EUROPEAN DATA PROTECTION SUPERVISOR

[NV: Only for EU institutions and bodies]

EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725

7 November 2019

Executive Summary

When processing personal data, **EU institutions and bodies (EUIs) must comply with specific data protection rules**. Depending on their role, their obligations differ. **The following guidelines provide explanation and practical advice to EU institutions and bodies on how to comply with Regulation (EU) 2018/1725** ('the Regulation').

Following the entry into force of the General Data Protection Regulation (the GDPR) and Regulation 2018/1725, many questions were raised on the changes to the concepts of controller, processor and 'joint controllership', and particularly on their respective roles and responsibilities. **These guidelines aim at providing practical advice and instructions to EUIs to comply with Regulation 2018/1725 by providing specific guidance on the concepts of controller, processor and joint controllership based on the definitions provided in the Regulation.** EUIs will have more clarity on the role these may assume for specific processing operations and their implications in terms of obligations and responsibilities under the Regulation.

While these guidelines are aimed at the Data Protection Officers, Data Protection Coordinators and all persons having responsibility within the EUIs for the processing operations of personal data, other external organisations might equally find them useful.

The guidelines focus on:

- the concepts of controller, processor and joint controllership;

-the distribution of their obligations and responsibilities, in particular when dealing with the exercise of the rights of data subjects;

-specific case studies on controller-processor, separate controllership and joint controllership situations.

The identification and assessment of whether EUIs may be considered as controllers, processors or joint controllers, together with their respective duties are presented in flowcharts and checklists.

These guidelines will also be useful to senior management in supporting a culture of data protection from the top of the organisation and to implement the principle of accountability.

The purpose of the guidelines is to make it easier for EUIs to fulfil their obligations. Under the accountability principle, EUIs remain responsible for compliance with their obligations.

TABLE OF CONTENTS

1. Introduction

Following the entry into force of the General Data Protection Regulation[1] ("the GDPR") and of Regulation (EU) 2018/1725[2] ("the Regulation"), many questions were raised on the changes to the concepts of controller and processor and their respective roles, and in particular to the implications of the concept of 'joint controllership' (as laid down in Article 28 of the Regulation).

When processing personal data, EU institutions and bodies (hereinafter "EUI" or "EUIs") must comply with specific data protection rules. Depending on their role, their obligations differ. The following guidelines aim to provide practical advice to EUIs on how to comply with the Regulation by providing explanation on the concepts of controller, processor and joint controllership based on the definitions provided in the Regulation. We hope to bring more clarity on the role these may assume for specific processing operations and their implications in terms of obligations under the Regulation.

As the independent supervisory authority competent for the processing of personal data by EUIs, the EDPS may, among other tasks, issue guidelines on specific aspects related to the processing of personal data.

These guidelines should be considered by Data Protection Officers (DPOs) and Data Protection Coordinators or Contacts (DPCs) and by all persons having responsibility for the EUIs acting as controllers, processors or joint controllers. They will also be useful to senior management in supporting a culture of data protection from the top of the organisation and to implementing the principle of accountability.

The purpose of the guidelines is to make it easier for EUIs to fulfil their obligations. Under the accountability principle, EUIs remain responsible for compliance with their obligations. EUIs may choose alternative, equally effective, measures other than the ones presented in this paper taking into account their specific needs. In such a case, they will need to demonstrate how they plan to obtain equivalent protection via these alternative measures.

2. Scope and structure of the Guidelines

2.1 Scope of the Guidelines

This document provides EUIs with guidance on the concepts of controller, processor and joint controllership in order provide further clarity on their role when processing personal data, thus identifying their responsibilities and complying with the Regulation.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), L119/1.

[2] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, L295/39.

It also focuses on providing examples of the concepts through additional case studies and checklists, in order to explain the Regulation in a practical way.

The guidelines address, in particular:

- The concepts of 'controller', 'processor' and 'joint controllership' in line with legislation and case law;
- The distribution of their obligations and responsibilities, in particular when dealing with the exercise of data subject rights;
- Specific case studies on controller-processor, separate controllership and joint controllership situations.

The following information is provided in the annexes to support the guidance:

- A flowchart indicating whether your institution or body may be considered as a controller, processor or joint controller;
- Checklists on the duties of controllers and processors.

This document does not consider/focus on:

- Template clauses for controller-processor contracts or joint controllers agreements - the EDPS will publish separate guidance on this;
- Safeguards for extra-EU/EEA transfers - the EDPS will publish separate guidance on this.

This document is also without prejudice to any update that may be needed in the light of forthcoming EU data protection legislation, case law and specific guidance concerning the concepts at issue and their implications in relation to responsibilities and liability.

2.2 Structure of the Guidelines

The guidelines are structured as follows:

- Chapter 1 introduces the purpose of the guidelines.
- Chapter 2 defines the scope and the structure of the document.
- Chapter 3 explains the concept of 'controller', defines its roles and responsibilities, then presents some case studies;
- Chapter 4 explains the concept of 'processor, defines its roles and responsibilities, then presents some case studies;

- Chapter 5 explains the concept of ‘joint controllership, defines its roles and responsibilities, then presents some case studies.

- Annex 1 presents a chart setting out how to identify whether your institution is a controller, processor or a joint controller;

- Annex 2 presents a checklist detailing the duties of a controller;

- Annex 3 presents a checklist outlining the duties of a processor.

3. The concept of 'controller'

Article 3(8) of the Regulation defines a 'controller' as "(…) *the Union institution or body or the directorate-general or any other organisational entity which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by a specific Union act, the controller or the specific criteria for its nomination can be provided for by Union law".*

Similarly as in Article 4(7) of the GDPR, the 'controller' is identified by five elements, which will be analysed separately in this Chapter. The GDPR defines the 'controller' in slightly different terms as the "*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 (...)*". However, both definitions are essentially functional: the entity that decides on the "what" and "how" of the processing will be the controller, independently of its organisational status.

3.1 The definition of 'controller'

3.1.1 'The Union institution or body or the directorate-general or any other organisational entity'

The first part of the definition refers to **the type of actors that can be controllers in line with the Regulation, i.e. EU institutions, bodies, a directorate-general or any other organisational entity**. This element underlines the fact that any of the institutions, agencies, bodies or directorates-general (i.e. organisational entities commonly found within most of the largest EUIs) can be considered as a 'controller' for the carrying out of specific processing operations.

Therefore, it is clear that **directorates-general and other organisational entities may assume the role of controllers (and joint controllers**, as will be assessed in Chapter 5 of the guidelines).

3.1.2 'Determines'

The second element of the concept of controllership refers to the **factual influence that the controller has over the processing operation**, by virtue of an exercise of decision-making power.[3]

How can this be assessed in practice? In order to evaluate the 'factual influence' of a controller over the processing operation, the entirety of the factual elements should be evaluated, by answering the questions **'*why is the processing taking place*'**, **'*who initiated the processing*'**[4] and **'*who benefits from the processing*'**[5].

[3] See Working Party 29 Opinion 1/2010 on the concepts of "controller" and "processor", p.9.
[4] See Working Party 29 Opinion 1/2010 on the concepts of "controller" and "processor", p.8.
[5] See 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.
Case C-40/17 Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV ECLI:EU:C:2019:629 paras. 78 -81 and Opinion of Advocate General Bobek in case C-40/17, *Fashion ID*. paras. 68-70.

Such control can derive:

a) From explicit legal competence

Article 3(8) of the Regulation states: "(...) *where the purposes and means of such processing are determined by a specific Union act, the controller or the specific criteria for its nomination can be provided for by Union law*". Where the EU legislator has explicitly designated the controller in a specific EU legal act, establishing the controller should in principle be a straightforward task.

The EDPS recommends identifying the controller of specific processing operation(s) already in the basic legislative act, in order for the determination of the controller to be clarified from the beginning and to avoid any possible problem of interpretation in assessing the role[6].

- An example of such explicit competence provided by law can be found in Article 57 and 58 of the ETIAS Regulation, according to which the roles of controller and processor of the processing of personal data are expressly established.[7]

b) From implicit competence

In the absence of explicit competence, **the responsibility of a party as a controller can be identified by implicit competence**. In this case, the role as controller is not explicitly laid down in the law. However, if a party is assigned a specific task that requires it to carry out certain duties that imply the processing of personal data, the role of controller would ultimately result from such tasks and duties assigned to that party.

- An example of such role established by implicit competence is the Regulation establishing EMA[8]: while that Regulation does not explicitly designate EMA as 'controller' for specific (sets of) processing operations, it assigns specific tasks and related duties. In order to fulfil these tasks (such as managing certain databases), the agency needs to process personal data, also entailing responsibilities from a data protection point of view. This is a clear indication that the entity in question is a 'controller'.

In the absence of explicit or implicit competences, the responsibility and the role of the party can be established by assessing the factual circumstances in which the entity operates in the context of a specific processing operation[9].

[6] Of course, such a determination must be aligned with the actual responsibilities assigned to the various actors by the legislative act.
[7] Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226, Articles 57 and 58.
[8] Regulation (EC) No 726/2004 of the European Parliament and of the Council of 31 March 2004 laying down Union procedures for the authorisation and supervision of medicinal products for human and veterinary use and establishing a European Medicines Agency, OJ L 136, 30.4.2004, p. 1–33, e.g. Article 24.
[9] Since EU institutions and bodies are most likely to have their role established by explicit or implicit competence, these guidelines will not assess this part into details. See WP29 Opinion 1/2010 on the concepts of "controller" and "processor", pp. 11 and 12.

3.1.3 'Purposes and means'

The third element of the definition relates to the essence of the controller's influence, namely the determination of the purposes and means of the processing operation. **The identification of the '*why*' and the '*how*' of a processing operation is the decisive factor for an entity to assume the role of 'controller' within the meaning of data protection law**. When carrying out of a processing operation, **the controller is the one deciding on the purpose ('*why*') and on the means to carry out such processing operation ('*how*')**[10].

In this perspective, the degree of influence of a party in determining both purpose and means may identify its role as a controller. It is worth underlining that, although **purposes and means** are linked, it is not necessary for a party to equally determine both to be considered as a controller of the processing of personal data: in fact, this also depends on the specific context in which the processing operation would be taking place.

Therefore, the crucial question is to **what level of detail** a party should determine the purposes and means in order to be considered as a data controller.

When assessing the **determination of the purpose,** the actor determining the reason for which a certain processing would take place, i.e. *'what for'* it would be carried out, is the controller within the meaning of data protection law. In other words, a controller is **the entity that *de facto* decides on the purpose ('*why*') of a processing operation.**

Concerning the **determination of the means**, the term includes different elements, and particularly refers to the technical and organisational measures that are put in place when carrying out a specific processing operation. However, **the determination of the means to be used for a specific processing operation only entails the role of controllership if the party decides on the essential elements of the means.**[11] According to the approach adopted by the Working Party 29 in its opinion, examples of such 'essential elements of the means' include: the type(s) of data to be processed, the period for which they would be retained, from which data subjects would the data be collected, who will have access to data (access control lists, user profiles etc.) and the recipients of data etc., these usually being reserved to the controller's determination.

As for the determination of **more practical aspects of the processing operation(s), the so-called 'non-essential elements of the means'**, in the same opinion, the Working Party 29 considers these to be the hardware or software to be used or the technical security measures. It may well be possible that these may be identified and determined by the data processor, to the extent this is carried out following the general instructions of the data controller. The role of the processor will be further detailed in the next chapter.

As a result, **the determination of the purpose is exclusively reserved to the controller of a processing operation**. On the other hand, the controller is **only required to determine the**

[10] See Case C-210/16 Wirtschaftsakademie Schleswig-Holstein ECLI:EU:C:2018:388 paras. 34-36, as well as Opinion of Advocate General Bot in *Wirtschaftsakademie*, para. 46 and following.
[11] See WP29 Opinion 1/2010 on the concepts of "controller" and "processor" "(...) *while determining the purpose of the processing would in any case trigger the qualification as controller, determining the means would imply control only when the determination concerns the essential elements of the means*.", p.14.

'essential elements' of the means of the processing operations. It is possible that a processor, while acting in the controller's interest, may identify the non-essential means of the processing operations, such as the software to be used or the technical and organisational measures that may need to be put in place, therefore assisting the controller in complying with its obligations under data protection law[12].

EXAMPLE:

In line with the powers laid down in its founding Regulation, OLAF decides to start an investigation on suspected fraud in an EUI and requests the latter to provide specific information concerning a case of fraud (which typically contains personal data). The Institution is therefore obliged to comply but wonders whether it qualifies as joint controller within the meaning of Article 28 of the Regulation.

What matters for the existence of a situation of joint controllership is the joint establishment of the purpose and means of the processing operations. If the parties involved do not jointly determine the same general objective (or purpose) or do not base their processing operations on jointly determined means, their relationship seems to be pointing to a 'separate controllership' situation**.**

In this specific case, it is evident that the two institutions do not jointly determine the purpose of the processing operation in place. The Institution/Agency/Body processes personal data for a specific purpose, e.g. a procurement procedure. This does not coincide with the purpose of OLAF's processing operations, i.e. investigating suspected fraud. Moreover, each of the parties involved processes personal data independently from the means used by the other controller.

Therefore, this situation points to a situation of separate controllership.

An entity does not need to have access to personal data to be considered a controller. It is enough if it determines the purposes and means of processing, has influence on the processing by causing the processing of personal data to start (and being able to make it stop), or receives the anonymous statistics based on personal data collected and processed by another entity[13].

[12] See e.g. obligations on controllers in the Regulation, Articles 26, 27 and 33.

[13] In this regards, see Case C-25/17 Jehovan todistajat ECLI:EU:C:2018, paraS. 68 to 72, as well as Case C-210/16 Wirtschaftsakademie Schleswig-Holstein and Case C-40/17 FashionID & Co.KG v Verbraucherzentrale NRW eV. Furthermore, it is not necessary that the controller distinguish in its processing the personal data and other types of information. In this regards, see pars. 28 and 41 of the judgement in Case C-131/12 Google Spain, where the court considers that:
- the search engines do not distinguish between personal data and other types of information it collects, indexes and stores and that
- the processing of information by search engines is a processing of personal data, when that information contains personal data.
If an actor determines purposes and means of a processing but at the same time the processing does not involve any personal data at all at any of the stages of processing, then the same actor may not be considered as a controller under data protection law.

3.1.4 'Alone or jointly with others'

Article 3(8) of the Regulation (same as Article 4(7) of the GDPR) **identifies the possibility for the purpose and means of a specific processing operation to be determined by more than one actor**. This specification, makes it explicitly clear that the concept of controllership does not necessarily refer to one single entity, but can also involve multiple parties playing a role in a processing operation. As a result, and as confirmed by the CJEU, each of the actors involved have obligations under data protection law[14]. Chapter 5 of the guidelines assesses the situation of 'joint controllership' in detail[15].

3.1.5 'Of the processing of personal data'

According to Article 3(3) of the Regulation "*processing means any operation or set of operations which is performed on personal data or on sets of personal data (…)*". This means that **one or a set of processing operations may be linked to the concept of controllership**. According to a literal interpretation of the Regulation, each action (collection, storage, analysis, disclosure etc.) is a distinct processing operation. In practice, processing operations are grouped in sets of processing operations that serve a defined purpose. Controllers have a certain margin of appreciation in defining the boundaries of sets of processing operations.

For example, controllers could see the recruitment and on-boarding process for new staff (for the EUIs meaning e.g. determination of rights under Staff Regulations, badge for physical access, access to IT resources, publication of info on intranet etc.) as one integrated set of processing operations, or split it into different sets of operations. As a rule of thumb, controllers should look at it from the data subjects' perspective: does it appear as an integrated process to them? For example, splitting appraisal procedures and the appeals in two would appear to be too narrow an approach, while grouping all HR management processes in one would be too broad.

The exercise of control by a specific actor may apply to the entire processing, but may also be limited to one of its specific operations[16].

EXAMPLE:

An EUI decides to outsource the guarding of its premises to an external company. That company manages its own staff - the EUI is not involved in scheduling etc. - it just requires that defined numbers of guards are present at defined checkpoints. Do the two parties qualify as joint controllers for the processing of personal data of the security guards for HR management by the outsourcing company, such as performance evaluation? Would the situation change, if the EUI also entrusted the external company with registering visitors to the premises?

[14] See Case C-210/16 Wirtschaftsakademie Schleswig-Holstein, para. 29.

[15] As an additional specification, if an EUI may need to enter into a specific arrangement with international organisations and given the fact that these rely on a special status, one may adopt an administrative arrangement. As this would necessarily fall within the scope of **data transfers**, Article 48(3)(b) of the Regulation specifies that, *the appropriate safeguards (...) may also be provided for, in particular, by (...) contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation (...)*".

[16] In relation to this, see AG Bobek's Opinion in the Fashion ID case, para. 99.

It is clear that both the purpose and the means to carry out the security guards' processing of personal data are not jointly determined by the parties involved, as these are autonomously defined by the external provider. Therefore, the parties do not jointly determine the purpose and means of the processing operations in relation to the HR management staff within the external company (the security guards). They would thus qualify as separate controllers of different operations within the overall processing of guarding of the EUI premises.

However, when processing the personal data of visitors to the Institution's premises, the external company would be acting on behalf of the Institution's instructions. In other words, the external provider would have to provide guarantees to implement technical and organisational means, based on the controller's requirements, thus acting as a processor for the Institution within the meaning of Article 29 of the Regulation. This does not affect the external company's role as a separate controller with regard to managing its own staff.

3.2 Obligations and liability of the controller

Article 26(1) of the Regulation provides that "[*t]aking into account the nature, scope, context and purpose of the processing as well as the risks varying likelihood and severity of the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation*". Moreover, Article 26(2) stipulates that "(…) *the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller*". It is thus clear that **the primary responsibility for ensuring compliance lies with the controller**. **In light of the principle of accountability, controllers are thus under a general obligation to demonstrate compliance with the Regulation**.

Article 65 of the Regulation states that "[*A]ny person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the Union institution or body for the damage suffered, subject to the conditions provided by the Treaties*".

However, in contrast to Article 82 of the GDPR, the Regulation does not specifically provide for liability of the controller (or processor) in case of non-compliance, but instead refers to the conditions provided by the Treaties.

Article 340 of the Treaty on the Functioning of the European Union (TFEU) states that 'in accordance with general principles common to the laws of the Member States, the Union shall make good any damage caused by its institutions'. Additionally, in accordance with data protection legislation, a controller is liable towards the data subject for total damage, this being both material or non-material (Article 65 the Regulation[17]). In line with Article 268 TFEU, the Court of Justice of the European Union shall have jurisdiction in disputes relating to compensation for damages relating to Article 340 TFEU.

[17] See also Article 82 of the GDPR.

3.3 Protection of data subjects

Under the Regulation (Articles 4(2) and 14(1) and 14 (2)), it is responsibility of the controller to ensure that data subjects can exercise the rights afforded to them by Articles 17 to 24 of the Regulation. Even if another entity is appointed as a point of contact for data subjects, **the controller of the processing operation remains the ultimate point of reference for this obligation.** The most recent case law of the CJEU confirms that the concept of controller has been defined broadly so that data subjects may be ensured effective and complete protection by avoiding any possible lack of responsibility in that regard[18].

3.4 When is an EUI a controller? A checklist

Summing up this chapter, when can an EUI be considered as a controller within the meaning of the Regulation? The following checklist may help EUIs to identify the most relevant elements based on which an entity may be identified as a controller. If the majority of the responses to the statements is YES, your EUI is likely to be a controller for a specific set of processing operations within the meaning of the Regulation.

	YES	NO
• You have decided to process personal data or caused that another entity processes it.		
• You decided what purpose or outcome the processing operation needs to have.		
• You decided on the essential elements of the processing operation, i.e. what personal data should be collected, about which individuals, the data retention period, who has access to the data, recipients etc.		
• The data subjects of your processing operations are your employees.		
• You exercise professional judgement in the processing of the personal data.		
• You have a direct relationship with the data subjects.		
• You have autonomy and independence (within the tasks assigned to you as a public institution) as to how the personal data is processed.		
• You have appointed a processor to carry out processing activities on your behalf, even if the entity chosen for that purpose implements specific technical and organisational means (non-essential elements).		

It is worth bearing in mind bearing in mind/remembering that for EUIs, in most cases, controllership would be defined by EU legislation either because it is specifically provided for

[18] Case C-131/12 Google Spain SL e Google Inc. v Agencia Española de Protección de Datos (AEPD) e Mario Costeja González ECLI:EU:C:2014:317 para. 34. See also Case C-210/16 Wirtschaftskademie Schleswig-Holstein paras. 27-28 and Case C-25/17 Jehovan todistajat para. 66.

or because the EUI would be assigned a specific obligation or permission to process data under a legislative act.

4. The concept of 'processor'

Article 3(12) of the Regulation defines a 'processor' as "(…) *a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller".*

Identical to the wording in Article 4(8) of the GDPR, the definition of 'processor' is identified by two elements, which will be analysed separately in the present Chapter.

4.1 The definition of 'processor'

4.1.1 A natural or legal person, public authority, agency or other body

As in the GDPR, the **definition of 'processor' involves a diverse range of actors, these being natural or legal person, public authorities, agencies or other bodies**[19]. The existence of a processor depends on a decision taken by the controller, who may decide to perform certain processing operations itself or delegate all or part of the processing to a processor.

Article 3(12) of the Regulation does not specifically list Directorates General as processors within the meaning of data protection law. It is thus clear, from a legal point of view and vis-a-vis the data subjects, that the EUI is responsible or liable as a processor for any non-compliance with the Regulation. However, it must be noted that, in specific Institutions, certain EU Directorates General act as 'support DGs', often carrying out processing operations under strict instructions and on behalf of other DGs (who are the owners of the business process). This would **not** normally be the situation for corporate wide processing operations, but rather for specific operations only belonging to one particular DG or unit. Moreover, this is reinforced by the existence of Service Level Agreements or other working agreements between Directorates General, which set out the governance process and the division of tasks and responsibilities between the different organisational entities involved in the processing.

In order to ensure an effective allocation of responsibilities and to ensure a better level of protection of natural persons in compliance with data protection legislation, the EDPS recommends identifying in internal agreements the roles and responsibilities of such DGs.

Internal agreements within an institution do not need to be as detailed as the ones with external processors, as long as responsibilities are defined. Such clear allocation of tasks and responsibilities between the different organisational entities involved in the processing is also in line with the need to fully ensure compliance with data protection rules and that the level of protection of natural persons guaranteed by the Regulation is not undermined by lack of clarity as to responsibilities.

[19] 'Other body' meaning 'any other entity' within the meaning of the GDPR, rather than Union body.

EXAMPLE:

In an EUI, one DG is only responsible for the development and technical management of an IT tool that another Directorate-General uses. The user Directorate-General defines the requirements for the IT tool. What would be the role of the DG developing the IT tool?

As explained above, a DG developing, running and maintaining an IT tool for other DGs performs a role that is very similar to that of a processor. This DG should not define the purposes or the essential elements of the means of the processing - the IT tool (e.g. the retention periods, the access to the data and the data recipients).[20] This does not prevent the service DG from suggesting means, as long as it is the controller DG who decides.

Additionally, and as in the case of a controller, the Regulation also provides for the possibility to designate a processor in a specific Union legal act:

- See e.g. Article 58(1) of Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226.[21]

4.1.2 On behalf of the controller

The essence of the role of a 'processor' is that **personal data is processed on behalf of the data controller**. In practice, it is the controller who determines the purpose (within the limits of the tasks assigned by legislation) and the essential elements of the means, while the processor has an implementing role. **In other words, 'acting on behalf of the controller' signifies that the processor is serving the controller's interest in carrying out a specific task and that it is thus following the instructions set out by the controller, at least with regards to the purpose and the essential elements of the means.**

The primary duty of compliance stands with the controller. However, it is important to recognise that the processor is not necessarily the controller's 'subordinate'. The fact that the processor acts 'on behalf of the controller' does not necessarily undermine its independence in carrying out specific tasks assigned to it. The processor may enjoy a considerable degree of autonomy in providing its services and may identify the non-essential elements of the processing operation.

For example, an agency or body providing investigation services and acting on behalf of another EUI (and thus having established working procedures in place), under a specific contract or another legal act, is entitled to maintain its operational and organisational independence in carrying out its core tasks as the nature of its mandate requires a certain degree

[20] If this were to be the case, then the entities would be joint controllers.

[21] OJ L 236, 19.9.2018, p. 1–71. *"Article 58* **Data processor:** eu-LISA is to be considered a processor in accordance with point (e) of Article 2 of Regulation (EC) No 45/2001 in relation to the processing of personal data in the ETIAS Information System."

of independence. However, this is due to the controller choosing to give that operational independence to the processor. It is up to the two parties involved to agree on the acceptance of the established procedures and on the roles and modalities in which certain processing operations are put in place. The processor may advise or propose certain measures (in particular in its field of expertise) but it is up to the controller to decide whether to accept such advice or proposal, after having been fully informed of the reasons for the measures, what the measures are and how they would be implemented. In other words, for an organisation to act 'on behalf' of a controller and thus be identified as a processor, it is not necessary that the controller 'imposes' the entire modalities according to which a certain processing operation should be carried out.

However, when **a processor acts beyond the mandate by infringing the contract or another legal act or making decisions about the purpose and the essential elements of the means of a specific processing operation, it may qualify as a controller (or a joint controller)**.

In practice, it is possible that the processor could go beyond its role i.e. by acting outside of the agreement or making decisions about the purpose and the essential elements of the means of a specific processing operation. Whether such situation means that a processor should automatically be classified as controller (with all of the responsibilities it entails) would depend *inter alia* on the scope of the deviation, for example when such behaviour serves to ensure compliance with data protection principles. However, if the processor further reuses data for its own purposes, clearly overstepping the general governance and purposes set out in the agreement with the controller, this would result in a clear breach of its obligations.

EXAMPLES:

1**. A Directive creates a voluntary Network of responsible authorities for a specific topic designated by Member States. The Directive also provides for Institution A to work as the Network's Secretariat. One of the main objectives of the Network is to enhance interoperability between national IT systems related to this field by exchanging personal data. In order to facilitate such exchanges, the Network has decided to set up an IT tool, designed and implemented by Institution A. Upon request of the contact points of national Member States, personal data is transferred to one or more Member States. The type of data to be exchanged within the interoperable IT tool is decided by the guidelines adopted by the Network and by the use of specific arrangements between the Member States' contact points. Institution A, in its role of the Network's Secretariat, is not involved in the decision-making process regarding the shaping and the functions of the system as such, but exclusively provides advice regarding the technical and legal feasibility of the option chosen.**

In line with the case's description, the purpose of the processing of personal data within the interoperability IT tool is set out in the Directive. Moreover, the same Directive also establishes Institution A as the Network's Secretariat. The decisions on the types of data to be exchanged and on the system to be used are provided by guidelines adopted by the Network and by specific agreements between contact points of the national Member States. Let us also assume that a further Implementing Act provides for specific roles of Institution A, these being the duties to manage and ensure the security of the IT tool, together with the duty to provide

the controllers with the information necessary to demonstrate compliance with their obligations.

In line with the description made so far, the IT platform through which personal data is exchanged is in fact a means of communication between Member States' databases. Given the legal framework related to the definition of the purposes and means of the infrastructure, and given the strict limitations of Institution A's tasks to ensure the security of the core services of the interoperable IT tool platform, Institution A may be considered as a processor acting on behalf of the Member States in this example.

4.2 The choice of the processor by the controller

Article 29(1) of the Regulation provides that "(...) *the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the data subject*". This **obliges the controller to assess whether the guarantees offered by the processor are sufficient. In light of the accountability principle, the controller should be able to prove it has taken all of the elements provided in the Regulation into serious consideration.**

The controller may take into account whether the processor provides **adequate documentation** proving such compliance, such as privacy policies, records management policies, information security policies, external audit reports, certifications etc. **The controller should take into account the processor's expert knowledge (e.g. technical expertise when dealing with data breaches and security measures), reliability and its resources.** Only if the controller can demonstrate that the processor is suitable, it can then enter into an arrangement that meets the requirements of Article 29 of the Regulation. Notwithstanding this, the controller must still comply with the accountability principle and regularly check on the processor's compliance and measures in use.

Before outsourcing the processing and in order to avoid any potential issues, **the controller should conclude a contract, another legal act or binding arrangement with the other entity already setting out clear and precise data protection obligations**.

Therefore, the EDPS wishes to address the following recommendations to EUIs:

- Only use processors providing sufficient guarantees to implement appropriate technical and organisational measures that the processing will meet the requirements of the Regulation and ensure the protection of the rights of the data subjects.
- Ensure that the processor does not further outsource/subcontract without the controller's prior written authorisation;
- Make sure that the processor keeps the controller informed of any changes, giving the opportunity to object;
- Sign a written contract or another (binding) legal arrangement with the processor with specific data protection clauses;
- Ensure that the same contractual obligations are passed on to any subcontractor chosen;

- In case of processors subject to the GDPR, that these provide for GDPR compliance as one of the elements to be used to demonstrate sufficient guarantees.

Following the recommendations and the assessment of the possible processor and in line with Article 29 of the Regulation**, the controller enters into a binding agreement with the processor, who must comply with the same obligations set out in the Regulation and the GDPR.**

The processor must only process personal data on the documented instructions of the controller, unless required to do so by Union or Member State law. The processor also has the obligation to assist the controller:

- with the controller's obligation to guarantee the rights of data subjects and;
- to fulfil the controller's obligations pursuant to Articles 33-41 of the Regulation (security and data breach notification, data protection impact assessment and prior consultation, confidentiality of electronic communications, information and consultation of EDPS).

The controller must therefore set out clear modalities for such assistance and give the processor precise instructions how to fulfil them, for example in the contract or another (binding) arrangement.

For example, when the processor is the only entity who may be able in practice to grant the exercise of data subjects' rights, it is expected to provide the controller with all of the information in order for the controller to reply to the data subject. Moreover, as the controller and the processor are aware of their respective responsibilities and have agreed on them through a specific contract, another legal act or binding arrangement, it may also be possible for the controller to transmit any request to the processor, where this is the only entity to grant rights to the data subject. We recommend that in the agreement in place between controllers and processors, the two parties agree on the modalities to be used in order to grant data subjects the full exercise of their rights, and that such modalities be reflected in the data protection notice to be provided to data subjects.

On controller-processor contracts, including standard contractual clauses, the EDPS will release further guidance.

4.3 The liability of the processor and the exercise of data subject rights

Compared to the previous data protection legal framework, the Regulation (Recitals 45, 50 and Article 29) [22] **strengthens the responsibilities of the processor.**

However, notwithstanding its obligations, Article 29 of the Regulation seems to suggest that **the processor's liability remains more limited in scope compared to the controller's liability**. In other words, while controllers can in principle be held liable for damages arising from any infringement related to the processing of personal data (including those committed

[22] As for the GDPR see Recitals 79 and 146; and Art. 82.

by the processor) or breach of contract or another (binding) arrangement, the processor may be held liable when it has acted outside the mandate given by the controller, or if it has not complied with its own obligations under the Regulation[23]. The processor can be held entirely or partially liable for the 'part' of the processing operation in which it is involved[24]. It may be held fully liable only when it is entirely responsible for the incurred damage.

Can **a processor following specific instructions given by the controller** be held liable for following such instructions? Articles 29(3) and (4) of the Regulation set out the obligation of the processor in relation to the agreement to be made with the controller. In practice, a processor carrying out specific processing operations under strict instructions given by the controller, would not be held liable for any infringement of the Regulation when strictly following the controller's instructions[25]. However, if the processor is found to have acted beyond the instructions and mandate given by the controller, it may be held liable for the infringement of the Regulation and/or damage or if it concerns a breach of the processor's obligations. It should also be noted that where the controller is an EUI and the processor an external actor, the latter will fall both under the Regulation (in particular for fulfilling the conditions under Article 29 of the Regulation), and the GDPR (for its internal organisation and compliance requirements).

In line with Article 29(1) of the Regulation, **vis-à-vis the data subject**, the controller carries the main responsibility for the processing operation and may be held liable for damages. However, the data subject may still hold the processor liable if it has specific reasons to believe the infringement, which resulted in damage to him or her, was made by the processor.

4.4 When is an EUI a processor? A checklist

In line with what has been discussed in the present chapter, when can an EUI be considered as a processor within the meaning of the Regulation? The following checklist is intended to help EUIs to identify the most relevant elements on the basis of which an entity may be identified as a processor. If the majority of the responses to the statements is YES, your EUI is likely to be a processor for a specific set of processing operations within the meaning of the Regulation

	YES	NO
• You follow instructions from another party with regard to the processing of personal data.		
• You do not decide to collect personal data from individuals.		
• You do not decide on the legal basis for the collection and use of that data.		

[23] Numerous articles in the Regulation set out obligations of processors, not just Article 29.
[24] E.g., a data breach happened at the data centre of the processor, because the processor did not implement appropriate security measures. However the controller did not check what, if any, security measures are in place and whether they are appropriate to mitigate the risks. They are both responsible for the data breach and both liable for the incurred damage.
[25] This is without prejudice to liability for any simultaneous infringements by the processor of any of its own obligations.

• You do not decide the purpose or purposes for which the data will be used.		
• You do not decide whether to disclose the data, or to whom.		
• You do not decide the data retention period.		
• You make certain decisions on how data is processed, but implement such decisions under a contract or another legal act or binding arrangement with the controller.		
• You are not interested in the end result of the processing.		

5. The concept of 'joint controllership'

The distinction between the concepts of 'controller' and 'processor' does not cover all the possible relationships. It may happen that more actors share the controller's responsibilities. As stated in Opinion 1/2010 of the Article 29 Working Party "(...) *Article 2.b of the Directive does not exclude the possibility that different actors are involved in different operations upon personal data*"[26].

The concept of joint controllership had already been envisaged in the definition of 'controller' under Article 2 (d) of Regulation 45/2001. Accordingly, Article 2(d) of Directive 95/46/EC had identified the notion of joint controller within the broader definition of 'controller'. Similarly, Article 26 of the GDPR states that where two or more controllers determine the purposes and means of the processing, they shall be joint controllers. Therefore, **'joint controllership' is not a new concept**.

Article 28(1) of the Regulation provides that *"[w]here two or more controllers or one or more controllers together with one or more controllers other than Union institutions and bodies jointly determine the purposes and means of the processing, they shall be jointly controllers. (...)".*

What does this mean in practice?

The following chapter aims at addressing two general questions: when does a situation of joint controllership occur and what are the joint controllers' obligations? Additionally, it will focus on the data subject rights and the liability of the parties within a joint controllership situation. Below, we will issue some guidance by identifying the elements that may be useful in assessing a situation of joint controllership.

5.1 When does a situation of joint controllership occur and what are its decisive elements?

The crucial element of the definition provided in Article 28(1) of the Regulation is that controllers "*jointly determine the purposes and means of processing".* The following chapter will discuss the consequences of the definition and will address the possible interpretation problems it entails.

Firstly, Article 28(1) clarifies that such situation may happen not only between two or more controllers in EUIs. Joint controllership may also occur between an EUI and an external actor (such as an external provider of a management portal or a national public authority etc.). Therefore, it is essential to keep in mind that a situation of joint controllership can indeed occur between an EUI and one or more external actors bound by GDPR[27]. In this case, **the obligations stemming from Article 28 of the Regulation fully apply**.

[26] See WP29 Opinion 1/2010 on the concepts of "controller" and "processor, p.18.
[27] Or Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, L 119/89.

An EUI may be in joint controllership situations together with an entity subject to the GDPR. For example, EUIs, in carrying out their tasks in the public interest, may be joint controllers together with Member State authorities (as also further clarified in the case studies).

However, the EDPS encourages EUIs making use of services provided by private companies to make sure that such private companies only act as processors for such processing operations. While EUIs are able to use outsourcing services when delivering the tasks assigned to them by law in the public interest, it would not be appropriate for a private party to exercise the kind of influence that would result in them being a joint controller.

- An example would be the use of an IT service provider by an Institution or body. In that circumstance, the EUI should indeed aim at deciding on the purpose and essential elements of the processing operation, thus keeping control of the processing operation in place, and only delegating the non-essential elements of the processing to the service provider.

Secondly, the notion of joint determination should be understood as any situation where each controller has a chance/right to determine purposes and essential elements of the means of a processing operation. It means that, before entering into a specific agreement with one or more parties, each controller is aware of the general purpose and (essential elements of) the means of processing. In other words, just **by entering into such agreement, the parties commonly determine (or converge on) the purpose and essential elements of the means to carry out a processing operation: this, in itself, is sufficient to trigger a situation of joint controllership.**

Thirdly, both the purposes and (the essential elements of) the means of the processing operation need to be determined. Chapter 2 of the guidelines explained the notion of means and purposes[28].

In sum, a '**general' level of complementarity and unity of purpose could already trigger a situation of joint controllership, if the purposes and (essential elements of the) means of the processing operation are jointly determined[29].**

Some situations regularly raise doubts regarding the existence of a joint controllership situation.

- It has been argued that not having access to personal data within the context of a processing operation is sufficient to exclude a situation of joint controllership. However, the CJEU in Case C-201/16 *Wirtschaftsakademie* (based on Directive 95/46/EC[30]), found that the Directive "(...) *does not, where several operators are jointly responsible for the same processing, require each of them to have access to the*

[28] Opinion of AG Bobek in the Fashion ID case, C-40/17, para.105. This has been confirmed by the CJEU in Case C-40/17 Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV judgment.
[29] Case C-40/17 Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV, para.85.
[30] There appears to be no reason why this would have been decided differently under the Regulation or GDPR.

personal data concerned."[31] Additionally, in the *Jehovah's Witnesses* case, the CJEU confirmed this approach by defining the parties involved in door-to-door preaching activities as joint controllers "(...) *without it being necessary that the community has access to those data* (...)".[32]

These judgments underline that what matters for the existence of a situation of joint controllership is the determination of the purpose and (essential elements of the) means of the processing operations. The fact that a party only has access to information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable, as was the case in *Wirtschaftsakademie*, does not influence the joint controllership situation. However, this may nonetheless matter when establishing the degree of responsibility of the parties involved.

In practice, it may be difficult to distinguish a situation of joint controllership from one in which two controllers act separately. In fact, multiple controllers may interact in various operations of the processing, without necessarily sharing all purposes and means as such.

It is clear that, **if the parties involved do not jointly determine or converge on the same general objective (or purpose) or do not base their processing operations on jointly determined (essential elements of the) means, their relationship seems to be pointing to a 'separate controllership' situation.**

- For example, EUIs usually have CCTV cameras in place for maintaining the premises' security. In case of an incident, which may need investigation by national law enforcement authorities, it may be necessary to transfer the CCTV data to the investigative authorities. In such case, the two parties involved do not jointly determine the purpose and means for the processing. As a consequence, they are not joint controllers.

EXAMPLES:

1. Two or more Directorates-General decided on the development of an IT application for the management of research projects, including their programming, calls, assessment, attribution and signature of contracts, payments and information on on-going contracts. Would the two DGs be considered as joint controllers?

Based on the definition of controller provided in Article 3(8) of the Regulation, two or more Directorates-Generals (DGs) using the same IT application for managing research projects can be internally considered as joint controllers within the EUI since the purpose and the application have been commonly decided and designed for the management of research projects, selection of their own experts and grant beneficiaries.

As already defined above in the controller-processor scenarios, the DG developing and maintaining the IT application, is the processor, executing the instructions of the other DGs.

[31] Case C-210/16 Wirtschaftskademie Schleswig-Holstein, para. 38.
[32] Case C-25/17 Jehovan todistajat, paras. 69 and 75. This has been reiterated in Case C-40/17 Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV, para. 69.

In practice, some EUIs use the notions of "internal controller" (or "controller in practice") and "internal processor" for departments or entities within the EUI to help with clarifications of internal responsibilities.

In case other EU bodies, such as executive or other type of EU agencies or joint undertakings, use the abovementioned IT tool to manage the research projects delegated to them, what would be the role of these EU bodies? The EDPS, in its joint prior checking opinions on management of experts and on grant management in the Participant Portal, has already found that this is a case of joint controllership between the Commission and the agencies and bodies using the Participant Portal.[33]

2. A web-based application is developed in support of a Network of Member States virtual contact points in order to share information and medical research on rare and complex diseases within the EU territory. The network was set up under a Directive and the same legislation mandates Institution A to support the network, through the adoption of delegated and implementing acts. This software allows the exchange of information between healthcare providers in Europe and contains the medical data of patients with rare diseases. Institution A has set up and manages the application, which has been developed by a subcontractor. This platform will thus contain medical data of patients with rare diseases in a central repository. Institution A decides on the categories of personal data processed on the platform, while the national healthcare process the data outside the platform's use with the purpose of using the system. Would it matter if the Institution A did not have access to the central repository?

Both Institution A and the healthcare providers jointly determine the purpose and the means of the application. Institution A is mandated by law to define the technical and non-technical measures that may be put in place for the processing operations of patients' data within the platform. It also set up and manages the platform itself. On the other hand, and in compliance with the jointly determined purpose and means, the national healthcare providers also process health data of patients at national level for the purpose of using the system, thus also taking care of informing the patients and guaranteeing their rights.

Both Institution A and the national healthcare providers jointly determine the purpose and means of the processing operations, thus acting as joint controllers within the meaning of Article 28 of The Regulation. What matters is "jointly defining" the purposes and means - even if Institution A did not have access itself, it would still remain a joint controller because of its role in defining the system.

3. A Regulation establishes an information system for designated MS authorities to share information, including personal data, using a central repository run by an EU Agency to facilitate cross-border recognition of decisions in a certain policy area. The same Regulation specifically assigns some tasks to the different stakeholders involved: the EU Agency will be responsible for information security in the central repository and for providing some analyses of the data in the system. The MS authorities feeding the data into the system are responsible for the correctness of the data. The Agency and the MS

[33] Joint Prior-checking Opinion regarding Grants Award and Management in the in the Participant Portal (under H2020 ÏT tools) in a number of European Union institutions - EDPS cases: C-2017-1080 REA, C- 2017-1076 SESAR, C-2017-1037 INEA, C- 2017-1068 CHAFEA, C-2017-0977 EASME and C-2017-1070 EIT.

authorities decide on the further development of the system in a steering committee. The Regulation is silent on who would inform data subjects.

It is clear that neither of the parties involved in the processing operations would be able to achieve the purpose independently. Furthermore, the parties themselves jointly develop the means. Therefore, as the purpose and means of the processing operations are jointly determined by the parties, it is evident that this appears to be a situation of joint controllership. The establishing Regulation does not specifically provide for which of the parties will inform data subjects on the processing of personal data in place: this is something for the joint controllers to decide in their arrangement. In this specific case, it would make sense to have the national authorities inform data subjects about the processing of personal data in the European database when issuing their decisions and communicating them to data subjects.

5.2 What are the obligations of joint controllers?

A situation of joint controllership entails specific obligations for the parties involved. Article 28(1) of the Regulation provides that joint controllers *"(..) shall in a transparent manner determine their respective responsibilities for compliance with their data protection obligations, in particular as regards the exercising of the rights of the data subject (...), by means of an arrangement between them unless, and in so far as, the respective responsibilities of the joint controllers are determined by Union or Member State law to which the controllers are subject (...)".*

While the scope of the joint controllership's obligations is broad, recital 50 of the Regulation also puts the '**clear allocation of the responsibilities' as a *sine qua non* condition for the *protection of the rights and freedoms of data subjects***. The data subjects focussed perspective is also underlined by Article 28, which mentions in particular the rules on exercising data subjects' rights and on the right to information. The fundamental right approach of the Regulation is also visible in the specific possibility for the joint controllers to establish a single contact point to facilitate the exercise of data subject rights.

5.2.1 The responsibilities of joint controllers

The first obligation is thus to define the responsibilities for compliance with data protection obligations, similar to the responsibilities of a controller as provided by the Regulation.

Therefore, where two or more parties act as joint controllers, they will need to clearly identify and define their respective responsibilities for specific obligations under the Regulation. In this context, it is important to remember that the **Regulation does not oblige joint controllers to share their responsibilities equally**. In relation to the parties' responsibility, the CJEU in *Wirtschaftsakademie* clarifies that "(…) *the existence of joint responsibility does not necessarily imply equal responsibility of the various operators involved in the processing of personal data. On the contrary, those operators may be involved at different stages of that processing of personal data and to different degrees, so that the level of responsibility of each*

of them must be assessed with regard to all the relevant circumstances of the particular case".[34]

Therefore, **the parties involved in the processing operations should assess their roles and responsibilities taking into account the different stages in which they operate**.

However, a clear allocation of responsibilities may not always be immediately apparent. Thus, it is necessary to carry out a case-by-case assessment in order to identify the obligations incumbent on each and every joint controller. A clear understanding of who does what will help to assign responsibilities in a way that makes sense - if e.g. some of the joint controllers will interact with data subjects, while others will not, it makes sense to assign responsibilities for informing data subjects and dealing with request to the former.

In case one of the joint controllers (or both) decides to engage a processor, how does this affect the situation of joint controllership and the responsibilities in place? In short, it does not: the fact that one of the joint controllers chooses to have some processing operations performed by a processor does not affect its own obligations as a joint controller. In practice**, joint controllers may want to create specific procedures for using processors in the arrangement between the joint controllers.** These procedures could stipulate that if one of the parties decides to engage a processor, it should consult the other controller(s) on the part of the processing to be entrusted to a processor and on the aspects of the contract to be put in place with a processor. Only once this has been agreed upon between the joint controllers, should the controller engaging the processor enter into a specific contract with the processor.

5.2.2 The arrangement between joint controllers

J**oint controllers have to enter into a specific arrangement**, laying down their roles and responsibilities, in particular towards the data subjects. This is an obligation under Article 28 of the Regulation, unless and insofar as a law already determines these roles and responsibilities.

In some cases, these roles and responsibilities are (partially) already determined by law, e.g. in the establishing act for an information system. In fact, Article 28 of the Regulation confirms that **EU legislation can directly provide for an allocation of roles and responsibilities between the parties**. Where this is the case, there is no obligation to conclude an arrangement insofar as the respective responsibilities of the joint controllers are determined by Union or Member State law. Consequently, a clear allocation of responsibilities should be made in the operative part of the relevant legislative act (or - regarding Union law - at the latest in an implementing or delegated act, where provided for in the basic act).

The EDPS strongly recommends to provide for a clear allocation of responsibilities in the relevant legislative acts, in order to ensure a clear distribution of tasks between joint controllers.

[34] Case C-210/16 Wirtschaftskademie Schleswig-Holstein, para. 43; Case C-25/17 Jehovan todistajat, para.66.; Case C-40/17 Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV, paras. 70 and 85.

When the roles and responsibilities of joint controllers are only partially determined by law, the arrangement needs to fill any gaps that remain.

Unless Union law **already allocates their responsibilities, the joint controllers need to enter into a specific arrangement**, **containing a clear and transparent allocation of responsibilities**. Such arrangement may take the form of a Memorandum of Understanding (hereinafter MoU) or a contract. A Service Level Agreement (hereinafter SLA) may be used in addition to the MoU as providing technical specifications. Furthermore, an SLA may be considered sufficient as an arrangement between joint controllers as long as this contains all of the elements in line with the Regulation.

Making sure that all parties involved share a clear understanding of their respective tasks is not only important in the field of data protection, but also in terms of good administration in general[35]: it ensures that queries arrive to the right people and helps to keep EUIs accountable.

Therefore, after having delineated the different possibilities leading to the necessity of entering into a specific arrangement (and unless provided by the law itself) it is essential to emphasise that the arrangements:

- Should be discussed and agreed by ALL joint controllers;
- Cannot be unilaterally adopted by one EUI;
- Should cover only the relevant processing operations and have a clearly defined scope (especially when it concerns a process that interfaces with other processes that the joint controllers may have in place);
- Should cover the subject-matter, duration, nature and purpose of the processing operations;
- Should cover the categories of personal data and data subjects involved in the processing operations.

Concerning the **substance of the arrangements**, these should at least cover the following points:

- The respective responsibilities, roles and relationships, so that the lawfulness, fairness and proportionality of the processing operations in place may be identified;
- The respective duties of the joint controllers to provide information referred to in Articles 15 and 16 of the Regulation (Art 28(1);

[35] See the right to good administration under Article 41 of the Charter as well as The European Code of Good Administrative Behaviour.

- The responsibilities for information security, including the reporting of personal data breaches;
- A contact point for data subjects requests;
- Cooperation between joint controllers for the reply to data subjects requests and as regards the exercise of other rights of the data subjects;
- Cooperation between joint controllers when carrying out DPIAs[36];
- Possible processor(s) engaged by one (or more) of the controllers.

In practice, such a written arrangement is the legal instrument establishing the relationship between the different parties involved in the joint controllership. In line with Article 31(1)(a) of the Regulation a reference to the joint controllership should be made in the public part of the record of the processing activities. We additionally recommend linking the MoU, or any other instrument used, to the internal part of the record.

5.2.3 Informing data subjects about the essence of the arrangement

Pursuant to Article 28(2) of the Regulation "[*T]he essence of the arrangement shall be made available to the data subject*".

This provision underlines the importance of identifying the roles and responsibilities between joint controllers in order, first and foremost, for data subjects to be able to understand clearly the division of responsibilities and whom to address first. **This information should be provided to data subjects through the data protection notice**. Each of the controllers may have a separate data protection notice. However, joint controllers may also coordinate on a common data protection notice to be provided to data subjects. In line with Articles 15(4) and 16(5)(a) of the Regulation, it is sufficient to inform data subjects through a data protection notice once. The arrangement may also assign the task of informing data subjects to one of the joint controllers.

EXAMPLE:

An EU Agency decides to organise an event on a specific topic with another institution. They decide to allocate their tasks and responsibilities, in particular about the processing of personal data of participants to the event.

It is clear that the overall purpose is jointly determined by the parties involved. The fact that the responsibilities and tasks may differ in relation to the carrying out of the processing operations in place does not influence the joint determination of the general purpose.

[36] When carrying out a Data Protection Impact Assessment (hereinafter DPIA), in case of a joint controllership situation, the controllers should agree on a common methodology and jointly carry out a DPIA. In the likely event that the controllers may not be involved during the same stages of the processing operation in place, the parties may agree on a common methodology but still carry out a separate DPIA for the specific stage of the processing operation during which these are involved.

Additionally, also the means can be considered as jointly determined, as the two parties involved agree on how these are used within the context of the event organisation and the processing of personal data of the participants. Although a party would carry out specific individual tasks (such as keeping a mailing list, access control etc.), such steps are in place simply because of an overarching jointly determined purpose (the event organisation as such). It is therefore evident that the parties involved are joint controllers within the meaning of Article 28 of the Regulation. Moreover, in the agreement that the parties put in place, the exercise of data subjects' rights will clearly be dealt with, specifically with reference to cooperation obligations between them when dealing with such requests. Such cooperation obligations, for example, may provide for a set contact point to which data subjects can address their requests.

5.3 What does a situation of joint controllership mean for the exercise of data subject rights?

The essence of the arrangement needs to be made available to data subjects so that they understand clearly the roles and responsibilities of the joint controllers. The Regulation, as the GDPR, goes one step further and provides that "*[I]rrespective of the terms of the arrangement (...), the data subject may exercise his or her rights under this Regulation in respect of and against each of the controllers".*[37] In other words, the terms of the arrangement may not limit data subjects from exercising their rights under the Regulation, specifically regulated under Chapter III (such as the rights of access and rights to rectification, to erasure, to data portability and to object to the data processing).

However, in case of an arrangement in place between the joint controllers providing for specific roles and responsibilities, in practice it may be complex for both (or more) parties to grant a full exercise of the data subjects' rights. It is, in fact, very much likely that the set roles and responsibilities may not allow the joint controllers the same means of granting data subjects the exercise of their rights within the meaning of the Regulation (such as the right of access, erasure or restriction). In relation to this, **if the roles and responsibilities are defined in the arrangement between joint controllers, this should also include cooperation obligations between them for dealing with such data subject requests**. Such cooperation obligations, for example, may provide for a set contact point to which data subjects could address their requests, such as a common email address. In practice, the modalities on the general responsibilities should be contained in the arrangement, while the details on the concrete instructions may be set out in the underlying documents.

Therefore, it is essential to **make sure that a data subject may always contact each joint controller to request access, erasure or restriction**. In order for such rights to be exercised, determining the exact roles and responsibilities between joint controllers is thus fundamental for the adequate organisation of the exercise of their rights.

[37] The Regulation, Article 28(3).

Notwithstanding the possibility for data subjects to direct their requests to each joint controller, the EDPS recommends to establish a single contact point to which data subjects may forward their requests in exercising their rights.

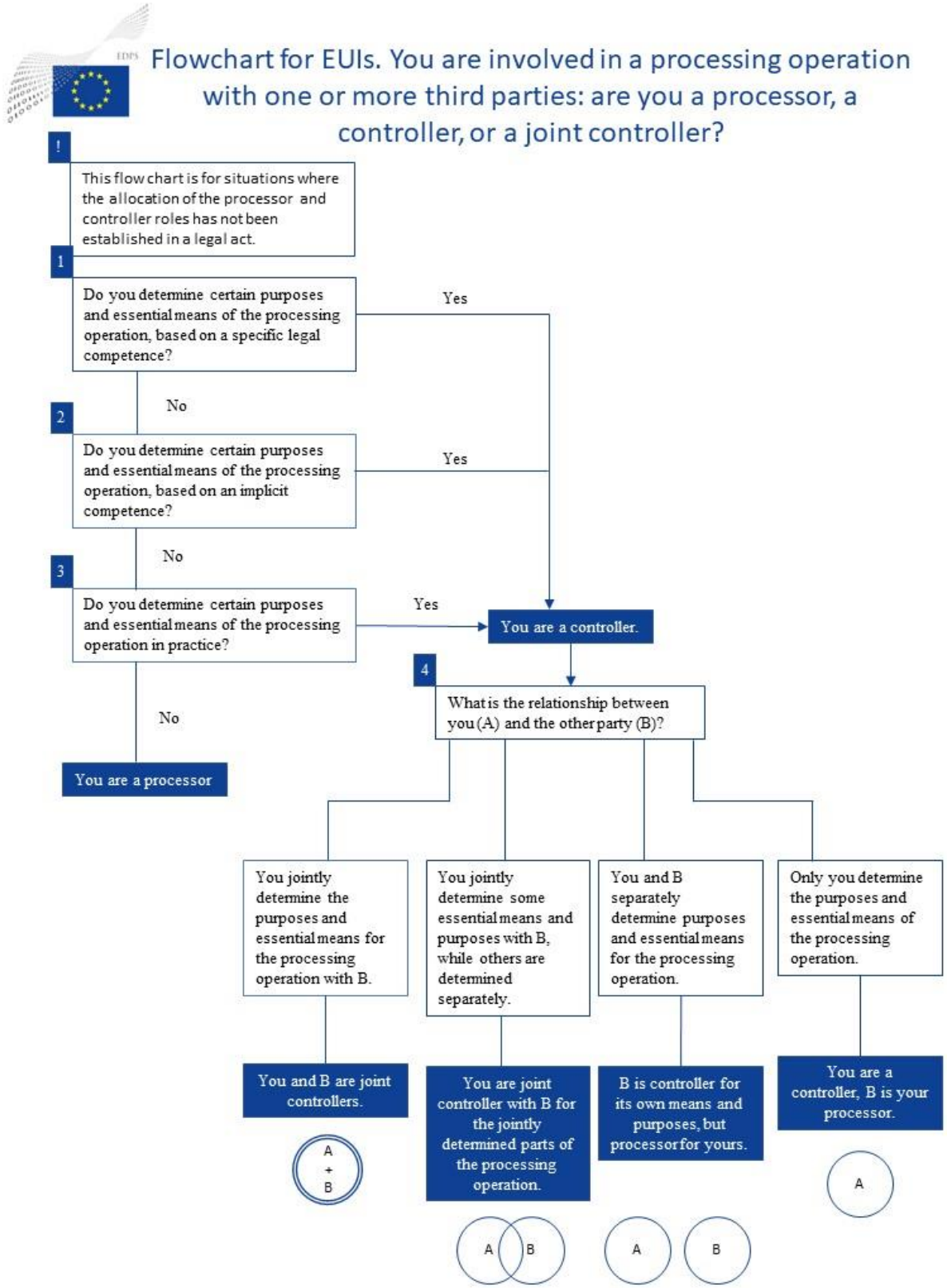
5.4 What are the liabilities of the parties involved in a joint controllership?

Article 65 of the Regulation provides for the right to compensation. It states that any person who has suffered any specific material or non-material damage deriving from an infringement of the Regulation has the right to receive compensation from the EUI for the damage suffered "*(...) subject to the conditions provided for in the Treaties*". When referring to such conditions, Article 340 second paragraph of the Treaty on the Functioning of the European Union (TFEU) provides that "*[I]n the case of non-contractual liability, the Union shall, in accordance with the general principles common to the laws of the Member States, make good any damage cause by its institutions or by its servants in the performance of their duties*".[38]

The Regulation does not specifically deal with non-compliance liability, unlike Articles 26 and 82 of the GDPR. Article 340 of the TFEU refers to the 'general principles common to the laws of the Member States'. As already mentioned in the chapter on controllership, Article 268 TFEU provides that the Court of Justice of the European Union shall have jurisdiction in disputes relating to compensation for damages relating to Article 340 TFEU. Therefore, the principles for the parties' liability in a joint controllership differ from the GDPR regime.

[38] TFEU, Article 340 Para. 2.

6. Annex 1



Note: The aim of this flowchart is to clarify the initial qualification as controller or processor, rather than setting out what happens when a processor exceeds its mandate/role by becoming involved in determining essential means of the processing.

7. Annex 2

Checklist 1: What are the duties of the controller?

Processing of personal data needs to adhere to the following principles:

- the processing operation should be lawful, fair and transparent ("**lawfulness**", "**fairness**", "**transparency**");
- the processing operation should be bound to specific purposes ("**purpose limitation**");
- the personal data processed should be adequate, relevant and limited to what is necessary ("**data minimisation**");
- the personal data should be accurate ("**accuracy**");
- the personal data should be kept no longer than necessary ("**storage limitation**");
- the personal data needs to remain well secured and confidential ("**integrity and confidentiality**").

See the EDPS "accountability on the ground" guidance, part I pages 20-22, as well as part II, pages 11-15, for guiding questions on these data protection principles.

The controller is responsible for compliance with these principles and should be able to demonstrate this compliance ("principle of accountability"). To achieve this, controllers in practice need to, in particular:

- document their processing operations with **records**
  (note: the EDPS strongly recommends keeping these records in a **central and publicly accessible register**);
- carry out a data protection impact assessment (**DPIA**), prior to operations which carry a high risk to the rights and freedoms of data subjects;
- under certain circumstances, **consult the EDPS** prior to such high-risk processing operations;
- when designing processing operations, keep in mind the principles of "**privacy by design**" and "**privacy by default**";
- take **adequate security measures** in order to protect personal data;
- in case of a **personal data breach**, notify the EDPS as well as, under certain circumstances, the data subjects involved;
- conclude **agreements / contracts with processors** (only those providing sufficient guarantees);
- conclude agreements with other controllers in cases of **joint controllership**;
- **transfer** personal data within the EUI, to other EUIs, to third countries or international organisations only when the conditions of the Regulation are complied with;
- **cooperate with the EDPS**.

See the EDPS accountability on the ground for guidance on records, DPIAs, prior consultation and more.

Finally, the controller needs to provide **clear and accessible information to data subjects** about the processing, **respect data subject rights** and ensure their availability in practice.

See the EDPS guidelines on transparency and other rights and obligations.

8. Annex 3

Checklist 2: What are the duties of the processor?

In order to comply with the Regulation, processors must in particular:

- only process personal data on the **documented instructions of the controller**, unless required to do so by Union or Member State law;
- process personal data as **governed by a contract or legal act** which is binding on the processor and that sets out the necessary prerequisites for the processing activity;
- **NOT further process** data for other incompatible purposes;
- **assist the controller** with the obligation to guarantee the **rights of data subjects** and to fulfil the controllers **obligations pursuant to Articles 33-41** of the Regulation (security and data breach notification, data protection impact assessment and prior consultation, confidentiality of electronic communications, information and consultation of EDPS);
- **notify** any legally binding **request for disclosure** of the personal data processed on behalf of the controller and may only give access to data with the prior written authorisation of the controller
- **ONLY outsource/subcontract with the prior written authorisation** of the controller; inform controller of any changes, giving controller the opportunity to object; pass on same contractual obligations to any subcontractors;
- **maintain a record** of all categories of processing activities carried out on behalf of the controller;
- take **adequate security measures** in order to protect the personal data;
- without undue delay, inform the controller of a **data breach**;
- **cooperate**, on request, with the EDPS in the performance of his or her tasks.

Brussels, 7 November 2019

Wojciech Wiewiórowski

European Data Protection Assistant Supervisor