influence**[16] of the processor is however not defined, meaning that the most secure option would be to agree by contract on a set of means between processor and controller. A distinction can also be made between essential (which data, from whom, how long, who should access it) and non-essential (practical, technical aspects of the processing) means of processing. The essential means are clearly to be provided by the controller as they are linked to the purposes of the processing. The non-essential means may be discussed by the processor in order to implement and execute the processing. However, as it has been discussed before, this issue has to be on a case-by-case basis.

[16] For more information on this level of competence and a distinction between essential and non-essential means see: EDBP. https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf p.14

With respect to the responsibilities, the processor has to provide *"sufficient guarantees"* (Art.28(1) GDPR) that the processing meets the requirements of the GDPR. These guarantees are essential as the controller has the duty to only use processors that can provide such guarantees and demonstrate GDPR compliance and the protection of data subjects. Art 28(3)(a-h) GDPR lists all the information that should be included in a written contract between processor and controller before any data is processed. That means that the processor must only act upon the controllers written instructions and guarantees data security and confidentiality as well as a documentation of all processing activities. Art.30(2) GDPR states that each processors needs to "maintain a record of all categories of processing activities carried out on behalf of a controller".

Example:

The research institution A has gathered a large database that contains personal data of data subjects through a questionnaire. Institution A assigns to data analytics company B task to analyze the data in order to find hidden relationships within the data. In this example, A acts as the controller as A determines the purposes and means of processing, while B acts as the processor that carries out the processing on behalf of the controller. Data analytics company B now decides to use the personal data for their own purposes, which have not been contractually agreed upon.

With this further processing of the personal data, B becomes a controller for this new type of processing. With these actions, B also infringes on the GDPR.[17] Consequently, institution B is in the situation to be imposed with administrative fine for any infringement of GDPR that might come out of new processing including possible personal data breach. Also, in that case, institution A bears no responsibility for mentioned incident. Institution A should have chosen a more suitable processor and should have obtained guarantees on the compliant processing of the data beforehand. Contractual agreements are used to clearly define roles, rights and obligations/responsibilities of all parties for the processing of the personal data.

3.5 Recipients

3.5.1 Who are these actors?

Art. 4(9) GDPR defines a recipient as *"a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not."*. However, public authorities that receive personal data through inquiries in accordance with the Union or member state law are explicitly excluded from this definition and are not to be regarded as third parties (Art. 4(9)(2) GDPR.

17 https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf p.25

Anyone else is considered a recipient by receiving personal data. Therefore, a processor or a third party, both discussed as main actors in this document, are regarded as a recipient if a controller transfers personal data to them.[18]

3.5.2 What are their tasks?

The recipient has no active part as it is defined only by access to the data. If an entity receives personal data and processes it, it naturally becomes a controller. This demonstrates that the type and roles of actor changes with the access and the processing of personal data.

3.5.3 What are their rights and responsibilities?

There are no special rights granted to recipients. As personal data is disclosed to a recipient, the controller has to inform the data subjects about the recipient. In case of rectification or erasure by the data subject's recipient have to be informed about such changes[19]. However, if recipients are controllers or processors themselves, they might be covered by the provisions of GDPR as a controller or processor, depending on the Regulation's territorial scope.

Example:

An individual uses an online food ordering and delivery service, company C, to order a meal. The company C that is offering the web interface is however not the restaurant that is producing the meal but acts on request of the individual by sending the order out to a restaurant and then delivering the food itself. Company C now distributes the personal data of the individual, name and address to a restaurant R. Both C and R are seen as controllers for the processing of the personal data that they carry out to offer their respective services. As C distributes the personal data, order information and address, to the restaurant R, R is seen as the recipient of the data. In this scenario, there is no controller-processor relationship.[20]

3.6 Third Party

3.6.1 Who are these actors?

Art. 4(10) defines a third party as *"a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the*

[18] See https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf p.29 for this example.

[19] Art. 19 GDPR Notification obligation regarding rectification or erasure of personal data or restriction of processing

[20] Example similar to the example on p.29 by the EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, 2020. Available under: https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf (Last accessed: 05.10.2021)

direct authority of the controller or processor, are authorized to process personal data." Employees that are not authorized to process personal data, which they obtained access to, are therefore defined as third parties.

Example:

A research organization, or a chair at a university, that is the controller of personal data, hires a cleaning service. Cleaning personnel may now technically access this personal data if they clean the desks of the organization on which the personal data might be stored. Even though the cleaning personnel does not, and does not want to, process the data, they may come in contact with the data. The cleaning service and its stuff are regarded as a third party. To be regarded as a controller, cleaning personnel in this example would for instance need to photograph or post the data on line. This would then count as processing the data, whereby the cleaning personnel becomes a controller. The organization, in its position as controller, must enforce technical and organizational measures to ensure that personal data cannot accessed by unauthorized persons – third parties. This includes the secure storage of the data in a such a way that other entities, here third parties, are not able to access the data, either involuntarily or on purpose.

3.7 Data Protection Officers (DPO)

3.7.1 Who are these actors?

The Data Protection Officer is a natural person that is professionally qualified to operate independently within an organization to ensure the application of the GDPR in that organization. DPOs therefore ensure the correct processing of personal data within a company, be it the personal data of its staff, its customers or other data subjects. Art. 37(1) GDPR lists circumstances in which and entities that are to appoint a DPO, such as public authorities that process data or instances where data subjects need to be monitored regularly. Art. 37 GDPR further states that a DPO should provide the professional qualities to fulfill its tasks and that DPOs contact details are to be provided to the supervisory authority. Subsequently, all EU institutions and bodies have an appointed DPO.[21] The EDPS states that a DPO should be "… an expert on data protection law and practices, and be in a position to operate independently within the organization." [22]

3.7.2 What are their tasks?

It is the task of a DPO to ensure that the rights of data subjects, such as the staff, customers or other individuals, are protected by ensuring the correct application of the GDPR in an organization. The DPO should keep a record of the processing that is performed or controlled in that organization.

[21] A list of the DPOs in EU institutions and bodies can be found here: "Network of DPOs", https://edps.europa.eu/node/53 (last visited: 02.12.2020)

[22] https://edps.europa.eu/data-protection/data-protection/glossary/d_en (last visited: 02.12.2020)

Furthermore, the DPO needs to ensure that controllers and data subjects know about their rights and responsibilities. This includes raising awareness on the GDPR and advising the controller on how best to implement it within the organization. This is done to create accountability for possible violations.

Should complaints or violations arise, the DPO has to handle such complaints and cooperate with the EDPS on how best to address them. Additionally, it is the task of the DPO to draw attention of the organization to any failure in complying with the GDPR.

3.7.3 What are their rights and responsibilities?

It is the responsibility of a DPO to ensure compliance with the GDPR when processing personal data. DPOs are responsible for ensuring that the rights of data subjects, e.g., Art. 12 – 23 GDPR such as the right of access and right to rectification, are not infringed upon. To do this, DPOs need to keep a register of the processing operations that are controlled or performed within their organization.

In order to fulfil the tasks mentioned above, DPOs should be provided with additional rights within their organization. DPOs should not be in a conflict of interest, which means that DPOs should not also be a processor or controller of data. DPOs should not be employees on a short contract and should not have to report to a direct superior as these circumstances could prevent a DPO from doing their job effectively. Instead, DPOs should be able to conduct their work independently and should report directly to the top-level management. Furthermore, DPOs should be responsible for managing their own budget and should receive the resources and staff they need to perform their work.[23] This includes having the authority to investigate independently within an organization or a research project.

3.8 Supervisory Authorities

3.8.1 Who are these actors?

The supervisory authority is an independent public authority established by the member states of the EU. Laws are only effective if compliance is supervised and violations are sanctioned. For this reason, the GDPR constitutes independent supervisory authorities in its Chapter 6. Less formally, they are also called Data Protection Authorities or DPAs. DPAs are part of the executive branch of government and work independently in order to be able to supervise other governmental agencies.

3.8.2 What are their tasks?

Supervisory authorities or DPAs are responsible for monitoring and enforcing the application of the GDPR. Furthermore, they shall promote public awareness and understanding in issues regarding data processing. They also aim to promote awareness about the obligations of controllers and processors of personal data under the GDPR.

[23] https://edps.europa.eu/data-protection/data-protection/reference-library/data-protection-officer-dpo_en

The supervisory authority is one of the contact persons for data subjects to lodge a complaint regarding malpractices and is entitled to conduct investigations in such malpractices. The supervisory authority also sets the criteria for certification of demonstrating compliance.

The precise tasks of supervisory authorities are regulated in Art. 57 GDPR. The following subset of the 22 tasks listed in Art. 57(1) shall provide a general idea:

- Monitor and enforce the GDPR.
- Promote awareness of data protection-related rights and obligation to data subjects, the public, controllers, and processors.
- Handle complaints lodged by data subjects.
- Conduct investigations.
- Adopt, authorize, or approve different kinds of contractual clauses, provisions, or binding corporate rules.

In order to enforce the GDPR, supervisory authorities have "corrective powers" (Art. 58(2) GDPR) that range from simple warnings, over administrative fines, up to imposing a ban on processing.

3.8.3 What are their rights and responsibilities?

The supervisory authority is responsible for enforcing the correct application of the GDPR in processing of personal data. To do so supervisory authority should act independently in exercising their powers, including powers of investigation, corrective powers and sanctions, power to impose a temporary or definitive limitation, including a ban, on processing, as well as imposing administrative fines. In particular each measure should be appropriate, necessary and proportionate in view of ensuring compliance with GDPR. EU member state have to ensure that the supervisory authority is provided with enough financial, human and technical resources.

3.8.4 Does every Member State have a Supervisory Authority?

"*Each Member State shall provide for one or more independent public [supervisory] authorities to be responsible for monitoring the application of [the GDPR].*" (Art. 51(1) GDPR)).

In practice, this means that some Member States have a single national supervisory authority, while others have several. For instance, France has a single supervisory authority called Commission nationale de l'informatique et des libertés (CNIL)[24]. Germany on the other hand has multiple supervisory authorities. They are all **at the same level** but are responsible and competent for different kinds of processing activities: processing activities by federal agencies and certain specific kinds of processing fall under the responsibility of the federal commissioner for data protection and freedom of information (BfDI)[25]; competence of other public and private processing

[24] https://www.cnil.fr/
[25] https://www.bfdi.bund.de

activities are subdivided geographically by federal state (Bundesland); specific data protection authorities by churches are responsible for processing activities of churches.

3.8.5 Can I appeal decisions by the supervisory authority? What is the highest court of appeal?

The decisions of a supervisory authority can be appealed in court (Art. 78 GDPR). This is typically done in a national administrative court. The decision of this first instance can be appealed in higher level courts up to the national supreme court. Beyond that, the highest judicial authority is the European Court of Justice.

Note that there is no mechanism for controllers or processors to appeal a decision by a supervisory authority of a member state at the European Data Protection Board.

3.9 European Data Protection Board (EDPB)

3.9.1 Who is the actor?

The European Data Protection Board (EDPB[26]) is a *"body of the Union" with "legal personality*" established based on Art. 68 GDPR. It is composed of a supervisory authority of each member state plus the EDPS (The European Data Protection Supervisor, which will be introduced later on). The EDPB replaced the Article 29 Data Protection Working Party (WP29) when the GDPR came into effect. In doing so, it has also endorsed some of the guideline's opinions of the working party[27].

The EDPB is responsible for a significant number of tasks that are listed in Art. 70 GDPR. These tasks include, but are not limited to, issuing guidelines, opinions, recommendations and best practices on the application of the GDPR, advising the European Commission on matters regarding the GDPR and promote the exchange of knowledge and information between different supervisory authorities.

Most importantly, the EDPB is concerned with the consistent application and interpretation of the GDPR in all Member States. According to Art. 65(1) GDPR, the EDPB shall adopt binding decisions should a lead supervisory authority not follow an opinion provided by the EDPB or if there exist conflicting views on the application of the GDPR by different supervisory authorities.[28] Such instances trigger *"**Consistency Mechanism**"* by which the EDPB may issue opinions on how the GDPR is to be applied across multiple member states. If the supervisory authorities of these member states fail to respect an opinion by the EDPB, the EDPB can make binding decisions, which have to be respected by the supervisory authorities, in order to solve disputes[29].

---

[26] For more information on the EDPB, please visit the official EU-website: https://edpb.europa.eu/about-edpb/about-edpb_en

[27] The European Data Protection Board, (EDPB), Endorsement 1/2018, https://edpb.europa.eu/sites/edpb/files/files/news/endorsement_of_wp29_documents_en_0.pdf (last visited 24.11.2020).

[28] Art. 65(1) GDPR "Dispute resolution by the Board"

[29] See "Consistency Findings", EDPB available at https://edpb.europa.eu/our-work-tools/consistency-findings_en (last visited 25.11.2020)

3.9.2 What are its tasks?

The EDPB is assigned to advise the European Commission on issues related to personal data protection and on the format and procedures for information exchange between controller, processors and supervisory authorities as well as on certification. In addition, it promotes the cooperation and effective bilateral and multilateral exchange of information and best practices between supervisory authorities. It issues guidelines, recommendations and best practices and examine any questions regarding these or the GDPR. Accreditation of certification bodies and their periodical review is done by the EDPB. Furthermore, it draws up an annual report on protection of natural persons, processing in the Union, third countries and international organizations.

3.9.3 What are its rights and responsibilities?

The EDPB acts independently when performing its tasks.

To fulfil its tasks, the EDPB can publish and establish binding decisions, opinions and guidelines. For instance, the EDPB endorsed the guidance by WP29, for instance on consent, transparency and many more[30], and published additional guidance[31]. As stated before, the EDPB can issue opinions and binding decisions on the application of the GDPR in member states.

3.10 European Data Protection Supervisors (EDPS)

3.10.1 Who are these actors?

The European Data Protection Supervisor (EDPS[32]) is the supervisory authority for processing activities by European institutions and bodies. It is an independent supervisory authority of the European Union. In contrast to the other actors the EDPS is not established by the GDPR but by Regulation (EU) No 2018/1725.

3.10.2 What are their tasks?

The tasks of the EDPS are to monitor and protect personal data when it is processed by EU institutions and advises other EU institutions on matters regarding such processing as well as related legislation and acts. Furthermore, it monitors technologies that could influence data protection and cooperates with the national supervisory authorities on data protection. Furthermore, the EDPS advises EU institutions such as the European Commission on affairs regarding data processing, such as new legislation and

[30] Endorsement 1/2018, EDPB, available at https://edpb.europa.eu/sites/edpb/files/files/news/endorsement_of_wp29_documents_en_0.pdf (last visited: 25.11.2020)

[31] See "GDPR: Guidelines, Recommendations, Best Practices", https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en for a list of guidelines and recommendations provided by the EDPB

[32] For more information on the EDPS, please visit the official EU-website: https://edps.europa.eu/about-edps_en. (Last visited 30.10.2020)

agreements. It also monitors new technologies that might impact data protection and cooperates with national supervisory authorities.[33]

3.10.3 What are their rights and responsibilities?

The EDPS can conduct investigations on the application of data protection. Therefore, it can order controllers and processors to provide information or conduct protection audits. Furthermore, the EDPS can issue warnings if infringements are likely or reprimands if infringements are ascertained and orders specific measures to handle infringements. In addition, it can impose fines for the unlawful processing of data or ban the processing altogether.

DOs

- Check what kind of actor or role you or your organization constitute when working with personal data under the GDPR. Every actor has specific rights and responsibilities.
- Ensure you know what kind of actor other entities are that you are working with. This may differ, depending on the flow of data between different entities and organizations.
- Understand the tasks, rights and responsibilities that each actor possesses when working with personal data.
- Ensure that contracts are being used to define the roles, responsibilities and tasks of different organizations that relate to the processing of personal data.
- Consult additional literature such as the EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725 and the Guidelines 07/2020 on the concepts of controller and processor in the GDPR.

[33] Ibid.