~~ARTICLE 29 DATA PROTECTION WORKING PARTY~~

~~00264/10/EN WP 169~~

REDLINE (unofficial)

made by **Christopher Schmidt, CIPP/E CIPM CIPT CDPO**

~~Opinion 1/2010 on the concepts of "controller" and "processor"~~

Guidelines 07/2020 on the concepts of controller and processor in the GDPR

Version 1.0

Adopted on ~~16 February 2010~~02 September 2020

EXECUTIVE SUMMARY

The ~~concept of data~~concepts of controller, joint controller and ~~its interaction with the concept of data~~ processor play a crucial role in the application of ~~Directive 95/46/EC~~the General Data Protection Regulation 2016/679 (GDPR), since they determine who shall be responsible for compliance with different data protection rules, and how data subjects can exercise their rights~~, which is the applicable national law and how effective Data Protection Authorities can operate.~~ in practice. The precise meaning of these concepts and the criteria for their correct interpretation must be sufficiently clear and consistent throughout the European Economic Area (EEA).

~~Organisational differentiation in the public and in the private sector, the development of ICT as well as the globalisation of data processing, increase complexity in the way personal data are processed and call for clarifications of these concepts, in order to ensure effective application and compliance in practice.~~

Controller

The ~~concept~~concepts of controller ~~is~~, joint controller and processor are *functional* concepts in that they aim to allocate responsibilities according to the actual roles of the parties and *autonomous*~~,~~ concepts in the sense that ~~it~~they should be interpreted mainly according to ~~Community~~EU data protection law~~, and functional, in the sense that it is intended to allocate responsibilities where the factual influence is, and thus based on a factual rather than a formal analysis~~.

~~The definition in the Directive contains three main building blocks:~~

- ~~the personal aspect ("*the natural or legal person, public authority, agency or any other body*");~~
- ~~the possibility of pluralistic control ("*which alone or jointly with others*"); and~~
- ~~the essential elements to distinguish the controller from other actors ("*determines the purposes and the means of the processing of personal data*").~~

~~The analysis of these building blocks leads to a number of conclusions that have been summarized in paragraph IV of the opinion.~~

In principle, there is no limitation as to the type of entity that may assume the role of a controller but in practice it is usually the organisation as such, and not an individual within the organisation (such as the CEO, an employee or a member of the board), that acts as a controller.

A controller is a body that *decides* certain key elements of the processing. Controllership may be defined by law or may stem from an analysis of the factual elements or circumstances of the case. Certain processing activities can be seen as naturally attached to the role of an entity (an employer to employees, a publisher to subscribers or an association to its members). In many cases, the terms of a contract can help identify the controller, although they are not decisive in all circumstances.

A controller determines the purposes and means of the processing, i.e. the *why* and *how* of the processing. The controller must decide on both purposes and means. However, some more practical aspects of implementation ("non-essential means") can be left to the processor. It is not necessary that the controller actually has access to the data that is being processed to be qualified as a controller.

Joint controllers

The qualification as joint controllers may arise where more than one actor is involved in the processing. The GDPR introduces specific rules for joint controllers and sets a framework to govern their relationship. The overarching criterion for joint controllership to exist is the joint participation of two or more entities in the determination of the purposes and means of a processing operation. Joint participation can take the form of a *common decision* taken by two or more entities or result from

converging decisions by two or more entities, where the decisions complement each other and are necessary for the processing to take place in such a manner that they have a tangible impact on the determination of the purposes and means of the processing. An important criterion is that the processing would not be possible without both parties' participation in the sense that the processing by each party is inseparable, i.e. inextricably linked. The joint participation needs to include the determination of purposes on the one hand and the determination of means on the other hand.

Processor

~~This opinion also analyzes the concept of processor, the existence of which depends on a decision taken by the controller, who can decide either to process data within his organization or to delegate all or part of the processing activities to an external organization. Two basic conditions for qualifying as processor are on the one hand being a separate legal entity with respect to the controller and on the other hand processing personal data on his behalf.~~

A processor is a natural or legal person, public authority, agency or another body, which processes personal data on behalf of the controller. Two basic conditions for qualifying as processor exist: that it is a separate entity in relation to the controller and that it processes personal data on the controller's behalf.

The processor must not process the data otherwise than according to the controller's instructions. The controller's instructions may still leave a certain degree of discretion about how to best serve the controller's interests, allowing the processor to choose the most suitable technical and organisational means. A processor infringes the GDPR, however, if it goes beyond the controller's instructions and starts to determine its own purposes and means of the processing. The processor will then be considered a controller in respect of that processing and may be subject to sanctions for going beyond the controller's instructions.

Relationship between controller and processor

A controller must only use processors providing sufficient guarantees to implement appropriate technical and organisational measures so that the processing meets the requirements of the GDPR. Elements to be taken into account could be the processor's expert knowledge (e.g. technical expertise with regard to security measures and data breaches); the processor's reliability; the processor's resources and the processor's adherence to an approved code of conduct or certification mechanism.

Any processing of personal data by a processor must be governed by a contract or other legal act which shall be in writing, including in electronic form, and be binding. The controller and the processor may choose to negotiate their own contract including all the compulsory elements or to rely, in whole or in part, on standard contractual clauses.

The GDPR lists the elements that have to be set out in the processing agreement. The processing agreement should not, however, merely restate the provisions of the GDPR; rather, it should include more specific, concrete information as to how the requirements will be met and which level of security is required for the personal data processing that is the object of the processing agreement.

Relationship among joint controllers

Joint controllers shall in a transparent manner determine and agree on their respective responsibilities for compliance with the obligations under the GDPR. The determination of their respective responsibilities must in particular regard the exercise of data subjects' rights and the duties to provide information. In addition to this, the distribution of responsibilities should cover other controller

obligations such as regarding the general data protection principles, legal basis, security measures, data breach notification obligation, data protection impact assessments, the use of processors, third country transfers and contacts with data subjects and supervisory authorities.

Each joint controller has the duty to ensure that they have a legal basis for the processing and that the data are not further processed in a manner that is incompatible with the purposes for which they were originally collected by the controller sharing the data.

The legal form of the arrangement among joint controllers is not specified by the GDPR. For the sake of legal certainty, and in order to provide for transparency and accountability, the EDPB recommends that such arrangement be made in the form of a binding document such as a contract or other legal binding act under EU or Member State law to which the controllers are subject.

The arrangement shall duly reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects and the essence of the arrangement shall be made available to the data subject.

Irrespective of the terms of the arrangement, data subjects may exercise their rights in respect of and against each of the joint controllers. Supervisory authorities are not bound by the terms of the arrangement whether on the issue of the qualification of the parties as joint controllers or the designated contact point.

~~The Working Party recognises the difficulties in applying the definitions of the Directive in a complex environment, where many scenarios can be foreseen involving controllers and processors, alone or jointly, with different degrees of autonomy and responsibility.~~
~~In its analysis, it has emphasized the need to allocate responsibility in such a way that compliance with data protection rules will be sufficiently ensured in practice. However, it has not found any reason to think that the current distinction between controllers and processors would no longer be relevant and workable in that perspective.~~
~~The Working Party therefore hopes that the explanations given in this opinion, illustrated with specific examples taken from the daily experience of data protection authorities, will contribute to effective guidance on the way to interpret these core definitions of the Directive.~~

Table of contents

~~The Working Party on the Protection of Individuals with regard to the processing of personal data~~

The European Data Protection Board

Having regard to Article 70 (1e) of the Regulation 2016/679/EU 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, (hereinafter "GDPR" or "the Regulation"),

~~set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995,~~

Having regard to ~~Articles 29 and 30 paragraphs 1(a) and 3 of that Directive, and Article 15 paragraph 3 of Directive 2002/58/EC of the European Parliament and of the Council of 12~~the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July ~~2002~~2018[1],

Having regard to Article 12 and Article 22 of its Rules of Procedure,

Whereas the preparatory work of these guidelines involved the collection of inputs from stakeholders, both in writing and at a stakeholder event, in order to identify the most pressing challenges;

HAS ADOPTED THE FOLLOWING ~~opinion:~~GUIDELINES

~~I.~~ INTRODUCTION

1. This document seeks to provide guidance on the concepts of controller and processor based on the GDPR's rules on definitions in Article 4 and the provisions on obligations in chapter IV. The main aim is to clarify the meaning of the concepts and to clarify the different roles and the distribution of responsibilities between these actors.

2. The concept of ~~data~~ controller and its interaction with the concept of ~~data~~ processor play a crucial role in the application of ~~Directive 95/46/EC~~the GDPR, since they determine who shall be responsible for compliance with different data protection rules, and how data subjects can exercise their rights in practice. The ~~concept of data controller is also essential for the determination of the applicable national law and the effective exercise of the supervisory tasks conferred on Data Protection Authorities.~~GDPR explicitly introduces the accountability principle, i.e. the controller shall be responsible for, and be able to demonstrate compliance with, the principles relating to processing of personal data in Article 5. Moreover, the GDPR also introduces more specific rules on the use of processor(s) and some of the provisions on personal data processing are addressed - not only to controllers - but also to processors.

3. It is therefore of paramount importance that the precise meaning of these concepts and the criteria for their correct use are sufficiently clear and shared ~~by all those in the Member States who play a role in the implementation of the Directive and in the application, evaluation and enforcement of the national provisions that give effect to it~~throughout the European Union and the EEA.

4. The Article 29 Working Party issued guidance on the concepts of controller/processor in its opinion

1/2010 (WP169)[2] in order to provide clarifications and concrete examples with respect to these concepts. Since the entry into force of the GDPR, many questions have been raised regarding to what extent the GDPR brought changes to the concepts of controller and processor and their respective roles. Questions were raised in particular to the substance and implications of the concept of joint controllership (e.g. as laid down in Article 26 GDPR) and to the specific obligations for processors laid down in Chapter IV (e.g. as laid down in Article 28 GDPR). Therefore, and as the EDPB recognizes that the concrete application of the concepts needs further clarification, the EDPB now deems it necessary

~~There are signs that there may be a lack of clarity, at least as to certain aspects of these concepts, and some divergent views among practitioners in different Member States that may lead to different interpretations of the same principles and definitions introduced for the purpose of harmonisation at European level. This is why the Article 29 Working Party has decided, as part of its strategic work programme for 2008-2009, to devote special attention to the elaboration of a document setting out a common approach to these issues.~~

[1] References to "Member States" made throughout this document should be understood as references to "EEA Member States".

~~The Working Party recognizes that the concrete application of the concepts of data controller and data processor is becoming increasingly complex. This is mostly due to the increasing complexity of the environment in which these concepts are used, and in particular due to a growing tendency, both in the private and in the public sector, towards organisational differentiation, in combination with the development of ICT and globalisation, in a way that may give rise to new and difficult issues and may sometimes result in a lower level of protection afforded to data subjects.~~

[2] Article 29 Working Party Opinion 1/2010 on the concepts of "controller" and "processor" adopted on 16 February 2010, 264/10/EN, WP 169

~~Although the provisions of the Directive have been formulated in a technology-neutral way and so far were able to resist well to the evolving context, these complexities may indeed lead to uncertainties with regard to the allocation of responsibility and the scope of applicable national laws. These uncertainties may have a negative effect on compliance with data protection rules in critical areas, and on the effectiveness of data protection law as a whole. The Working Party has already dealt with some of these issues~~

~~in relation to specific questions[1], but deems it necessary now to give more developed guidelines and specific guidance in order to ensure a consistent and harmonised approach.~~

to give more developed and specific guidance in order to ensure a consistent and harmonised approach throughout the EU and the EEA. The present guidelines replace the previous opinion of Working Party 29 on these concepts (WP169).

5. In part I, these guidelines discuss the definitions of the different concepts of controller, joint controllers, processor and third party/recipient. In part II, further guidance is provided on the consequences that are attached to the different roles of controller, joint controllers and processor.

~~Therefore, the Working Party has decided to provide in this opinion - in a similar way as already done in the Opinion on the concept of personal data[2] – some clarifications and some concrete examples[3] with respect to the concepts of data controller and data processor.~~

PART I – CONCEPTS

~~II.~~1 GENERAL OBSERVATIONS ~~and policy issues~~

6. The GDPR, in Article 5(2), explicitly introduces the accountability principle which means that:

   – the controller shall be *responsible for the compliance* with the principles set out in Article 5(1) GDPR; and that
   – the controller shall be able to *demonstrate compliance* with the principles set out in Article 5(1) GDPR.

   This principle has been described in an opinion by the Article 29 WP [3] and will not be discussed in detail here.

7. The aim of incorporating the accountability principle into the GDPR and making it a central principle was to emphasize that data controllers must implement appropriate and effective measures and be able to demonstrate compliance. [4]

8. The accountability principle has been further elaborated in Article 24, which states that the controller shall implement appropriate technical and organisational measures to ensure and to be able **to demonstrate** that processing is performed in accordance with the GDPR. Such measures shall be reviewed and updated if necessary. The accountability principle is also reflected in Article 28, which lays down the controller's obligations when engaging a processor.

9. The accountability principle is directly addressed to the controller. However, some of the more specific rules are addressed to both controllers and processors, such as the rules on supervisory authorities' powers in Article 58. Both controllers and processors can be fined in case of non-compliance with the obligations of the GDPR that are relevant to them and both are directly accountable towards supervisory authorities by virtue of the obligations to maintain and provide appropriate documentation upon request, co-operate in case of an investigation and abide by administrative orders. At the same time, it should be recalled that processors must always comply with, and act only on, instructions from the controller.

10. The accountability principle, together with the other, more specific rules on how to comply with the GDPR and the distribution of responsibility, therefore makes it necessary to define the different roles of several actors involved in a personal data processing activity.

~~The Directive explicitly refers to the concept of controller in several provisions. The definitions of~~

~~'controller' and 'processor' in Article 2 (d) and (e) of Directive 95/46/EC (further "the Directive") read as follows:~~

[3] Article 29 Working Party Opinion 3/2010 on the principle of accountability adopted on 13 July 2010, 00062/10/EN WP 173.
[4] Recital 74 GDPR

11. A general observation regarding the concepts of controller and processor in the GDPR is that they have not changed compared to the Directive 95/46/EC and that overall, the criteria for how to attribute the different roles remain the same.

12. The concepts of controller and processor are *functional* concepts: they aim to allocate responsibilities according to the actual roles of the parties.[5] This implies that the legal status of an actor as either a "controller" or a "processor" must in principle be determined by its actual activities in a specific situation, rather than upon the formal designation of an actor as being either a "controller" or "processor" (e.g. in a contract).[6]

13. The concepts of controller and processor are also *autonomous* concepts in the sense that, although external legal sources can help identifying who is a controller, it should be interpreted mainly according to EU data protection law. The concept of controller should not be prejudiced by other - sometimes colliding or overlapping - concepts in other fields of law, such as the creator or the right holder in intellectual property rights or competition law.

14. As the underlying objective of attributing the role of controller is to ensure accountability and the effective and comprehensive protection of the personal data, the concept of 'controller' should be interpreted in a sufficiently broad way so as to ensure full effect of EU data protection law, to avoid lacunae and to prevent possible circumvention of the rules.

2 DEFINITION OF CONTROLLER

2.1 Definition of controller

15. A controller is defined by Article 4(7) GDPR as

> ~~*'Controller' shall mean*~~ "***the natural or legal person, public authority, agency or*** ~~*any*~~ ***other body*** *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* ~~*national or Community laws or regulations*~~*Union or Member State law, the controller or the specific criteria for* ~~*his*~~*its nomination may be* ~~*designated by national or Community*~~***provided for by Union or Member State law***~~*;*~~*".*
>
> ~~*'Processor' shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.*~~

~~These definitions have been shaped during the negotiations about the draft proposal for the Directive in the early 1990's and the concept of 'controller' was essentially taken from the Council of Europe's Convention 108 concluded in 1981. During these negotiations some important changes took place.~~

~~In the first place, 'controller of the file' in Convention 108 was replaced by 'controller' in relation to 'processing of personal data'. This is a wide notion, defined in Article 2 (b) of the Directive as "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction." The concept of 'controller' was thus no longer used for a static object ('the file') but related to activities reflecting the life cycle of information from its collection to its destruction, and this needed to be looked at both in detail and in its entirety ('operation or set of operations'). Although the result may have been the same in many cases, the concept was thereby given a much wider and more dynamic meaning and scope.~~

[1] ~~See e.g. Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial~~

Telecommunication (SWIFT), adopted on 22 November 2006 (WP 128), and more recently Opinion 5/2009 on online social networking, adopted on 12 June 2009 (WP 163).

[2] Opinion 4/2007 on the concept of personal data, adopted on 20 June 2007 (WP 136)

[3] These examples are based on current national or European practice and may have been amended or edited to ensure a better understanding.

Other changes involved the introduction of the possibility of 'pluralistic control' ("either alone or jointly with others"), the requirement that the controller should "determine the purposes and means of the processing of personal data", and the notion that this determination could be made by national or Community law or in another way. The Directive also introduced the concept of 'processor', which is not mentioned in Convention 108. These and other changes will be analyzed in more detail in the course of this opinion.

II.1. Role of concepts

While the concept of controller (of the file) plays a very limited role[4] in Convention 108, this is completely different in the Directive. Article 6 (2) explicitly provides that "it shall be for the controller to ensure that paragraph 1 is complied with". This refers to the main principles relating to data quality, including the principle in Article 6 (1)(a) that "personal data must be processed fairly and lawfully". This means in effect that all provisions setting conditions for lawful processing are essentially addressed to the controller, even if this is not always clearly expressed.

Furthermore, the provisions on the rights of the data subject, to information, access, rectification, erasure and blocking, and to object to the processing of personal data (Articles 10-12 and 14), have been framed in such a way as to create obligations for the controller. The controller is also central in the provisions on notification and prior checking (Articles 18-21). Finally, it should be no surprise that the controller is also held liable, in principle, for any damage resulting from unlawful processing (Article 23).

This means that the first and foremost role of the concept of controller is to determine who shall be responsible for compliance with data protection rules, and how data subjects can exercise the rights in practice.[5] In other words: to allocate responsibility.

This goes to the heart of the Directive, its first objective being "to protect individuals with regard to the processing of personal data". That objective can only be realised and made effective in practice, if those who are responsible for data processing can be sufficiently stimulated by legal and other means to take all the measures that are necessary to ensure that this protection is delivered in practice. This is confirmed in Article 17 (1) of the Directive, according to which the controller "*must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing*."

---

[4] It is not used in any of the substantive provisions, except in Article 8.a in relation to the right to be informed (principle of transparency). The controller as the responsible party is only visible in certain parts of the explanatory memorandum.

[5] See also Recital 25 of Directive 95/46/EC: "*Whereas the principles of protection must be reflected, on the one hand, in the obligations imposed on persons, public authorities, enterprises, agencies or other bodies responsible for processing, in particular regarding data quality, technical security, notification to the supervisory authority, and the circumstances under which processing can be carried out, and, on the other hand, in the right conferred on individuals, the data on whom are the subject of processing, to be informed that processing is taking place, to consult the data, to request corrections and even to object to processing in certain circumstances.*"

The means to stimulate responsibility can be pro-active and reactive. In the first case, they are to ensure an effective implementation of data protection measures and sufficient means of accountability for controllers. In the second case, they may involve civil liability and sanctions in order to ensure that any relevant damage is compensated and that adequate measures are taken to correct any mistakes or wrongdoing.

The concept of controller is also an essential element in determining which national law is applicable to a processing operation or set of processing operations. The main rule of applicable law under Article 4 (1)(a) of the Directive is that each Member State applies its national provisions to "*the processing of personal data, where (…) carried out in the context of the activities of an establishment of the controller on the territory of the Member State*". This provision continues as follows: "*when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable*". This means that the establishment(s) of the controller is (are) also determinative for the applicable national law(s), and possibly for a number of different applicable national laws and the way in which they relate to each other.[6]

Finally, it should be noted that the concept of controller appears in many different provisions of the Directive as an element of their scope or of a specific condition applying under them: e.g. Article 7 provides that personal data may be processed only if: "*(c) processing is necessary for compliance with a legal obligation to which the controller is subject, (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the date are disclosed, or (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party or parties to whom the data are disclosed, except where such interests are overridden …*" . The identity of the controller is also an important element of the information to the data subject that is required under Articles 10 and 11.

The concept of 'processor' plays an important role in the context of confidentiality and security of processing (Articles 16-17), as it serves to identify the responsibilities of those who are more closely involved in the processing of personal data, either under direct authority of the controller or elsewhere on his behalf. The distinction between 'controller' and 'processor' mostly serves to distinguish between those involved that are responsible as controller(s) and those that are only acting on their behalf. This is again mostly a matter of how to allocate responsibility. Other consequences, either in terms of applicable law or otherwise, may flow from there.

However, in case of a processor, there is a further consequence – both for controller and processor – that under Article 17 of the Directive, the applicable law for security of processing shall be the national law of the Member State where the processor is established.[7]

---

[6] The Working Party intends to adopt a separate opinion on "applicable law" in the course of 2010. When Community institutions and bodies process personal data, the assessment of controllership is also relevant with regard to the possible application of Regulation (EC) 45/2001 or other relevant EU legal instruments.

[7] See Article 17 (3) second indent: "the obligation …. as defined by the law of the Member State in which the processor is established, shall also be incumbent on the processor".

Finally, as defined in Article 2(f), "*third party' shall mean any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process data*." Controller and processor and their staff are therefore considered as the 'inner circle of data processing' and are not covered by special provisions on third parties.

II.2. Relevant context

Different developments in the relevant environment have made these issues more urgent and also more complex than before. At the time of signature of Convention 108, and to a large extent also when Directive 95/46/EC was adopted, the context of data processing was still relatively clear and straightforward, but that is no longer the case.

This is first of all due to a growing tendency towards organisational differentiation in most relevant sectors. In the private sector, the distribution of financial or other risks has led to ongoing corporate diversification, which is only enhanced by mergers and acquisitions. In the public sector, a similar differentiation is taking place in the context of decentralisation or separation of policy departments and executive agencies. In both sectors, there is a growing emphasis on the development of delivery chains or service delivery across organisations and on the use of subcontracting or outsourcing of services in order to benefit from specialisation and possible economies of scale. As a result, there is a growth in various services, offered by service providers, who do not always consider themselves responsible or accountable. Due to organisational choices of companies (and their contractors or subcontractors) relevant databases may be located in one or more countries within or outside the European Union.

The development of Information and Communication Technologies ("ICT") has greatly facilitated these organisational changes and has also added a few of its own. Responsibilities on different levels – often the result of organisational differentiation – usually require and stimulate the extensive use of ICT. The development and deployment of ICT products and services also lead to new roles and responsibilities in their own right, which do not always clearly interact with existing or developing responsibilities in client organisations. It is therefore important to be aware of relevant differences and to clarify responsibilities where required. The introduction of micro-technology – such as RFID chips in consumer products – raises similar issues of shifting responsibilities. At the other end, there are new and difficult issues involved in the use of distributed computing, notably 'cloud computing' and 'grids'.[8]

Globalisation is another complicating factor. Where organisational differentiation and development of ICT involve multiple jurisdictions, such as often around the Internet, issues of applicable law are bound to arise, not only within the EU or EEA, but also in relation to third countries. An illustration can be found in the framework of the anti- doping context, where the World Anti Doping Agency (WADA), established in Switzerland, operates a database including information on athletes (ADAMS) which is managed from Canada in co-operation with national anti-doping organisations around the

[8] 'Cloud computing' is a kind of computing where scalable and elastic IT capabilities are provided as a service to multiple customers using internet technologies. Typical cloud computing services provide common business applications online that are accessed from a web browser, while the software and data are stored on the servers. In this sense the cloud is not an island but a global connector of the world's information and users. With regard to 'grids', see below example 19.

~~world. The division of responsibilities and the attribution of controllership have been pointed out by the WP29 as raising specific difficulties.[9]~~
~~This means that the central issues at stake in this opinion have a high degree of practical relevance and may have great consequences.~~

~~II.3. Some key challenges~~

~~In terms of the objectives of the Directive, it is most important to ensure that the responsibility for data processing is clearly defined and can be applied effectively.~~
~~If it is not sufficiently clear what is required from whom – e.g. no one is responsible or a multitude of possible controllers – there is an obvious risk that too little, if anything, will happen and that the legal provisions will remain ineffective. It is also possible that ambiguities in interpretation will lead to competing claims and other controversies, in which case the positive effects will be less than expected or could be reduced or outweighed by unforeseen negative consequences.~~
~~In all these cases, the crucial challenge is thus to provide sufficient clarity to allow and ensure effective application and compliance in practice. In case of doubt, the solution that is most likely to promote such effects may well be the preferred option.~~
~~However, the same criteria that provide sufficient clarity may also lead to additional complexity and unwanted consequences. For example, the differentiation of control, in line with organisational realities, may lead to complexity in applicable national law, where different jurisdictions are involved.~~
~~The analysis should therefore have a sharp eye for the difference between acceptable consequences under present rules, and the possible need for adjustment of present rules to ensure continued effectiveness and to avoid undue consequences under changing circumstances.~~
~~This means that the current analysis is of great strategic importance and should be applied with care and in full awareness of possible interconnections between different issues.~~

~~III. Analysis of definitions~~

~~III.1. Definition of controller~~

16. The definition of controller ~~in the Directive~~ contains ~~three~~five main building blocks, which will be ~~analyzed~~analysed separately for the purposes of ~~this opinion~~these Guidelines. They are the following:

- ~~o~~ "the natural or legal person, public authority, agency or ~~any~~ other body"
- "determines"
- ~~o~~ "~~which~~ alone or jointly with others"
- "the purposes and means"
- ~~o~~ "~~determines the purposes and means~~ of the processing of personal data".

[5] Article 29 Working Party Opinion 1/2010, WP 169, p. 9.

~~[9] Opinion 3/2008 of 1 August 2008 on the World Anti-Doping Code Draft International Standard for the Protection of Privacy, WP156~~

[6] See also the Opinion of Advocate General Mengozzi, in *Jehovah's witnesses*, C-25/17, ECLI:EU:C:2018:57, paragraph 68 ("*For the purposes of determining the 'controller' within the meaning of Directive 95/46, I am inclined to consider [….] that excessive formalism would make it easy to circumvent the provisions of Directive 95/46 and that, consequently, it is necessary to rely upon a more factual than formal analysis […].*")

~~The first building block relates to the personal aspect of the definition. The third block contains the essential elements to distinguish the controller from other actors, while the second block looks into the possibility of 'pluralistic control'. These building blocks are closely inter-related. However for the sake of the methodology to be followed in this opinion, each of these items will be dealt with separately.~~

2.1.1 "Natural or legal person, public authority, agency or other body"

17. The first building block relates to the type of entity that can be a controller. Under the GDPR, a controller can be "*a natural or legal person, public authority, agency or other body*". This means that, in principle, there is no limitation as to the type of entity that may assume the role of a controller. It might be an organisation, but it might also be an individual or a group of individuals.[7] In practice, however, it is usually the organisation as such, and not an individual within the organisation (such as the CEO, an employee or a member of the board), that acts as a controller within the meaning of the GDPR. As far as data processing within a company group is concerned, special attention must be paid to the question of whether an establishment acts as a controller or processor, e.g. when processing data on behalf of the parent company.

18. Sometimes, companies and public bodies appoint a specific person responsible for the implementation of the processing operations. Even if a specific natural person is appointed to ensure compliance with data protection rules, this person will not be the controller but will act on behalf of the legal entity (company or public body) which will be ultimately responsible in case of infringement of the rules in its capacity as controller.

~~For practical purposes, it is helpful to start with the *first element* of the third building block – i.e. the meaning of the word "determines" – and to continue with the rest of the third block, and only then deal with the first and the second block.~~
~~III.1.a) Preliminary element: "determines"~~

2.1.2 "Determines"

~~As already mentioned above, the concept of controller played a minor role in Convention 108. Pursuant to Article 2 of the Convention, the "controller of the file" was defined as the body "who is competent ... to decide". The Convention emphasizes the need for a competence, which is determined "according to the national law". Therefore, the Convention referred back to national data protection laws, which, pursuant to the explanatory memorandum, would contain "precise criteria for determining who the competent person is".~~
~~While the first Commission proposal reflects this provision, the amended Commission proposal refers instead to the body "who decides", thereby eliminating the need that the competence to decide is established by law: the definition by law is still possible but not necessary. This is then confirmed by the Council Common Position and the adopted text, both referring to the body "which determines".~~
~~Against this background, the historic development highlights two important elements: firstly, that it is possible to be a controller irrespective of a specific competence or power to control data conferred by law; secondly, that in the process of adoption of Directive 95/46 the determination of the controller becomes a Community concept, a concept which has its own independent meaning in Community law, not varying because of - possibly divergent - provisions of national law. This latter element is essential with a view to ensuring the effective application of the Directive and a high level of protection in the Member States, which requires a uniform and therefore autonomous interpretation of such a key concept as "controller", which in the Directive acquires an importance which it didn't have in Convention 108.~~

~~In this perspective, the Directive completes this evolution by establishing that, even if the capacity to "determine" may arise from a specific attribution made by law, it would usually~~19. The second building block of the controller concept refers to the controller's *influence* over the processing, by virtue of an *exercise of decision-making power*. A controller is a body that *decides* certain key elements about the processing. This controllership may be defined by law or may stem from an analysis of the factual elements or circumstances of the case~~:~~. One should look at the specific processing operations in question and understand who determines them, by ~~replying in a first stage to the~~first considering the following questions: "*why is this processing taking place*? ~~Who initiated it~~" and "*who decided that the processing should take place for a particular purpose*?~~"~~".

Circumstances giving rise to control

~~Being a controller is primarily the consequence of the factual circumstance that an entity has chosen to process personal data for its own purposes. Indeed, a merely formal criterion would not be sufficient at least for two kinds of reasons: in some cases the formal appointment of a controller – laid down for example by law, in a contract or in a notification to the data protection authority – would just be lacking; in other cases, it may happen that the formal appointment would not reflect the reality, by formally entrusting the role of controller to a body which actually is not in the position to "determine".~~

The relevance of factual influence is also shown by the SWIFT case[10], where SWIFT was formally considered data processor but de facto acted - at least to a certain extent - as data controller. In that case, it was made clear that even though the designation of a party as data controller or processor in a contract may reveal relevant information regarding the legal status of this party, such contractual designation is nonetheless not decisive in determining its actual status, which must be based on concrete circumstances.

This factual approach is also supported by the consideration that the directive establishes that the controller is the one who "determines" rather than "lawfully determines" the purpose and means. The effective identification of controllership is decisive, even if the designation appears to be unlawful or the processing of data is exercised in an unlawful way. It is not relevant whether the decision to process data was "lawful" in the sense that the entity making such a decision was legally capable of doing so, or that a controller was formally appointed according to a specific procedure. The question of the lawfulness of the processing of personal data will still be relevant in a different stage and be assessed in the light of other Articles (in particular, Articles 6-8) of the Directive. In other terms, it is important to ensure that even in those cases where data are processed unlawfully, a controller can be easily found and held responsible for the processing.

A last characteristic of the concept of controller is its autonomy, in the sense that, although external legal sources can help identifying who is a controller, it should be interpreted mainly according to data protection law.[11] The concept of controller should not be prejudiced by other - sometimes colliding or overlapping - concepts in other fields of law, such as the creator or the right holder in intellectual property rights. Being a right holder for intellectual property does not exclude the possibility of qualifying as "controller" as well and thus be subject to the obligations stemming from data protection law.

The need for a typology

20. Having said that the concept of controller is a functional concept, intended to allocate responsibilities where the factual influence is, and thusit is therefore based on a **factual rather than a formal analysis**. Therefore, determining control may sometimes require an in-depth and lengthy investigation. However, the need to ensure effectiveness requires that a pragmatic approach is taken with a view to ensure predictability with regard to control. In this perspective,In order to facilitate the analysis, certain rules of thumb and practical presumptions are neededmay be used to guide and simplify the application of data protection law.

process. In most situations, This calls for an interpretation of the Directive ensuring that the "determining body" can be easily and clearly identified in most situations, by reference to those certain legal and/or factual circumstances from which factual"influence" normally can be inferred, unless other elements indicate the contrary. Two categories of situations can be distinguished: (1) control stemming from *legal provisions*; and (2) control stemming from *factual influence*.

[10] The case concerns the transfer to US authorities, with a view to fight terrorism financing, of banking data collected by SWIFT with a view to perform financial transactions on behalf of banks and financial institutions.

[11] See infra, the interference with concepts existing in other areas of law (for example, the concept of right holder for intellectual property or scientific research, or responsibility pursuant to civil law).

~~These circumstances can be analysed and classified according to the following three categories of situations, which allow a systematic approach to these issues:~~

1) Control stemming from legal provisions

~~1)~~21. There are cases where control ~~*stemming*~~can be inferred from explicit legal competence~~. This is *inter alia* the case referred to in the second part of the definition, i.~~ e.g., when the controller or the specific criteria for ~~his~~its nomination are designated by national or ~~Community law. The explicit appointment of the controller by law is not frequent and usually does not pose big problems~~Union law. Indeed, Article 4(7) states that "*where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.*" Where the controller has been specifically identified by law this will be determinative for establishing who is acting as controller. This presupposes that the legislator has designated as controller the entity that has a genuine ability to exercise control. In some countries, the

[7] For example, in its Judgment in *Jehovah's witnesses*, C-25/17, ECLI:EU:C:2018:551, paragraph 75, the CJEU considered that a religious community of Jehovah's witnesses acted as a controller, jointly with its individual members. Judgment in *Jehovah's witnesses*, C-25/17, ECLI:EU:C:2018:551, paragraph 75.

national law ~~has provided~~provides that public authorities are responsible for processing of personal data within the context of their duties.

22. However, more ~~frequent is the case where the law~~commonly, rather than directly appointing the controller or setting out the criteria for ~~his~~its appointment, ~~establishes~~the law will establish a task or ~~imposes~~impose a duty on someone to collect and process certain data. In those cases, the purpose of the processing is often determined by the law. The controller will normally be the one designated by law for the realization of this purpose, this public task. For example, this would be the case ~~of~~where an entity which is entrusted with certain public tasks (e.g., social security) which cannot be fulfilled without collecting at least some personal data, ~~and~~ sets up a database or register ~~with a view~~in order to fulfil ~~them~~those public tasks. In that case, ~~it follows from~~ the law, albeit indirectly, sets out who is the controller. More generally, the law may also impose an obligation on either public or private entities to retain or provide certain data. These entities would then normally be considered as ~~the controller for any~~controllers with respect to the processing ~~of personal data in that context~~that is necessary to execute this obligation.

~~2) *Control stemming from implicit competence*. This is the case where the capacity to determine is not explicitly laid down by law, nor the direct consequence of explicit legal provisions, but still stems from common legal provisions or established legal practice pertaining to different areas (civil law, commercial law, labour law, etc). In this case, existing traditional roles that normally imply a certain responsibility will help identifying the controller: for example, the employer in relation to data on his employees, the publisher in relation to data on subscribers, the association in relation to data on its members or contributors.~~

~~Example No. 1: Telecom operators~~

Example: Legal provisions

~~An interesting example of legal guidance to the private sector relates to the role of telecommunication operators: Recital 47 of Directive 95/46/EC clarifies that "*where a message containing personal data is transmitted by means of a telecommunications or electronic mail service, the sole purpose of which is the transmission of such messages, the controller in respect of the personal data contained in the message will normally be considered to be the person from whom the message originates, rather than the person offering the transmission services; (...) nevertheless, those offering such services will normally be considered controllers in respect of the processing of the additional personal data necessary for the operation of the service*". The provider of telecommunications services should therefore, in principle, be considered controller only for traffic and billing data, and not for any data being transmitted[12]. This legal guidance from the Community legislator is completely in line with the functional approach followed in this opinion.~~The national law in Country A lays down an obligation for municipal authorities to provide social welfare benefits such as monthly payments to citizens depending on their financial situation. In order to carry out these payments, the municipal authority must collect and process data about the applicants' financial circumstances. Even though the law does not explicitly state that the municipal authorities are controllers for this processing, this follows implicitly from the legal provisions.

~~In all these cases, the capacity to determine processing activities can be considered as naturally attached to the functional role of a (private) organization, ultimately entailing responsibilities also from a data protection point of view. In legal terms, this would apply regardless of whether the capacity to determine would be vested in the mentioned legal bodies, would be exercised by the appropriate organs acting on their behalf, or by a natural person in a similar role (see further below on the first element in point c). However, the same would be the case for a public authority with certain administrative tasks, in a country where the law would not be explicit as to its responsibility for data protection.~~

~~3~~2) *Control stemming from factual influence*~~. This is the case where the responsibility as controller is attributed on the basis of an assessment of the factual circumstances. In many cases, this will involve an assessment of the contractual relations between the different parties involved. This assessment allows for the drawing of external conclusions, assigning the role and responsibilities of controller to one or more parties. This might be particularly helpful in complicated environments, often making use of new information technologies, where relevant actors are often inclined to see themselves as "facilitators" and not as responsible controllers.~~

23. In the absence of control arising from legal provisions, the qualification of a party as controller must be established on the basis of an assessment of the factual circumstances surrounding the processing. All relevant factual circumstances must be taken into account in order to reach a conclusion as to whether a particular entity exercises a determinative influence with respect to the processing of personal data in question.

24. The need for factual assessment also means that the role of a controller does not stem from the nature of an entity that is processing data but from its concrete activities in a specific context. In other words, the same entity may act at the same time as controller for certain processing operations and as processor for others, and the qualification as controller or processor has to be assessed with regard to each specific data processing activity.

25. In practice, certain processing activities can be considered as naturally attached to the role or activities of an entity ultimately entailing responsibilities from a data protection point of view. This can be due to more general legal provisions or an established legal practice in different areas (civil law, commercial law, labour law etc.). In this case, existing traditional roles and professional expertise that normally imply a certain responsibility will help in identifying the controller, for example an employer in relation to processing personal data about his employees, a publisher processing personal data about its subscribers, or an association processing personal data about its members or contributors. When an entity engages in processing of personal data as part of its interactions with its own employees, customers or members, it will generally be the one who factually can determine the purpose and means around the processing and is therefore acting as a controller within the meaning of the GDPR.

Example: Law firms

The company ABC hires a law firm to represent it in a dispute. In order to carry out this task, the law firm needs to process personal data related to the case. The reasons for processing the personal data is the law firm's mandate to represent the client in court. This mandate however is not specifically targeted to personal data processing. The law firm acts with a significant degree of independence, for example in deciding what information to use and how to use it, and there are no instructions from the client company regarding the personal data processing. The processing that the law firm carries out in order to fulfil the task as legal representative for the company is therefore linked to the functional role of the law firm so that it is to be regarded as controller for this processing.

~~It may be that~~26. In many cases, an assessment of the contractual terms between the different parties involved can facilitate the determination of which party (or parties) is acting as controller. Even if a contract is silent ~~on~~as to who is the controller, ~~but contains~~it may contain sufficient elements to ~~assign the responsibility of controller to a party that apparently~~infer who exercises a ~~dominant~~decision-making role ~~in this~~with respect to the purposes and means of the processing. It may also be that the contract ~~is more~~contains an explicit statement as to the identity of the controller. If there is no reason to doubt that this accurately reflects the reality, there is nothing against following the terms of the contract. However, the terms of a contract are not decisive ~~under~~in all circumstances, as this would simply allow parties to allocate responsibility ~~where~~as they ~~think~~see fit. It is not possible either to become a controller or to escape controller obligations simply by shaping the contract in a certain way where the factual circumstances say something else.

27. If one party in fact decides why and how personal data are processed that party will be a controller even if a contract says that it is a processor. Similarly, it is not because a commercial contract uses the term "subcontractor" that an entity shall be considered a processor from the perspective of data protection law.[8]

28. In line with the factual approach, the word "determines" means that the entity that actually exerts influence on the purposes and means of the processing is the controller. Normally, a processor agreement establishes who the determining party (controller) and the instructed party (processor) are. Even if the processor offers a service that is preliminary defined in a specific way, the controller has to be presented with a detailed description of the service and must make the final decision to actively approve the way the processing is carried out and to be able to request changes if necessary. Furthermore, the processor cannot at a later stage change the essential elements of the processing without the approval of the controller.

2.1.3 "Alone or jointly with others"

29. Article 4(7) recognizes that the "purposes and means" of the processing might be determined by more than one actor. It states that the controller is the actor who "alone or jointly with others" determines the purposes and means of the processing. This means that several different entities may act as controllers for the same processing, with each of them then being subject to the applicable data

~~The fact itself that somebody determines how personal data are processed may entail the qualification of data controller, even though this qualification arises outside the scope of a contractual relation or is explicitly excluded by a contract. A clear example of this was the SWIFT case, whereby this company took the decision to make available certain personal data - which were originally processed for commercial purposes on behalf of financial institutions - also for the purpose of the fight against terrorism financing, as requested by subpoenas issued by the U.S. Treasury.~~

[8] See e.g., Article 29 Data Protection Working Party, Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT), 22 November 2006, WP128, p. 11.

~~[12] A DPA dealt with control in a case brought by a data subject complaining against unsolicited e-mail advertising. Through his complaint, the data subject requested the communication network provider to either confirm or deny that it was the sender of the advertising e-mail. The DPA stated that the company only providing a client with access to a communication network, i.e. neither initiating the data transmission nor selecting the addressees or modifying the information contained in the transmission, cannot be considered as data controller.~~

In case of doubt, other elements than the terms of a contract may be useful to find the controller, such as the degree of actual control exercised by a party, the image given to data subjects and reasonable expectations of data subjects on the basis of this visibility (see also below on the third element in point b). This category is particularly important since it allows to address and to allocate responsibilities also in those cases of unlawful conduct, where the actual processing activities may even be carried out against the interest and the willingness of some of the parties.

Preliminary conclusion

Among these categories, the first two allow in principle a more secure indication of the determining body and may well cover more than 80% of the relevant situations in practice. However, a formal legal designation should be in line with data protection rules, by ensuring that the designated body has effective control over the processing operations, or in other words that the legal appointment reflects the reality of things.

Category 3 requires a more complex analysis and is more likely to lead to divergent interpretations. The terms of a contract can often help to clarify the issue, but are not decisive under all circumstances. There is a growing number of actors who do not consider themselves as determining the processing activities, and thus responsible for them. A conclusion on the basis of factual influence is in those cases the only feasible option. The question of the lawfulness of this processing will still be assessed in the light of other Articles (6-8).

If none of the abovementioned categories is applicable, the appointment of a controller should be considered as "null and void". Indeed, a body which has neither legal nor factual influence to determine how personal data are processed cannot be considered as a controller.

From a formal perspective, a consideration which corroborates this approach is that the definition of data controller should be considered as a mandatory legal provision, from which parties cannot simply derogate or deviate. From a strategic perspective, such an appointment would run counter to the effective application of data protection law and would nullify the responsibility that data processing entails.

III.1.b) Third element: "purposes and means of processing"

The third element represents the substantive part of the test: what a party should determine in order to qualify as controller.

The history of this provision shows many developments. Convention 108 referred to the purpose of the automated data files, the categories of personal data and the operations to be applied to them. The Commission took these substantive elements, with minor language modifications, and added the competence to decide which third parties may have access to the data. The amended Commission proposal made a step forward in shifting from "the purposes of the file" to "the purposes and objective of the processing", thus passing from a static definition linked to a file to a dynamic definition linked to the processing activity. The amended proposal still referred to four elements (purposes/objective, personal data, operations and third parties having access to them), which were reduced to two ("purposes and means") only by the Council Common Position.

protection provisions. Correspondingly, an organisation can still be a controller even if it does not make all the decisions as to purposes and means. The criteria for joint controllership and the extent to which two or more actors jointly exercise control may take different forms, as clarified later on.[9]

2.1.4 "Purposes and means"

30. The fourth building block of the controller definition refers to the object of the controller's influence, namely the "purposes and means" of the processing. It represents the substantive part of the controller concept: what a party should determine in order to qualify as controller.

31. Dictionaries define "purpose" as "an anticipated outcome that is intended or that guides your planned actions" and "means" as "how a result is obtained or an end is achieved".

~~On~~32. The ~~other hand, the Directive~~GDPR establishes that data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Determination of the "purposes" of the processing and the "means" to achieve them is therefore particularly important.

~~It can also be said that~~33. Determining the purposes and the means amounts to ~~determining~~deciding respectively the "why" and the "how" of ~~certain~~the processing ~~activities. In this perspective, and taking into account that both elements go together, there is a need to provide guidance about which level of influence on the "why" and the "how" may entail the qualification of an entity as a controller.~~: [10] given a particular processing operation, the controller is the actor who has determined *why* the processing is taking place (i.e., "to what end"; or "what for") and *how* this objective shall be reached (i.e. which means shall be employed to attain the objective). A natural or legal person who exerts such influence over the processing of personal data, thereby participates in the determination of the purposes and means of that processing in accordance with the definition in Article 4(7) GDPR.[11]

34. The controller must decide on both purpose and means of the processing as described below. As a result, the controller cannot settle with only determining the purpose. It must also make decisions about the means of the processing. Conversely, the party acting as processor can never determine the purpose of the processing.

35. In practice, if a controller engages a processor to carry out the processing on its behalf, it often means that the processor shall be able to make certain decisions of its own on how to carry out the processing. The EDPB recognizes that some margin of manoeuvre may exist for the processor also to be able to make some decisions in relation to the processing. In this perspective, there is a need to provide guidance about which **level of influence** on the "why" and the "how" should entail the qualification of an entity as a controller and to what extent a processor may make decisions of its own.

36. When one entity clearly determines purposes and means, entrusting another entity with processing activities that amount to the execution of its detailed instructions, the situation is straightforward, and there is no doubt that the second entity should be regarded as a processor, whereas the first entity is the controller.

Essential vs. non-essential means

~~When it comes to assessing the determination of the purposes and the means with a view to attribute the role of data controller, the crucial question is therefore to which level of~~

details somebody should determine purposes and means in order to be considered as a controller. And in correlation to this, which is the margin of manoeuvre that the Directive allows for a data processor. These definitions become particularly relevant when various actors are involved in the processing of personal data, and it is necessary to determine which of them are data controller (alone or jointly with others) and which are instead to be considered data processors – if any.

37. The question is where to draw the line between decisions that are reserved to the controller and decisions that can be left to the discretion of the processor. Decisions on the purpose of the processing are clearly always for the controller to make.

The emphasis to be put on purposes or means may vary depending on the specific context in which the processing takes place.

A pragmatic approach is needed, placing greater emphasis on discretion in determining purposes and on the latitude in making decisions. In these cases, the question is why the processing is happening and what is the role of possible connected actors like outsourcing companies: would the outsourced company have processed data if it were not asked by the controller, and at what conditions? A processor could operate further to general guidance provided mainly on purposes and not going very deep in details with regard to means.

[9] See section 3, p.15

[10] See also the Opinion of Advocate General Bot in *Wirtschaftsakademie*, C-210/16, ECLI:EU:C:2017:796, paragraph 46.

[11] Judgment in *Jehovah's witnesses*, C-25/17, ECLI:EU:C:2018:551, paragraph 68.

With regard to the determination of the means, the term "means" evidently comprises very different sorts of elements, which is also illustrated by the history of this definition.

38. As regards the determination of means, a distinction can be made between essential and non-essential means. "Essential means" are closely linked to the purpose and the scope of the processing and are traditionally and inherently reserved to the controller. Examples of essential means are the type of personal data which are processed ("*which data shall be processed*?"), the duration of the processing ("*for how long shall they be processed?*"), the categories of recipients ("*who shall have access to them?*") and the categories of data subjects ("*whose personal data are being processed?*"). "Non-essential means" concern more practical aspects of implementation, such as the choice for a particular type of hard- or software or the detailed security measures which may be left to the processor to decide on.

Example: Payroll administration

Employer A hires another company to administer the payment of salaries to its employees. Employer A gives clear instructions on who to pay, what amounts, by what date, by which bank, how long the data shall be stored, what data should be disclosed to the tax authority etc. In this case, the processing of data is carried out for Company A's purpose to pay salaries to its employees and the payroll administrator may not use the data for any purpose of its own. The way in which the payroll administrator should carry out the processing is in essence clearly and tightly defined. Nevertheless, the payroll administrator may decide on certain detailed matters around the processing such as which software to use, how to distribute access within its own organisation etc. This does not alter its role as processor as long as the administrator does not go against or beyond the instructions given by Company A.

Example: Bank payments

As part of the instructions from Employer A, the payroll administration transmits information to Bank B so that they can carry out the actual payment to the employees of Employer A. This activity includes processing of personal data by Bank B which it carries out for the purpose of performing banking activity. Within this activity, the bank decides independently from Employer A on which data that have to be processed to provide the service, for how long the data must be stored etc. Employer A cannot have any influence on the purpose and means of Bank B's processing of data. Bank B is therefore to be seen as a controller for this processing and the transmission of personal data from the payroll administration is to be regarded as a disclosure of information between two controllers, from Employer A to Bank B.

Example: Accountants

Employer A also hires Accounting firm C to carry out audits of their bookkeeping and therefore transfers data about financial transactions (including personal data) to C. Accounting firm C processes these data without detailed instructions from A. Accounting firm C decides itself, in accordance with legal provisions regulating the tasks of the auditing activities carried out by C, that the data it collects will only be processed for the purpose of auditing A and it determines what data it needs to have, which categories of persons that need to be registered, how long the data shall be kept and what technical means to use. Under these circumstances, Accounting firm C is to be regarded as a controller of its own when performing its auditing services for A. However, this assessment may be different depending on the level of

instructions from A. In a situation where the law does not lay down specific obligations for the accounting firm and the client company provides very detailed instructions on the processing, the accounting firm would indeed be acting as a processor. A distinction could be made between a situation where the processing is - in accordance with the laws regulating this profession - done as part of the accounting firm's core activity and where the processing is a more limited, ancillary task that is carried out as part of the client company's activity.

Example: Hosting services

Employer A hires hosting service H to store encrypted data on H's servers. The hosting service H does not determine whether the data it hosts are personal data nor does it process data in any other way than storing it on its servers. As storage is one example of a personal data processing activity, the hosting service H is processing personal data on employer A's behalf and is therefore a processor. Employer A must provide the necessary instructions to H on, for example, which technical and organisational security measures are required and a data processing agreement according to Article 28 must be concluded. H must assist A in ensuring that the necessary security measures are taken and notify it in case of any personal data breach.

~~In the original proposal, the role of controller would stem from determining four elements (purposes/objective, personal data, operations and third parties having access to them). The final formulation of the provision, referring only to "purposes and means", cannot be construed as being in contradiction to the older version, as there cannot be any doubt about the fact that e.g. the controller must determine which data shall be processed for the envisaged purpose(s). Therefore, the final definition must rather be understood as being only a shortened version comprising nevertheless the sense of the older version. In other words, "means" does not only refer to the technical ways~~ 39. Even though decisions on non-essential means can be left to the processor, the controller must still stipulate certain elements in the processor agreement, such as – in relation to the security requirement, e.g. an instruction to take all measures required pursuant to Article 32 of the GDPR. The agreement must also state that the processor shall assist the controller in ensuring compliance with, for example, Article 32. In any event, the controller remains responsible for the implementation of appropriate technical and organisational measures to ensure and be able to demonstrate that the processing is performed in accordance with the Regulation (Article 24). In doing so, the controller must take into account the nature, scope, context and purposes of the processing as well as the risks for rights and freedoms of natural persons. For this reason, the controller must be fully informed about the means that are used so that it can take an informed decision in this regard. In order for the controller to be able to demonstrate the lawfulness of the processing, it is advisable to document at the minimum necessary technical and organisational measures in the contract or other legally binding instrument between the controller and the processor.

~~of~~2.1.5 "Of the processing of personal data~~, but also to the "how" of processing, which includes questions like "which data shall be processed", "which third parties shall have access to this data", "when data shall data be deleted", etc.~~"

~~Determination of the "means" therefore includes both technical and organizational questions where the decision can be well delegated to processors (as e.g. "which hardware or software shall be used?") and essential elements which are traditionally and inherently reserved to the determination of the controller, such as "which data shall be processed?", "for how long shall they be processed?",~~

"who shall have access to them?", and so on.

Against this background, 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.

In this perspective, it is well possible that the technical and organizational means are determined exclusively by the data processor.

In these cases – where there is a good definition of purposes, but little or even no guidance on technical and organizational means – the means should represent a reasonable way of achieving the purpose(s) and the data controller should be fully informed about the means used. Would a contractor have an influence on the purpose and carry out the processing (also) for its own benefit, for example by using personal data received with a view to generate added-value services, it would be a controller (or possibly a joint controller) for another processing activity and therefore subject to all the obligations of the applicable data protection law.

Example No. 3: Company referred to as data processor but acting as controller

Company MarketinZ provides services of promotional advertisement and direct marketing to various companies. Company GoodProductZ concludes a contract with MarketinZ, according to which the latter company provides commercial advertising for GoodProductZ customers and is referred to as data processor. However, MarketinZ decides to use GoodProducts customer database also for the purpose of promoting products of other customers. This decision to add an additional purpose to the one for which the personal data were transferred converts MarketinZ into a data controller for this processing operation. The question of the lawfulness of this processing will still be assessed in the light of other Articles (6-8).

~~In some legal systems decisions taken on security measures are particularly important, since security measures are explicitly considered as an essential characteristic to be defined by the controller. This raises the issue of which decisions on security may entail the qualification of controller for a company to which processing has been outsourced.~~

~~*Preliminary conclusion*~~

~~Determination of the "purpose" of processing is reserved to the "controller". Whoever makes this decision is therefore (*de facto*) controller. The determination of the "means" of processing can be delegated by the controller, as far as technical or organisational questions are concerned. Substantial questions which are essential to the core of lawfulness of processing are reserved to the controller. A person or entity who decides~~

~~e.g. on how long data shall be stored or who shall have access to the data processed is acting as a 'controller' concerning this part of the use of data, and therefore has to comply with all controller's obligations.~~

~~III.1.c)~~ ~~First element: "natural person, legal person or any other body"~~

~~The first element of the definition refers to the personal side: who can be a controller, and therefore considered ultimately responsible for the obligations stemming from the Directive. The definition mirrors exactly the formulation of Article 2 of Convention 108 and was not object of specific discussion in the decision-making process of the Directive. It refers to a broad series of subjects, which can play the role of controller, ranging from natural to legal persons and including "any other body".~~

~~It is important that the interpretation of this element should ensure the effective application of the Directive by favouring as much as possible a clear and univocal identification of the controller in all circumstances, irrespective of whether a formal appointment has been made and publicised.~~

~~First of all, it is important to stay as close as possible to the practice established both in the public and private sector by other areas of law, such as civil, administrative and criminal law. In most cases these provisions will indicate to which persons or bodies responsibilities should be allocated and will in principle help to identify who is the data controller.~~

~~In the strategic perspective of allocating responsibilities, and in order to provide data subjects with a more stable and reliable reference entity for the exercise of their rights under the Directive, preference should be given to consider as controller the company or body as such rather than a specific person within the company or the body. It is the company or the body which shall be considered ultimately responsible for data processing and the obligations stemming from data protection legislation, unless there are clear elements indicating that a natural person shall be responsible. In general, it should be assumed that a company or public body is responsible as such for the processing activities taking place within its realm of activities and risks.~~

40. The purposes and means determined by the controller must relate to the "processing of personal data". Article 4(2) GDPR defines the processing of personal data as "*any operation or set of operations which is performed on personal data or on sets of personal data*". As a result, the concept of a controller can be linked either to a single processing operation or to a set of operations. In practice, this may mean that the control exercised by a particular entity may extend to the entirety of processing at issue but may also be limited to a particular stage in the processing.[12]

[12] Judgment in *Fashion ID*, C-40/17, ECLI:EU:C:2019:629, paragraph 74: "*(A)s the Advocate General noted, [...-] it appears that a natural or legal person may be a controller, within the meaning of Article 2(d) of Directive 95/46, jointly with others only in respect of operations involving the processing of personal data for which it determines*

41. Anyone who decides to process data must consider whether this includes personal data and, if so, what the obligations are according to the GDPR. An actor will be considered a "controller" even if it does not deliberately target personal data as such or has wrongfully assessed that it does not process personal data.

42. It is not necessary that the controller actually has access to the data that is being processed[13]. Someone who outsources a processing activity and in doing so, has a determinative influence on the purpose and (essential) means of the processing (e.g. by adjusting parameters of a service in such a way that it influences whose personal data shall be processed), is to be regarded as controller even though he or she will never have actual access to the data.

Example: Market research

Company ABC wishes to understand which types of consumers are most likely to be interested in its products and contracts a service provider, XYZ, to obtain the relevant information.

Company ABC instructs XYZ on what type of information it is interested in and provides a list of questions to be asked to those participating in the market research.

Company ABC receives only statistical information (e.g., identifying consumer trends per region) from XYZ and does not have access to the personal data itself. Nevertheless, Company ABC decided that the processing should take place, the processing is carried out for its purpose and its activity and it has provided XYZ with detailed instructions on what information to collect. Company ABC is therefore still to be considered a controller with respect of the processing of personal data that takes place in order to deliver the information it has requested. XYZ may only process the data for the purpose given by Company ABC and according to its detailed instructions and is therefore to be regarded as processor.

3 DEFINITION OF JOINT CONTROLLERS

3.1 Definition of joint controllers

43. The qualification as joint controllers may arise where more than one actor is involved in the processing.

44. While the concept is not new and already existed under Directive 95/46/EC, the GDPR, in its Article 26, introduces specific rules for joint controllers and sets a framework to govern their relationship. In

jointly the purposes and means. By contrast, […] that natural or legal person cannot be considered to be a controller, within the meaning of that provision, in the context of operations that precede or are subsequent in the overall chain of processing for which that person does not determine either the purposes or the means".

[13] Judgment in *Wirtschaftsakademie*, C-201/16, ECLI :EU :C :2018 :388, paragraph 38.

addition, the Court of Justice of the European Union (CJEU) in recent rulings has brought clarifications on this concept and its implications[14].

45. As further elaborated in Part II, section 2, the qualification of joint controllers will mainly have consequences in terms of allocation of obligations for compliance with data protection rules and in particular with respect to the rights of individuals.

46. In this perspective, the following section aims to provide guidance on the concept of joint controllers in accordance with the GDPR and the CJEU case law to assist entities in determining where they may be acting as joint controllers and applying the concept in practice.

3.2 Existence of joint controllership

3.2.1 General considerations

47. The definition of a controller in Article 4 (7) GDPR forms the starting point for determining joint controllership. The considerations in this section are thus directly related to and supplement the considerations in the section on the concept of controller. As a consequence, the assessment of joint controllership should mirror the assessment of "single" control developed above.

48. Article 26 GDPR, which reflects the definition in Article 4 (7) GDPR, provides that *"[w]here two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers."* In broad terms, joint controllership exists with regard to a specific processing activity when different parties determine *jointly* the purpose and means of this processing activity. Therefore, assessing the existence of joint controllers requires examining whether the determination of purposes and means that characterize a controller are decided by more than one party. "Jointly" must be interpreted as meaning "together with" or "not alone", in different forms and combinations, as explained below.

49. The assessment of joint controllership should be carried out on a factual, rather than a formal, analysis of the actual influence on the purposes and means of the processing. All existing or envisaged arrangements should be checked against the factual circumstances regarding the relationship between the parties. A merely formal criterion would not be sufficient for at least two reasons: in some cases, the formal appointment of a joint controller - laid down for example by law or in a contract - would be absent; in other cases, it may be that the formal appointment does not reflect the reality of the arrangements, by formally entrusting the role of controller to an entity which actually is not in the position to "determine" the purposes and means of the processing.

50. Not all processing operations involving several entities give rise to joint controllership. The overarching criterion for joint controllership to exist is the **joint participation of two or more entities in the determination of the purposes and means** of a processing operation. More specifically, joint participation needs to include the determination of purposes on the one hand and the determination

[14] See in particular, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie*, (C-210/16), *Tietosuojavaltuutettu v Jehovan todistajat — uskonnollinen yhdyskunta* (C-25/17), *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV* (C-40/17). To be noted that while these judgments were issued by the CJUE on the interpretation of the concept of joint controllers under Directive 95/46/CE, they remain valid in the context of the GDPR, given that the elements determining this concept under the GDPR remain the same as under the Directive.

~~Sometimes, companies and public bodies appoint a specific person responsible for the implementation of the processing operations. However, also in such a case where a specific natural person is appointed to ensure compliance with data protection principles or to process personal data, he/she will not be the controller but will act on behalf of the legal entity (company or public body), which will still be liable in case of breach of the principles in its capacity as controller.~~[13]

of means on the other hand. If each of these elements are determined by all entities concerned, they should be considered as joint controllers of the processing at issue.

3.2.2 Assessment of joint participation

51. Joint participation in the determination of purposes and means implies that more than one entity have a decisive influence over whether and how the processing takes place. In practice, joint participation can take several different forms. For example, joint participation can take the form of a **common decision** taken by two or more entities or result from **converging decisions** by two or more entities regarding the purposes and essential means.

52. Joint participation through a *common decision* means deciding together and involves a common intention in accordance with the most common understanding of the term "jointly" referred to in Article 26 of the GDPR.

53. The situation of joint participation through *converging decisions* results more particularly from the case law of the CJEU on the concept of joint controllers. 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**. As such, an important criterion to identify converging decisions in this context **is whether the processing would not be possible without both parties' participation in the sense that the processing by each party is inseparable, i.e. inextricably linked.** The situation of joint controllers acting on the basis of converging decisions should however be distinguished from the case of a processor, since the latter – while participating in the performance of a processing – does not process the data for its own purposes but carries out the processing on behalf of the controller.

54. The fact that one of the parties does not have access to personal data processed is not sufficient to exclude joint controllership [15] . For example, in *Jehovah's Witnesses*, the CJEU considered that a religious community must be considered a controller, jointly with its members who engage in preaching, of the processing of personal data carried out by the latter in the context of door-to-door preaching.[16] The CJEU considered that it was not necessary that the community had access to the data in question, or to establish that that community had given its members written guidelines or instructions in relation to the data processing.[17] The community participated in the determination of purposes and means by organising and coordinating the activities of its members, which helped to achieve the objective of the Jehovah's Witnesses community. [18] In addition, the community had knowledge on a general level of the fact that such processing was carried out in order to spread its faith.[19]

55. It is also important to underline, as clarified by the CJEU, that an entity will be considered as joint controller with the other(s) only in respect of those operations for which it determines, jointly with others, the means and the purposes of the processing. If one of these entities decides alone the

~~Especially for big and complex structures, it is a crucial issue of "data protection governance" to ensure both a clear responsibility of the natural person representing the company and concrete functional responsibilities within the structure, for example by entrusting other persons to act as representatives or points of contact for data subjects.~~

Special analysis is needed in cases where a natural person acting within a legal person uses data for his or her own purposes outside the scope and the possible control of the legal person's activities. In this case the natural person involved would be controller of the processing decided on, and would bear responsibility for this use of personal data. The original controller could nevertheless retain some responsibility in case the new processing occurred because of a lack of adequate security measures.

As already mentioned above, the role of the controller is crucial and particularly relevant when it comes to determining liability and imposing sanctions. Even if liability and sanctions will vary depending on the Member States, since they are imposed according to national laws, the need to clearly identify the natural or legal person responsible for breaches of data protection law is beyond doubt an essential pre-condition for the effective application of the Directive.

The identification of 'the controller' in a data protection perspective will be interconnected in practice with the civil, administrative or criminal law rules providing for the allocation of responsibilities or sanctions to which a legal or a natural person can be subject[14].

Civil liability should not raise specific issues in this context as it applies in principle to both legal and natural persons. Criminal and/or administrative liability, however, may according to national law sometimes apply only to natural persons. If there are criminal or administrative sanctions for data protection infringements according to the respective national law, this law will normally also decide who is responsible: where criminal or administrative liability of legal persons is not recognised, such liability might be taken on by functionaries of legal persons according to the special rules of national law[15].

[15] Judgment in *Wirtschaftsakademie*, C-210/16, ECLI:EU:C:2018:388, paragraph 38.
[16] Judgment in Jehovah's witnesses, C-25/17, ECLI:EU:C:2018:551, paragraph 75.
[17] Ibid.
[18] Ibid, paragraph 71.
[19] Ibid.

[13] A similar reasoning is applied with regard to Regulation (EC) 45/2001, whose Article 2(d) refers to "the Community institution or body, the Directorate-General, the unit or any other organisational entity". It has been made clear in supervision practice that officials of EU institutions and bodies, who have been appointed as "controllers", act on behalf of the body for which they work.

[14] See the Commission's "Comparative Study on the Situation in the 27 Member States as regards the Law Applicable to Non-contractual Obligations Arising out of Violations of Privacy and Rights relating to Personality", February 2009, available at http://ec.europa.eu/justice_home/doc_centre/civil/studies/doc/study_privacy_en.pdf

[15] This does not exclude that national laws may provide for criminal or administrative liability not only for the controller but also for any person infringing data protection law.

European law contains useful examples of criteria attributing criminal responsibility[16], notably when an offence is committed for the benefit of the legal person: Responsibility can be attributed in such a case to any person, "acting either individually or as part of an organ of the legal person, who has a leading position within the legal person, based on one of the following:

(a) a power of representation of the legal person;

(b) an authority to take decisions on behalf of the legal person;

(c) an authority to exercise control within the legal person."

Preliminary conclusion

Summarising the above reflections it can be concluded that the one liable for a data protection breach is always the controller, i.e. the legal person (company or public body) or the natural person as formally identified according to the criteria of the Directive. If a natural person working within a company or public body uses data for his or her own purposes, outside the activities of the company, this person shall be considered as a de facto controller and will be liable as such.

III.1.d) Second element: "alone or jointly with others"

Example No. 4: Secret monitoring of employees

A member of the board of a company decides to secretly monitor the employees of the company, even though this decision is not formally endorsed by the board. The company should be considered as controller and face the possible claims and liability with regard to the employees whose personal data have been misused.

The liability of the company is notably due to the fact that as a controller, it has the obligation to ensure compliance with security and confidentiality rules. Misuse by a functionary of the company or an employee could be considered as the result of inappropriate security measures. This is irrespective of whether at a later stage also the member of the board or other natural persons within the company may be considered liable, both from a civil law perspective - also towards the company - as well as from a criminal law perspective. This could be the case e.g. if the board member made use of collected data for extorting personal favours from employees: he would have to be considered as 'controller' and be liable concerning this specific use of data.

This paragraph, drawing on the previous analysis of the typical characteristics of a controller, will deal with those cases where multiple actors interact in the processing of personal data. Indeed, there are an increasing number of cases in which different actors act as controllers and the definition laid down by the Directive caters for this.

The possibility that the controller operates "alone or jointly with others" was not mentioned in Convention 108 and was actually introduced only by the European Parliament before the adoption of the Directive. In the Commission opinion on the EP's

[16] See e.g. Directive 2008/99/EC of 19 November 2008 on the protection of the environment through criminal law, Council Framework Decision of 13 June 2002 on combating terrorism. Legal instruments are either based on Article 29, Article 31(e) and Article 34(2)(b) TEU or correspond to the legal bases for instruments used in the first pillar, resulting from the ECJ jurisprudence in cases C- 176/03, COM/Council, [ECJR] 2005, I-7879 and C-440/05, COM/Council, [ECJR] 2007, I-9097. See also the Communication by the COM (2005) 583 final).

purposes and means of operations that precede or are subsequent in the chain of processing, this entity must be considered as the sole controller of this preceding or subsequent operation[20].

56. 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, the CJEU has clarified that those operators may be involved at different stages of that processing 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.

3.2.2.1 Jointly determined purpose(s)

57. Joint controllership exists when entities involved in the same processing operation process such data for jointly defined purposes. This will be the case if the entities involved process the data for the same, or common, purposes.

58. In addition, when the entities do not have the same purpose for the processing, joint controllership may also, in light of the CJEU case law, be established when the entities involved pursue purposes which are closely linked or complementary. Such may be the case, for example, when there is a mutual benefit arising from the same processing operation, provided that each of the entities involved participates in the determination of the purposes and means of the relevant processing operation. In *Fashion ID*, for example, the CJEU clarified that a website operator participates in the determination of the purposes (and means) of the processing by embedding a social plug-in on a website in order to optimize the publicity of its goods by making them more visible on the social network. The CJEU considered that the processing operations at issue were performed in the economic interests of both the website operator and the provider of the social plug-in.[21]

59. Likewise, as noted by the CJEU in *Wirtschaftsakademie*, the processing of personal data through statistics of visitors to a fan page is intended to enable Facebook to improve its system of advertising transmitted via its network and to enable the administrator of the fan page to obtain statistics to manage the promotion of its activity.[22] Each entity in this case pursues its own interest but both parties participate in the determination of the purposes (and means) of the processing of personal data as regards the visitors to the fan page.[23]

60. In this respect, it is important to highlight that the mere existence of a mutual benefit (for ex. commercial) arising from a processing activity does not give rise to joint controllership. If the entity involved in the processing does not pursue any purpose(s) of its own in relation to the processing activity, but is merely being paid for services rendered, it is acting as a processor rather than as a joint controller.

3.2.2.2 Jointly determined means

61. Joint controllership also requires that two or more entities have exerted influence over the means of the processing. This does not mean that, for joint controllership to exist, each entity involved needs in all cases to determine all of the means. Indeed, as clarified by the CJEU, different entities may be

---

[20] Judgment in *Fashion ID*, C-40/17, ECLI:EU:2018:1039, paragraph 74 "*By contrast, and without prejudice to any civil liability provided for in national law in this respect, that natural or legal person cannot be considered to be a controller, within the meaning of that provision, in the context of operations that precede or are subsequent in the overall chain of processing for which that person does not determine either the purposes orthe means*".

[21] Judgment in *Fashion ID*, C-40/17, ECLI:EU:2018:1039, paragraph 80.

[22] Judgment in *Wirtschaftsakademie*, C-210/16, ECLI:EU:C:2018:388, paragraph 34.

[23] Judgment in Wirtschaftsakademie, C-210/16, ECLI:EU:C:2018:388, paragraph 39.

involved at different stages of that processing and to different degrees. Different joint controllers may therefore define the means of the processing to a different extent, depending on who is effectively in a position to do so.

62. It may also be the case that one of the entities involved provides the means of the processing and makes it available for personal data processing activities by other entities. The entity who decides to make use of those means so that personal data can be processed for a particular purpose also participates in the determination of the means of the processing.

63. This scenario can notably arise in case of platforms, standardised tools, or other infrastructure allowing the parties to process the same personal data and which have been set up in a certain way by one of the parties to be used by others that can also decide how to set it up[24]. The use of an already existing technical system does not exclude joint controllership when users of the system can decide on the processing of personal data to be performed in this context.

64. As an example of this, the CJEU held in *Wirtschaftsakademie* that the administrator of a fan page hosted on Facebook, by defining parameters based on its target audience and the objectives of managing and promoting its activities, must be regarded as taking part in the determination of the means of the processing of personal data related to the visitors of its fan page.

65. Furthermore, the choice made by an entity to use for its own purposes a tool or other system developed by another entity, allowing the processing of personal data, will likely amount to a joint decision on the means of that processing by those entities. This follows from the Fashion ID case where the CJEU concluded, that by embedding on its website the Facebook Like button made available by Facebook to website operators, Fashion ID has exerted a decisive influence in respect of the operations involving the collection and transmission of the personal data of the visitors of its website to Facebook and had thus jointly determined with Facebook the means of that processing[25].

66. It is important to underline that **the use of a common data processing system or infrastructure will not in all cases lead to qualify the parties involved as joint controllers,** in particular where the processing they carry out is separable and could be performed by one party without intervention from the other or where the provider is a processor in the absence of any purpose of its own (the existence of a mere commercial benefit for the parties involved is not sufficient to qualify as a purpose of processing).

> **Example: Travel agency**
>
> A travel agency sends personal data of its customers to the airline and a chain of hotels, with a view to making reservations for a travel package. The airline and the hotel confirm the availability of the seats and rooms requested. The travel agency issues the travel documents and vouchers for its customers. Each of the actors processes the data for carrying out their own activities and using their own means. In this case, the travel agency, the airline and the

[24] The provider of the system can be a joint controller if the criteria mentioned above are met, i.e. if the provider participates in the determination of purposes and means. Otherwise, the provider should be considered as a processor.
[25] Judgment in Fashion ID, C-40/17, ECLI:EU:2018:1039, paragraphs 77-79.

hotel are three different data controllers processing the data for their own purposes and there is no joint controllership.

The travel agency, the hotel chain and the airline then decide to participate jointly in setting up an internet-based common platform for the common purpose of providing package travel deals. They agree on the essential means to be used, such as which data will be stored, how reservations will be allocated and confirmed, and who can have access to the information stored. Furthermore, they decide to share the data of their customers in order to carry out joint marketing actions. In this case, the travel agency, the airline and the hotel chain, jointly determine why and how personal data of their respective customers are processed and will therefore be joint controllers with regard to the processing operations relating to the common internet-based booking platform and the joint marketing actions. However, each of them would still retain sole control with regard to other processing activities outside the internet-based common platform.

Example: Research project by institutes

Several research institutes decide to participate in a specific joint research project and to use to that end the existing platform of one of the institutes involved in the project. Each institute feeds personal data it holds into the platform for the purpose of the joint research and uses the data provided by others through the platform for carrying out the research. In this case, all institutes qualify as joint controllers for the personal data processing that is done by storing and disclosing information from this platform since they have decided together the purpose of the processing and the means to be used (the existing platform). Each of the institutes however is a separate controller for any other processing that may be carried out outside the platform for their respective purposes.

Example: Marketing operation

Companies A and B have launched a co-branded product C and wish to organise an event to promote this product. To that end, they decide to share data from their respective clients and prospects database and decide on the list of invitees to the event on this basis. They also agree on the modalities for sending the invitations to the event, how to collect feedback during the event and follow-up marketing actions. Companies A and B can be considered as joint controllers for the processing of personal data related to the organisation of the promotional event as they decide together on the jointly defined purpose and essential means of the data processing in this context.

Example: Clinical Trials

A health care provider (the investigator) and a university (the sponsor) decide to launch together a clinical trial with the same purpose. They collaborate together to the drafting of the study protocol (i.e. purpose, methodology/design of the study, data to be collected, subject exclusion/inclusion criteria, database reuse (where relevant) etc.). They may be considered as joint controllers, for this clinical trial as they jointly determine and agree on the same purpose and the essential means of the processing. The collection of personal data from the medical

amendment, the Commission refers to the possibility that "*for a single processing operation a number of parties may jointly determine the purpose and means of processing to be carried out" and therefore that in such a case "each of the co- controllers must be considered as being constrained by the obligations imposed by the Directive so as to protect the natural persons about whom the data are processed".*

record of the patient for the purpose of research is to be distinguished from the storage and use of the same data for the purpose of patient care, for which the health care provider remains the controller.

In the event that the investigator does not participate to the drafting of the protocol (he just accepts the protocol already elaborated by the sponsor), and the protocol is only designed by the sponsor, the investigator should be considered as a processor and the sponsor as the controller for this clinical trial.

The Commission opinion did not completely reflect the complexities in the current reality of data processing, since it focused only on the case where all the controllers equally determine and are equally responsible for a single processing operation. Instead, the reality shows that this is only one of the different kinds of 'pluralistic control' which may exist. In this perspective, "jointly" must be interpreted as meaning "together with" or "not alone" in different forms and combinations.

Example: Headhunters

Company X helps Company Y in recruiting new staff- with its famous value-added service "global matchz". Company X looks for suitable candidates both among the CVs received directly by Company Y and those it already has in its own database. Such database is created and managed by Company X on its own. This ensures that Company X enhances the matching between job offers and job seekers, thus increasing its revenues. Even though they have not formally taken a decision together, Companies X and Y jointly participate to the processing with the purpose of finding suitable candidates based on converging decisions: the decision to create and manage the service "global matchz" for Company X and the decision of Company Y to enrich the database with the CVs it directly receives. Such decisions complement each other, are inseparable and necessary for the processing of finding suitable candidates to take place. Therefore, in this particular case they should be considered as joint controllers of such processing. However, Company X is the sole controller of the processing necessary to manage its database and Company Y is the sole controller of the subsequent hiring processing for its own purpose (organisation of interviews, conclusion of the contract and management of HR data).

First of all, it should be noted that the likelihood of multiple actors involved in processing personal data is naturally linked to the multiple kinds of activities that according to the Directive may amount to "processing", which is at the end of the day the object of the "joint control". The definition of processing laid down by Article 2.b of the Directive does not exclude the possibility that different actors are involved in different operations or sets of operations upon personal data. These operations may take place simultaneously or in different stages.

In such a complex environment it is even more important that roles and responsibilities can be easily allocated, so as to ensure that the complexities of joint control do not result in an unworkable distribution of responsibilities which would hamper the effectiveness of data protection law. Unfortunately, due to the multiplicity of possible arrangements, it is not possible to draw up an

~~exhaustive "closed" list or categorization of the different kinds of "joint control". However, it is useful to provide also in this context guidance both through some categories and examples of joint control and through some factual elements from which joint control may be inferred or assumed.~~

3.2.3 Situations where there is no joint controllership

67. The fact that several actors are involved in the same processing does not mean that they are necessarily acting as joint controllers of such processing. Not all kind of partnerships, cooperation or collaboration imply qualification of joint controllers as such qualification requires a case-by-case analysis of each processing at stake and the precise role of each entity with respect to each processing. The cases below provide non-exhaustive examples of situations where there is no joint controllership.

68. For example, the exchange of the same data or set of data between two entities without jointly determined purposes or jointly determined means of processing should be considered as a transmission of data between separate controllers.

> ~~Example No. 5: Installing video-surveillance cameras~~
> **Example: Transmission of employee data to tax authorities**
>
> ~~The owner of a building concludes a contract with a security company, so that the latter installs some cameras in various parts of the building on behalf of the controller. The purposes of the video-surveillance and the way the images are collected and stored are determined exclusively by the owner of the building, which therefore has to be considered as the sole controller for this processing operation.~~A company collects and processes personal data of its employees with the purpose of managing salaries, health insurances, etc. A law imposes an obligation on the company to send all data concerning salaries to the tax authorities, with a view to reinforce fiscal control.
>
> In this case, even though both the company and the tax authorities process the same data concerning salaries, the lack of jointly determined purposes and means with regard to this data processing will result in qualifying the two entities as two separate data controllers.

~~In general, the assessment of joint control should mirror the assessment of "single" control developed above in paragraph III.1.a to c. In the same line, also in assessing joint control a substantive and functional approach should be taken, as illustrated above, focusing on whether the purposes and means are determined by more than one party.~~

~~Also in this context, contractual arrangements can be useful in assessing joint control, but should always be checked against the factual circumstances of the relationship between the parties.~~

69. Joint controllership may also be excluded in a situation where several entities use a shared database or a common infrastructure, if each entity independently determines its own purposes.

~~Example No. 6: Headhunters~~

Example: Marketing operations in a group of companies using a shared database:

~~Company Headhunterz Ltd helps Enterprize Inc in recruiting new staff. The contract clearly states that "Headhunterz Ltd will act on behalf of Enterprize and in processing personal data acts as a data processor. Enterprize is the sole data controller". However, Headhunterz Ltd is in an ambiguous position: on the one hand it plays the role of a controller towards the job seekers, on the other hand it assumes to be processor acting on behalf of the controllers, such as Enterprize Inc and other companies seeking staff trough it. Furthermore, Headhunterz – with its famous value-added service "global matchz" – looks for suitable candidates both among the CVs received directly by Enterprize and those it already has in its extensive database. This ensures that Headhunterz, which according to the contract is paid only for contracts actually signed, enhances the matching between job offers and job seekers, thus increasing its revenues. From the elements above, it can be said that, in spite of the contractual qualification, Headhunterz Ltd shall be considered as a controller, and as controlling jointly with Enterprize Inc at least those sets of operations relating to Enterprize recruitment.~~A group of companies uses the same database for the management of clients and prospects. Such database is hosted on the servers of the mother company who is therefore a processor of the companies with respect to the storage of the data. Each entity of the group enters the data of its own clients and prospects and processes such data for its own purposes only. Also, each entity decides independently on the access, the retention periods, the correction or deletion of their clients and prospects' data. They cannot access or use each other's data. The mere fact that these companies use a shared group database does not as such entail joint controllership. Under these circumstances, each company is thus a separate controller.

Example: Independent controllers when using a shared infrastructure

Company XYZ hosts a database and makes it available to other companies to process and host personal data about their employees. Company XYZ is a processor in relation to the processing and storage of other companies' employees as these operations are performed on behalf and according to the instructions of these other companies. In addition, the other companies process the data without any involvement from Company XYZ and for purposes which are not in any way shared by Company XYZ.

~~In this perspective, joint control will arise when different parties determine with regard to specific processing operations either the purpose or those essential elements of the means which characterize a controller (see supra paragraph III.1.a to c).~~

~~However, in the context of joint control the participation of the parties to the joint determination may take different forms and does not need to be equally shared. Indeed, in case of plurality of actors, they may have a very close relationship (sharing, for example, all purposes and means of a processing) or a more loose relationship (for example, sharing only purposes or means, or a part thereof). Therefore, a broad variety of typologies for joint control should be considered and their legal consequences assessed, allowing some flexibility in order to cater for the increasing~~

~~complexity of current data processing reality.~~

~~Against this background, it is necessary to deal with the different degrees in which multiple parties may interact or be linked between them in processing personal data.~~

70. Also, there can be situations where various actors successively process the same personal data in a chain of operations, each of these actors having an independent purpose and independent means in their part of the chain. In the absence of joint participation in the determination of the purposes and means of the same processing operation or set of operations, joint controllership has to be excluded and the various actors must be regarded as successive independent controllers.

~~First of all, the mere fact that different subjects cooperate in processing personal data, for example in a chain, does not entail that they are joint controllers in all cases, since an exchange of data between two parties without sharing purposes or means in a common set of operations should be considered only as a transfer of data between separate controllers.~~

~~Example No. 7: Travel agency (1)~~
Example: Statistical analysis for a task of public interest

~~A travel agency sends personal data of its customers to the airlines and a chain of hotels, with a view to making reservations for a travel package. The airline and the hotel confirm the availability of the seats and rooms requested. The travel agency issues the travel documents and vouchers for its customers. In this case, the travel agency, the airline and the hotel will be three different data controllers, each subject to the data protection obligations relating to its own processing of personal data.~~A public authority (Authority A) has the legal task of making relevant analysis and statistics on how the country's employment rate develops. To do that, many other public entities are legally bound to disclose specific data to Authority A. Authority A decides to use a specific system to process the data, including collection. This also means that the other units are obligated to use the system for their disclosure of data. In this case, without prejudice to any attribution of roles by law, Authority A will be the only controller of the processing for the purpose of analysis and statistics of the employment rate processed in the system, because Authority A determines the purpose for the processing, and has decided how the processing will be organised. Of course, the other public entities, as controllers for their own processing activities, are responsible for ensuring the accuracy of the data they previously processed, which they then disclose to Authority A.

~~However, the assessment may change when different actors would decide to set up a shared infrastructure to pursue their own individual purposes. When in setting up this~~

infrastructure these actors determine the essential elements of the means to be used, they qualify as joint data controllers - in any case to that extent - even if they do not necessarily share the same purposes.

> Example No. 8: Travel agency (2)
>
> The travel agency, the hotel chain and the airline decide to set up an internet based common platform in order to improve their cooperation with regard to travel reservation management. They agree on important elements of the means to be used, such as which data will be stored, how reservations will be allocated and confirmed, and who can have access to the information stored. Furthermore, they decide to share the data of their customers in order to carry out integrated marketing actions.
>
> In this case, the travel agency, the airline and the hotel chain, will have joint control on how personal data of their respective customers are processed and will therefore be joint controllers with regard to the processing operations relating to the common internet-based booking platform. However, each of them would still retain sole control with regard to other processing activities, e.g. those relating to the management of their human resources.

4 DEFINITION OF PROCESSOR

71. A processor is defined in Article 4 (8) as a natural or legal person, public authority, agency or another body, which processes personal data on behalf of the controller. Similar to the definition of controller, the definition of processor envisages a broad range of actors - it can be "*a natural or legal person, public authority, agency or other body*". This means that there is in principle no limitation as to which type of actor might assume the role of a processor. It might be an organisation, but it might also be an individual.

72. The GDPR lays down obligations directly applicable specifically to processors as further specified in Part II section 1 of these guidelines. A processor can be held liable or fined in case of failure to comply with such obligations or in case it acts outside or contrary to the lawful instructions of the controller.

73. Processing of personal data can involve multiple processors. For example, a controller may itself choose to directly engage multiple processors, by involving different processors at separate stages of the processing (multiple processors). A controller might also decide to engage one processor, who in turn - with the authorisation of the controller - engages one or more other processors ("sub processor(s)"). The processing activity entrusted to the processor may be limited to a very specific task or context or may be more general and extended.

74. Two basic conditions for qualifying as processor are:

    a) being *a separate entity* in relation to the controller and

    b) processing personal data *on the controller's behalf*.

In some cases, various actors process the same personal data in a sequence. In these cases, it is likely that at micro-level the different processing operations of the chain appear as disconnected, as each of them may have a different purpose. However, it is necessary to double-check whether at macro-level these processing operations should not be considered as a "set of operations" pursuing a joint purpose or using jointly defined means.

75. *A separate entity* means that the controller decides to delegate all or part of the processing activities

to an external organisation. Within a group of companies, one company can be a processor to another company acting as controller, as both companies are separate entities. On the other hand, a department within a company cannot generally be a processor to another department within the same entity.

76. If the controller decides to process data itself, using its own resources within its organisation, for example through its own staff, this is not a processor situation. Employees and other persons that are acting under the direct authority of the controller, such as temporarily employed staff, are not to be seen as processors since they will process personal data as a part of the controller's entity. In accordance with Article 29, they are also bound by the controller's instructions.

~~The following two examples clarify this idea by providing two different possible scenarios.~~

~~Example No. 9: Transfer of employee data to tax authorities~~

~~Company XYZ collects and processes personal data of its employees with the purpose of managing salaries, missions, health insurances, etc. However, a law also imposes an obligation on the company to send all data concerning salaries to the tax authorities, with a view to reinforce fiscal control.~~

~~In this case, even though both company XYZ and the tax authorities process the same data concerning salaries, the lack of shared purpose or means with regard to this data processing will result in qualifying the two entities as two separate data controllers.~~

~~Example No. 10: Financial transactions~~

~~Instead, let's take the case of a bank, which uses a financial messages carrier in order to carry out its financial transactions. Both the bank and the carrier agree about the means of the processing of financial data. The processing of personal data concerning financial transactions is carried out at a first stage by the financial institution and only at a later stage by the financial messages carrier. However, even if at micro level each of these subjects pursues its own purpose, at macro level the different phases and purposes and means of the processing are closely linked. In this case, both the bank and the message carrier can be considered as joint controllers.~~

77. *Processing personal data on the controller's behalf* firstly requires that the separate entity processes personal data for the benefit of the controller. In Article 4(2), processing is defined as a concept including a wide array of operations ranging from collection, storage and consultation to use, dissemination or otherwise making available and destruction. In practice, this means that all imaginable handling of personal data constitutes processing.

78. Secondly, the processing must be done on behalf of a controller but otherwise than under its direct authority or control. Acting "on behalf of" means serving someone else's interest and recalls the legal concept of "delegation". In the case of data protection law, a processor is called to implement the instructions given by the controller at least with regard to the purpose of the processing and the essential elements of the means. The lawfulness of the processing according to Article 6, and if relevant Article 9, of the Regulation will be derived from the controller's activity and the processor must not process the data otherwise than according to the controller's instructions. Even so, as described above, the controller's instructions may still leave a certain degree of discretion about how to best serve the

Other cases exist where the various actors involved jointly determine, in some cases to a different extent, the purposes and/or the means of a processing operation.
There are cases where each controller is responsible for only a part of the processing, but the information is put together and processed through a platform.

> Example No. 11: E-Government portals
>
> E-Government portals act as intermediaries between the citizens and the public administration units: the portal transfers the requests of the citizens and deposits the documents of the public administration unit until these are recalled by the citizen. Each public administration unit remains controller of the data processed for its own purposes. Nevertheless, the portal itself may be also considered controller. Indeed, it processes (i.e. collects and transfers to the competent unit) the requests of the citizens as well as the public documents (i.e. stores them and regulates any access to them, such as the download by the citizens) for further purposes (facilitation of e-Government services) than those for which the data are initially processed by each public administration unit. These controllers, among other obligations, will have to ensure that the system to transfer personal data from the user to the public administration's system is secure, since at a macro-level this transfer is an essential part of the set of processing operations carried out through the portal.

Another possible structure is the "origin-based approach", which arises when each controller is responsible for the data it introduces in the system. This is the case of some EU-wide databases, where control – and thus the obligation to act on requests for access and rectification – is attributed on the basis of the national origin of personal data.
Another interesting scenario is provided by online social networks.

> Example No 12: Social networks
>
> Social network service providers provide online communication platforms which enable individuals to publish and exchange information with other users. These service providers are data controllers, since they determine both the purposes and the means of the processing of such information. The users of such networks, uploading personal data also of third parties, would qualify as controllers provided that their activities are not subject to the so-called "household exception" [17].

After analysing those cases where the different subjects determine jointly only part of the purposes and means, a very clear cut and unproblematic case is the one where multiple subjects jointly determine and share all the purposes and the means of processing activities, giving rise to a full-fledged joint control.

[17] For more details and examples, see the Article 29 Working Party's Opinion 5/2009 on online social networking, adopted on 12 June 2009 (WP 163)

In the latter case, it is easy to determine who is competent and in a position to ensure data subjects' rights as well as to comply with data protection obligations. However, the task of determining which controller is competent – and liable - for which data subjects' rights and obligations is much more complex where the various joint controllers share purposes and means of processing in an asymmetrical way.

Need to clarify distribution of control

First of all, it should be pointed out that, especially in cases of joint control, not being able to directly fulfil all controller's obligations (ensuring information, right of access, etc) does not exclude being a controller. It may be that in practice those obligations could easily be fulfilled by other parties, which are sometimes closer to the data subject, on the controller's behalf. However, a controller will remain in any case ultimately responsible for its obligations and liable for any breach to them.

According to a previous text presented by the Commission during the process of adoption of the Directive, having access to certain personal data would have entailed being (joint) controller for these data. However, this formulation was not retained in the final text and the experience shows that on the one hand access to data does not entail as such control, while on the other hand having access to data is not an essential condition to be a controller. Therefore, in complex systems with multiple actors access to personal data and other data subjects' rights can be ensured at different levels by different actors.

Legal consequences also relate to the liability of controllers, raising in particular the issue of whether "joint control" established by the Directive always entails joint and several liability. Article 26 on liability uses the singular "controller", thus hinting at a positive reply. However, as already mentioned, the reality may present various ways of acting "jointly with", i.e. "together with". This might lead in some circumstances to joint and several liability, but not as a rule: in many cases the various controllers maybe be responsible – and thus liable - for the processing of personal data at different stages and to different degrees.

The bottom line should be ensuring that even in complex data processing environments, where different controllers play a role in processing personal data, compliance with data protection rules and responsibilities for possible breach of these rules are clearly allocated, in order to avoid that the protection of personal data is reduced or that a "negative conflict of competence" and loopholes arise whereby some obligations or rights stemming from the Directive are not ensured by any of the parties.

In these cases, more than ever, it is important that a clear information notice is given to the data subjects, explaining the various stages and actors of the processing. Moreover, it should be made clear if every controller is competent to comply with all data subject's rights or which controller is competent for which right.

~~Example No. 14: Behavioural advertising~~

~~Behavioural advertising uses information collected on an individual's web-browsing behaviour, such as the pages visited or the searches made, to select which advertisements to display to that individual. Both publishers, which very often rent advertising spaces on their websites, and ad network providers, who fill those spaces with targeted advertising, may collect and exchange information on users, depending on specific contractual arrangements.~~

~~From a data protection perspective, the publisher is to be considered as an autonomous controller insofar as it collects personal data from the user (user profile, IP address, location, language of operating system, etc) for its own purposes. The ad network provider will also be controller insofar as it determines the purposes (monitoring users across websites) or the essential means of the processing of data. Depending on the conditions of collaboration between the publisher and the ad network provider, for instance if the publisher enables the transfer of personal data to the ad network provider, including for instance through a re-direction of the user to the webpage of the ad network provider, they could be joint controllers for the set of processing operations leading to behavioural advertising.~~

~~In all cases, (joint) controllers shall ensure that the complexity and the technicalities of the behavioural advertising system do not prevent them from finding appropriate ways to comply with controllers' obligations and to ensure data subjects' rights. This would include notably:~~

- ~~*information* to the user on the fact that his/her data are accessible by a third party: this could be done more efficiently by the publisher who is the main interlocutor of the user,~~
- ~~and conditions of *access* to personal data: the ad network company would have to answer to users' requests on the way they perform targeted advertising on users data, and comply with correction and deletion requests.~~

~~In addition, publishers and ad network providers may be subject to other obligations stemming from civil and consumer protection laws, including tort laws and unfair commercial practices.~~

controller's interests, allowing the processor to choose the most suitable technical and organisational means.[26]

79. Acting "on behalf of" also means that the processor may not carry out processing for its own purpose(s). As provided in Article 28(10), a processor infringes the GDPR by going beyond the controller's instructions and starting to determine its own purposes and means of processing. The processor will be considered a controller in respect of that processing and may be subject to sanctions for going beyond the controller's instructions.

Example: Service provider referred to as data processor but acting as controller

Service provider MarketinZ provides promotional advertisement and direct marketing services to various companies. Company GoodProductZ concludes a contract with MarketinZ, according to which the latter company provides commercial advertising for GoodProductZ customers and is referred to as data processor. However, MarketinZ decides to use GoodProducts customer database also for other purposes than advertising for GoodProducts, such as developing their own business activity. The decision to add an additional purpose to the one for which the personal data were transferred converts MarketinZ into a data controller for this set of processing operations and their processing for this purpose would constitute an infringement of the GDPR.

80. The EDPB recalls that not every service provider that processes personal data in the course of delivering a service is a "processor" within the meaning of the GDPR. The role of a processor does not stem from the nature of an entity that is processing data but from its concrete activities in a specific context. The nature of the service will determine whether the processing activity amounts to processing of personal data on behalf of the controller within the meaning of the GDPR. In practice, where the provided service is not specifically targeted at processing personal data or where such processing does not constitute a key element of the service, the service provider may be in a position to independently determine the purposes and means of that processing which is required in order to provide the service. In that situation, the service provider is to be seen as a separate controller and not as a processor.[27] A case-by-case analysis remains necessary, however, in order to ascertain the degree of influence each entity effectively has in determining the purposes and means of the processing.

Example: Taxi service

A taxi service offers an online platform which allows companies to book a taxi to transport employees or guests to and from the airport. When booking a taxi, Company ABC specifies the name of the employee that should be picked up from the airport so the driver can confirm the employee's identity at the moment of pick-up. In this case, the taxi service processes personal data of the employee as part of its service to Company ABC, but the processing as such is not the target of the service. The taxi service has designed the online booking platform as part of

[26] See section 2.1.4 describing the distinction between essential and non-essential means.

[27] See also Recital 81 of the GDPR, which refers to "entrusting a processor processing activities", indicating that the processing activity as such is an important part of the decision of the controller to ask a processor to process personal data on its behalf.

developing its own business activity to provide transportation services, without any instructions from Company ABC. The taxi service also independently determines the categories of data it collects and how long it retains. The taxi service therefore acts as a controller in its own right, notwithstanding the fact that the processing takes places following a request for service from Company ABC.

81. The EDPB notes that a service provider may still be acting as a processor even if the processing of personal data is not the main or primary object of the service, provided that the customer of the service still determines the purposes and means of the processing in practice. When considering whether or not to entrust the processing of personal data to a particular service provider, controllers should carefully assess whether the service provider in question allows them to exercise a sufficient degree of control, taking into account the nature, scope, context and purposes of processing as well as the potential risks for data subjects.

Example: Call center

Company X outsources its client support to Company Y who provides a call center in order to help Company X's clients with their questions. The client support service means that Company Y has to have access to Company X client data bases. Company Y can only access data in order to provide the support that Company X has procured and they cannot process data for any other purposes than the ones stated by Company X. Company Y is to be seen as a personal data processor and a processor agreement must be concluded between Company X and Y.

Example: General IT support

Company Z hires an IT service provider to perform general support on its IT systems which include a vast amount of personal data. The access to personal data is not the main object of the support service but it is inevitable that the IT service provider systematically has access to personal data when performing the service. Company Z therefore concludes that the IT service provider - being a separate company and inevitably being required to process personal data even though this is not the main objective of the service – is to be regarded as a processor. A processor agreement is therefore concluded with the IT service provider.

Example: IT-consultant fixing a software bug

Company ABC hires an IT-specialist from another company to fix a bug in a software that is being used by the company. The IT-consultant is not hired to process personal data, and Company ABC determines that any access to personal data will be purely incidental and therefore very limited in practice. ABC therefore concludes that the IT-specialist is not a processor (nor a controller in its own right) and that Company ABC will take appropriate measures according to Article 32 of the GDPR in order to prevent the IT-consultant from processing personal data in an unauthorised manner.

82. As stated above, nothing prevents the processor from offering a preliminary defined service but the controller must make the final decision to actively approve the way the processing is carried out and/or to be able to request changes if necessary.

Preliminary conclusion

Parties acting jointly have a certain degree of flexibility in distributing and allocating obligations and responsibilities among them, as long as they ensure full compliance. Rules on how to exercise joint responsibilities should be determined in principle by controllers. However, factual circumstances should be considered also in this case, with a view to assessing whether the arrangements reflect the reality of the underlying data processing.

In this perspective, the assessment of joint control should take into account on the one hand the necessity to ensure full compliance with data protection rules, and on the other hand that the multiplication of controllers may also lead to undesired complexities and to a possible lack of clarity in the allocation of responsibilities. This would risk making the entire processing unlawful due to a lack of transparency and violate the principle of fair processing.

Example No. 15: Platforms for managing health data

Example: Cloud service provider

In a Member State, a public authority establishes a national switch point regulating the exchange of patient data between healthcare providers. The plurality of controllers – tens of thousands – results in such an unclear situation for the data subjects (patients) that the protection of their rights would be in danger. Indeed, for data subjects it would be unclear whom they could address in case of complaints, questions and requests for information, corrections or access to personal data. Furthermore, the public authority is responsible for the actual design of the processing and the way it is used. These elements lead to the conclusion that the public authority establishing the switch point shall be considered as a joint controller, as well as a point of contact for data subjects' requests.A municipality has decided to use a cloud service provider for handling information in its school and education services. The cloud service provides messaging services, videoconferences, storage of documents, calendar management, word processing etc. and will entail processing of personal data about school children and teachers. The cloud service provider has offered a standardized service that is offered worldwide. The municipality however must make sure that the agreement in place complies with Article 28(3) of the GDPR, that the personal data of which it is controller are processed for the municipality's purposes only. It must also make sure that their specific instructions on storage periods, deletion of data etc. are respected by the cloud service provider regardless of what is generally offered in the standardized service.

Against this background, it can be argued that joint and several liability for all parties involved should be considered as a means of eliminating uncertainties, and therefore assumed only in so far as an alternative, clear and equally effective allocation of obligations and responsibilities has not been established by the parties involved or does not clearly stem from factual circumstances.

III.2.5 DEFINITION OF processorTHIRD PARTY/RECIPIENT

The concept of processor was not laid down by Convention 108. For the first time, the role of processor is recognised by the first Commission proposal, but without the introduction of this concept, with a view to "*avoid situations whereby processing by a third party on behalf of the controller of the file has the effect of reducing the level of protection enjoyed*

~~*by the data subject*". Only with the amended Commission proposal and further to a proposal of the European Parliament, the concept of processor is explicitly and autonomously spelt out, before acquiring the current formulation in the Council Common position.~~

83. The Regulation not only defines the concepts of controller and processor but also the concepts of recipient and third party. As opposed to the concepts of controller and processor, the Regulation does not lay down specific obligations or responsibilities for recipients and third parties. These can be said to be relative concepts in the sense that they describe a relation to a controller or processor from a specific perspective, e.g. a controller or processor discloses data to a recipient. A recipient of personal data and a third party may well simultaneously be regarded as a controller or processor from other perspectives. For example, entities that are to be seen as recipients or third parties from one perspective, are controllers for the processing for which they determine the purpose and means.

Third party

84. Article 4(10) defines a "*third party*" as a natural or legal person, public authority, agency or body other than

- the data subject,
- the controller,
- the processor and
- persons who, under the direct authority of the controller or processor, are authorised to process personal data.

~~In the same way as for~~ the definition of controller, the definition of processor envisages a broad range of actors ~~that can play the role of processor ("… a~~ natural or legal person, public authority, agency or ~~any other body …").~~

85. The definition generally corresponds to the previous definition of "*third party*" in Directive 95/46/EC.

86. Whereas the terms "*personal data*", "*data subject*", "*controller*" and "*processor*" are defined in the Regulation, the concept of "*persons who, under the direct authority of the controller or processor, are authorised to process personal data*" is not. It is, however, generally understood as referring to persons that belong to the legal entity of the controller or processor (an employee or a role highly comparable to that of employees, e.g. interim staff provided via a temporary employment agency) but only insofar as they are authorized to process personal data. An employee etc. who obtains access to data that he or she is not authorised to access and for other purposes than that of the employer does not fall within this category. Instead, this employee should be considered as a third party vis-à-vis the processing undertaken by the employer. Insofar as the employee processes personal data for his or her own

~~The existence of a processor depends on a decision taken by the controller, who can decide either to process data within his organization, for example through staff authorized to process data under his direct authority (see *a contrario* Article 2.f), or to delegate all or part of the processing activities to an external organization, i.e. – as put forward by the explanatory memorandum of the amended Commission proposal – by "a legally separate person acting on his behalf".~~

purposes, distinct from those of his or her employer, he or she will then be considered a controller and take on all the resulting consequences and liabilities in terms of personal data processing.[28]

87. A third party thus refers to someone who, in the specific situation at hand, is not a data subject, a controller, a processor or an employee. For example, the controller may hire a processor and instruct it to transfer personal data to a third party. This third party will then be considered a controller in its own right for the processing that it carries out for its own purposes. It should be noted that, within a group of companies, a company other than the controller or the processor is a third party, even though it belongs to the same group as the company who acts as controller or processor.

Example ~~No. 16: Internet service providers of hosting~~**: Cleaning services**

~~An ISP providing hosting services is in principle a processor for the personal data published online by its customers, who use this ISP for their website hosting and maintenance. If however, the ISP further processes for its own purposes the data contained on the websites then it is the data controller with regard to that specific processing. This analysis is different from an ISP providing email or internet access services (see also example No. 1: telecom operators).~~Company A concludes a contract with a cleaning service company to clean its offices. The cleaners are not supposed to access or otherwise process personal data. Even though they may occasionally come across such data when moving around in the office, they can carry out their task without accessing data and they are contractually prohibited to access or otherwise process personal data that Company A keeps as controller. The cleaners are not employed by Company A nor are they seen as being under the direct authority of that company. There is no intention to engage the cleaning service company or its employees to process personal data on Company A's behalf. The cleaning service company and its employees are therefore to be seen as a third party and the controller must make sure that there are adequate security measures to prevent that they have access to data and lay down a confidentiality duty in case they should accidentally come across personal data.

Example: Company groups – parent company and subsidiaries

Companies X and Y form part of the Group Z. Companies X and Y both process data about their respective employees for employee administration purposes. At one point, the parent company ZZ decides to request employee data from all subsidiaries in order to produce group wide statistics. When transferring data from companies X and Y to ZZ, the latter is to be regarded as a third party regardless of the fact that all companies are part of the same group. Company ZZ will be regarded as controller for its processing of the data for statistical purposes.

~~Therefore, two basic conditions for qualifying as processor are on the one hand being a separate legal entity with respect to the controller and on the other hand processing personal data on his behalf. This processing activity may be limited to a very specific task or context or may be more general and extended.~~

~~Furthermore, the role of processor does not stem from the nature of an entity processing data but from its concrete activities in a specific context. In other words, the same entity may act at the same time as a controller for certain processing operations and as a processor for others, and the qualification as controller or processor has to be assessed with regard to specific sets of data or operations.~~

The most important element is the prescription that the processor act "…on behalf of the controller…". Acting on behalf means serving someone else's interest and recalls the legal concept of "delegation". In the case of data protection law, a processor is called to implement the instructions given by the controller at least with regard to the purpose of the processing and the essential elements of the means.

Recipient

88. Article 4(9) 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. Public authorities are however not to be seen as recipients when they receive personal data in the framework of a particular inquiry in accordance with Union or Member State law (e.g. tax and customs authorities, financial investigation units etc.)[29]

89. The definition generally corresponds to the previous definition of "*recipient*" in Directive 95/46/EC.

In this perspective, the lawfulness of the processor's data processing activity is determined by the mandate given by the controller. A processor that goes beyond its mandate and acquires a relevant role in determining the purposes or the essential means of processing is a (joint) controller rather than a processor. The question of the lawfulness of this processing will still be assessed in the light of other Articles (6-8). However, delegation may still imply a certain degree of discretion about how to best serve the controller's interests, allowing the processor to choose the most suitable technical and organizational means.

Example No. 17: Outsourcing of mail services

Private bodies provide mail services on behalf of (public) agencies – e.g. the mailing of family and maternity allowances performed on behalf of the National Social Security Agency. In that case a DPA indicated that the private bodies in question should be appointed as processors considering that their task, though carried out with a certain degree of autonomy, was limited to only a part of the processing operations necessary for the purposes determined by the data controller.

Still with a view to ensuring that outsourcing and delegation do not result in lowering the standard of data protection, the Directive contains two provisions which are specifically addressed to the processor and which define in great detail his obligations with regard to confidentiality and security.

- Article 16 establishes that the processor himself, as well as any person acting under his authority who has access to personal data, must not process them except on instructions from the controller.

- Article 17 in relation to security of processing establishes the need for a contract or a binding legal act regulating the relations between data controller and data processor. This contract shall be in written form for evidence purpose and shall have a minimum content, stipulating in particular that the data processor shall act only on instructions from the controller and implement technical and organizational measures to adequately protect personal data. The contract should include a detailed enough description of the mandate of the processor.

[28] The employer (as original controller) could nevertheless retain some responsibility in case the new processing occurred because of a lack of adequate security measures.

[29] See also Recital 31 of the GDPR

90. The definition covers anyone who receives personal data, whether they are a third party or not. For example, when a controller sends personal data to another entity, either a processor or a third party, this entity is a recipient. A third party recipient shall be considered a controller for any processing that it carries out for its own purpose(s) after it receives the data.

> **Example: Disclosure of data between companies**
>
> The travel agency ExploreMore arranges travels on request from its individual customers. Within this service, they send the customers' personal data to airlines, hotels and organisations of excursions in order for them to carry out their respective services. ExploreMore, the hotels, airlines and excursion providers are each to be seen as controllers for the processing that they carry out within their respective services. There is no controller-processor relation. However, the airlines, hotels and excursion providers are to be seen as recipients when receiving the personal data from ExploreMore.

PART II – CONSEQUENCES OF ATTRIBUTING DIFFERENT ROLES

1 RELATIONSHIP BETWEEN CONTROLLER AND PROCESSOR

91. A distinct new feature in the GDPR are the provisions that impose obligations directly upon processors. For example, a processor must ensure that persons authorised to process the personal data have committed themselves to confidentiality (Article 28(3)); a processor must maintain a record of all categories of processing activities (Article 30(2)) and must implement appropriate technical and organisational measures (Article 32). A processor must also designate a data protection officer under certain conditions (Article 37) and has a duty to notify the controller without undue delay after becoming aware of a personal data breach (Article 33(2)). Furthermore, the rules on transfers of data to third countries (Chapter V) apply to processors as well as controllers. In this regard, the EDPB considers that Article 28(3) GDPR imposes direct obligations upon processors, including the duty to assist the controller in ensuring compliance.

1.1 Choice of the processor

92. The controller has the **duty to use "only processors providing sufficient guarantees** to implement appropriate technical and organisational measures", so that processing meets the requirements of the GDPR - including for the security of processing - and ensures the protection of data subject rights.[30] The controller is therefore responsible for assessing the sufficiency of the guarantees provided by the processor and should be able to prove that it has taken all of the elements provided in the GDPR into serious consideration.

93. The guarantees "provided" by the processor are actually those that the processor is able to **demonstrate to the satisfaction of the controller**, as those are the only ones that can effectively be

[30] Article 28(1) and Recital 81 GDPR.

taken into account by the controller when assessing compliance with its obligations. Often this will require an exchange of relevant documentation (e.g. privacy policy, terms of service, record of processing activities, records management policy, information security policy, reports of external audits, recognised international certifications, like ISO 27000 series).

94. The controller's assessment of whether the guarantees are sufficient is a form of risk assessment, which will greatly depend on the type of processing entrusted to the processor and needs to be made on a case-by-case basis, taking into account the nature, scope, context and purposes of processing as well as the risks for the rights and freedoms of natural persons.

95. The following elements [31] should be taken into account by the controller in order to assess the sufficiency of the guarantees: the processor's **expert knowledge** (e.g. technical expertise with regard to security measures and data breaches); the processor's **reliability**; the processor's **resources**. The reputation of the processor on the market may also be a relevant factor for controllers to consider.

96. Furthermore, the adherence to an approved code of conduct or certification mechanism can be used as an element by which sufficient guarantees can be demonstrated.[32] The processors are therefore advised to inform the controller as to this circumstance, as well as to any change in such adherence.

97. The obligation to use only processors "providing sufficient guarantees" contained in Article 28(1) GDPR is a continuous obligation. It does not end at the moment where the controller and processor conclude a contract or other legal act. Rather the controller should, at appropriate intervals, verify the processor's guarantees, including through audits and inspections where appropriate.[33]

1.2 Form of the contract or other legal act

98. Any processing of personal data by a processor must be governed by a contract or other legal act under EU or Member State law between the controller and the processor, as required by Article 28(3) GDPR.

99. Such legal act must be **in writing, including in electronic form**.[34] Therefore, non-written agreements (regardless of how thorough or effective they are) cannot be considered sufficient to meet the requirements laid down by Article 28 GDPR. To avoid any difficulties in demonstrating that the contract or other legal act is actually in force, the EDPB recommends ensuring that the necessary signatures are included in the legal act.

100. Furthermore, the contract or the other legal act under Union or Member State law must be **binding on the processor** with regard to the controller, i.e. it must establish obligations on the processor that are binding as a matter of EU or Member State law. Also it must set out the obligations of the controller. In most cases, there will be a contract, but the Regulation also refers to "other legal act", such as a national law (primary or secondary) or other legal instrument. If the legal act does not include all the minimum required content, it must be supplemented with a contract or another legal act that includes the missing elements.

[31] Recital 81 GDPR.
[32] Article 28(5) and Recital 81 GDPR.
[33] See also Article 28(3)h GDPR.
[34] Article 28(9) GDPR.

101. Since the Regulation establishes a clear obligation to enter into a written contract, where no other relevant legal act is in force, the absence thereof is an infringement of the GDPR.[35] Both the controller and processor are responsible for ensuring that there is a contract or other legal act to govern the processing.[36] Subject to the provisions of Article 3 of the GDPR, the competent supervisory authority will be able to direct an administrative fine against both the controller and the processor, taking into account the circumstances of each individual case. Contracts that have been entered into before the date of application of the GDPR should have been updated in light of Article 28(3). The absence of such update, in order to bring a previously existing contract in line with the requirements of the GDPR, constitutes an infringement of Article 28(3).

102. In order to comply with the duty to enter into a contract, **the controller and the processor may choose to negotiate their own contract** including all the compulsory elements **or to rely, in whole or in part, on standard contractual clauses in relation to obligations under Article 28**.[37]

103. A set of standard contractual clauses (SCCs) may be, alternatively, adopted by the Commission[38] or adopted by a supervisory authority, in accordance with the consistency mechanism.[39] These clauses could be part of a certification granted to the controller or processor pursuant to Articles 42 or 43.[40]

104. The EDPB would like to clarify that there is no obligation for controllers and processors to enter into a contract based on SCCs, nor is it to be necessarily preferred over negotiating an individual contract. Both options are viable for the purposes of compliance with data protection law, depending on the specific circumstances, as long as they meet the Article 28(3) requirements.

105. If the parties wish to take advantage of standard contractual clauses, the data protection clauses of their agreement must be the same as those of the SCCs. The SCCs will often leave some blank spaces to be filled in or options to be selected by the parties. Also, the SCCs will generally be embedded in a larger agreement describing the object of the contract, its financial conditions, and other agreed clauses: it will be possible for the parties to add additional clauses (e.g. applicable law and jurisdiction)

[35] The presence (or absence) of a written arrangement, however, is not decisive for the existence of a controller-processor relationship. Where there is reason to believe that the contract does not correspond with reality in terms of actual control, the agreement may be set aside. Conversely, a controller-processor relationship might still be held to exist in absence of a written processing agreement. This would, however, imply a violation of Article 28(3) GDPR. Moreover, in certain circumstances, the absence of a clear definition of the relationship between the controller and the processor may raise the problem of the lack of legal basis on which every processing should be based, e.g. in respect of the communication of data between the controller and the alleged processor.

[36] Article 28(3) is not only applicable to controllers. In the situation where only the processor is subject to the territorial scope of the GDPR, the obligation shall only be directly applicable to the processor, see also EDPB Guidelines 3/2018 on the territorial scope of the GDPR, p. 12.

[37] Article 28(6) GDPR. The EDPB recalls that standard contractual clauses for the purposes of compliance with Article 28 GDPR are not the same as standard contractual clauses referred to in Article 46(2). While the former further stipulate and clarify how the provisions of Article 28(3) and (4) will be fulfilled, the latter provide appropriate safeguards in case of transfer of personal data to a third country or an international organisation in the absence of an adequacy decision pursuant to Article 45(3).

[38] Article 28(7) GDPR.

[39] Article 28(8) GDPR. The Register for Decisions taken by supervisory authorities and courts on issues handled in the consistency mechanism, including standard contractual clauses for the purposes of compliance with art. 28 GDPR, can be accessed here: https://edpb.europa.eu/our-work-tools/consistency-findings/register-for-decisions

[40] Article 28(6) GDPR.

as long as they do not contradict, directly or indirectly, the SCCs[41] and they do not undermine the protection afforded by the GDPR and EU or Member State data protection laws.

106. Contracts between controllers and processors may sometimes be drafted unilaterally by one of the parties. Which party or parties that draft the contract may depend on several factors, including: the parties' position in the market and contractual power, their technical expertise, as well as access to legal services. For instance, some service providers tend to set up standard terms and conditions, which include data processing agreements.

~~In this respect, it should be noted that in many cases service providers specialized in certain processing of data (for example, payment of salaries) will set up standard services and contracts to be signed by data controllers, de facto setting a certain standard manner of processing personal data[18]. However,~~107. The fact that the contract and its detailed terms of business are prepared by the service provider rather than by the controller is not in itself problematic and is not in itself a sufficient basis to conclude that the service provider should be considered as a controller~~, in so far as the controller has freely accepted the contractual terms, thus accepting full responsibility for them.~~

. Also, ~~In the same line,~~ the imbalance in the contractual power of a small data controller with respect to big service providers should not be considered as a justification for the controller to accept clauses and terms of contracts which are not in compliance with data protection law~~.~~, nor can it discharge the controller from its data protection obligations. The controller must evaluate the terms and in so far as it freely accepts them and makes use of the service, it has also accepted full responsibility for compliance with the GDPR. Any proposed modification, by a processor, of data processing agreements included in standard terms and conditions should be directly notified to and approved by the controller. The mere publication of these modifications on the processor's website is not compliant with Article 28.

~~Example No. 18: Email platforms~~

~~John Smith looks for an email platform to be used by himself and the five employees of his company. He discovers that a suitable user-friendly platform - and also the only one offered for free - keeps personal data for an excessive amount of time and transfers them to third countries without adequate safeguards. Furthermore, the contractual terms are "take it or leave it".~~

~~In this case, Mr Smith should either look for another provider or - in case of alleged non compliance with data protection rules or lack of availability in the market of other suitable providers - refer the matter to competent authorities, such as DPAs, consumer protection and antitrust authorities, etc.~~

1.3 Content of the contract or other legal act

108. Before focusing on each of the detailed requirements set out by the GDPR as to the content of the contract or other legal act, some general remarks are necessary.

109. While the elements laid down by Article 28 of the Regulation constitute the core content of the agreement, the contract should be a way for the controller and the processor to further clarify how such core elements are going to be implemented with detailed instructions. Therefore, **the processing agreement should not merely restate the provisions of the GDPR**: rather, it should include more specific, concrete information as to how the requirements will be met and which level of security is required for the personal data processing that is the object of the processing agreement. Far from being a pro-forma exercise, the negotiation and stipulation of the contract are a chance to specify

details regarding the processing.[42] Indeed, the "protection of the rights and freedoms of data subjects as well as the responsibility and liability of controllers and processors [...] requires a clear allocation of the responsibilities" under the GDPR.[43]

~~The fact that the Directive requires a written contract to ensure security of processing does not mean that there cannot be controllers/processors relations without prior contracts. In this perspective, the contract is neither constitutive nor decisive, even if it~~

[41] The EDPB recalls that the same degree of flexibility is allowed when the parties choose to use SCCs as appropriate safeguard for transfers to third countries pursuant to Article 46(2)(c) or Article 46(2)(d) GDPR. Recital 109 GDPR clarifies that "*The possibility for the controller or processor to use standard data-protection clauses adopted by the Commission or by a supervisory authority should prevent controllers or processors neither from including the standard data-protection clauses in a wider contract, such as a contract between the processor and another processor, nor from adding other clauses or additional safeguards provided that they do not contradict, directly or indirectly, the standard contractual clauses [...] or prejudice the fundamental rights or freedoms of the data subjects. Controllers and processors should be encouraged to provide additional safeguards via contractual commitments that supplement standard protection clauses*".

[42] See also EDPB Opinion 14/2019 on the draft Standard Contractual Clauses submitted by the DK SA (Article 28(8) GDPR), p. 5.

[43] Recital 79 GDPR.

~~[18] The elaboration of the terms of the contract by the service provider is without prejudice to the fact that essential aspects of the processing, as described in point III.1.b, are determined by the controller.~~

110. At the same time, the contract should **take into account "*the specific tasks and responsibilities of the processor in the context of the processing to be carried out and the risk to the rights and freedoms of the data subject*"**.[44] Generally speaking, the contract between the parties should be drafted in light of the specific data processing activity. For instance, there is no need to impose particularly stringent protections and procedures on a processor entrusted with a processing activity from which only minor risks arise: while each processor must comply with the requirements set out by the Regulation, the measures and procedures should be tailored to the specific situation. In any event, all elements of Article 28(3) must be covered by the contract. At the same time, the contract should include some elements that may help the processor in understanding the risks to the rights and freedoms of data subjects arising from the processing: because the activity is performed on behalf of the controller, often the controller has a deeper understanding of the risks that the processing entails since the controller is aware of the circumstances in which the processing is embedded.

111. Moving on to the **required content** of the contract or other legal act, EDPB interprets Article 28(3) in a way that it needs to set out:

- the **subject-matter** of the processing (for instance, video surveillance recordings of people entering and leaving a high-security facility). While the subject matter of the processing is a broad concept, it needs to be formulated with enough specifications so that it is clear what the main object of the processing is;
- the **duration**[45] of the processing: the exact period of time, or the criteria used to determine it, should be specified; for instance, reference could be made to the duration of the processing agreement;
- the **nature** of the processing: the type of operations performed as part of the processing (for instance: "filming", "recording", "archiving of images", ...) **and purpose** of the processing (for instance: detecting unlawful entry). This description should be as comprehensive as possible, depending on the specific processing activity, so as to allow external parties (e.g. supervisory authorities) to understand the content and the risks of the processing entrusted to the processor.
- the **type of personal data**: this should be specified in the most detailed manner as possible (for instance: video images of individuals as they enter and leave the facility). It would not be adequate merely to specify that it is "personal data pursuant to Article 4(1) GDPR" or "special categories of personal data pursuant to Article 9". In case of special categories of data, the contract or legal act should at least specify which types of data are concerned, for example, "information regarding health records", or "information as to whether the data subject is a member of a trade union";
- the **categories of data subjects**: this, too, should be indicated in a quite specific way (for instance: "visitors", "employees", delivery services etc.);
- the **obligations and rights of the controller**: the rights of the controller are further dealt with in the following sections (e.g. with respect to the right of the controller to perform inspections and audits). As regards the obligations of the controller, examples include the controller's obligation to provide the processor with the data mentioned in the contract, to provide and document, in

[44] Recital 81 GDPR.
[45] The duration of the processing is not necessarily equivalent to the duration of the agreement (there may be legal obligations to keep the data longer or shorter).

writing, any instruction bearing on the processing of data by the processor, to ensure, before and throughout the processing, compliance with the obligations set out in the GDPR on the processor's part, to supervise the processing, including by conducting audits and inspections with the processor.

112. While the GDPR lists elements that always need to be included in the agreement, other relevant information may need to be included, depending on the context and the risks of the processing as well as any additional applicable requirement.

1.3.1 The processor must only process data on documented instructions from the controller (Art. 28(3)(a) GDPR)

113. The need to specify this obligation stems from the fact that the processor processes data on behalf of the controller. Controllers must provide its processors with instructions related to each processing activity. Such instructions can include permissible and unacceptable handling of personal data, more detailed procedures, ways of securing data, etc. The processor shall not go beyond what is instructed by the controller.

114. When a processor processes data outside or beyond the controller's instructions, and this amounts to a decision determining the purposes and means of processing, the processor will be in breach of its obligations and will even be considered a controller in respect of that processing in accordance with Article 28(10) (see section 1.5 below).

115. Because such instructions must be **documented**, it is recommended to include a procedure and a template for giving further instructions in an annex to the contract or other legal act. Alternatively, they can be provided in any written form (e.g. e-mail), as long as it is possible to keep records of such instructions. In any event, to avoid any difficulties in demonstrating that the controller's instructions have been duly documented, the EDPB recommends keeping such instructions together with the contract or other legal act.

116. The duty for the processor to refrain from any processing activity not based on the controller's instructions also applies to **transfers** of personal data to a third country or international organisation. The contract should specify the requirements for transfers to third countries or international organisations, taking into account the provisions of Chapter V of the GDPR.

117. The EDPB recommends that controller pay due attention to this specific point especially when the processor is going to delegate some processing activities to other processors, and when the processor has divisions or units located in third countries. If the instructions by the controller do not allow for transfers or disclosures to third countries, the processor will not be allowed to assign the processing to a sub-processor in a third country, nor will he be allowed to have the data processed in one of his non-EU divisions.

118. A processor may process data other than on documented instructions of the controller **when the processor is required to process and/or transfer personal data on the basis of EU law or Member State law to which the processor is subject**. This provision further reveals the importance of carefully negotiating and drafting data processing agreements, as, for example, legal advice may need to be sought by either party as to the existence of any such legal requirement. This needs to be done in a timely fashion, as the processor has an obligation to inform the controller of such requirement before starting the processing. Only when that same (EU or Member State) law forbids the processor to inform the controller on "important grounds of public interest", there is no such information obligation. In

any case, any transfer or disclosure may only take place if authorised by Union law, including in accordance with Article 48 of the GDPR.

1.3.2 The processor must ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality (Art. 28(3)(b) GDPR)

119. The contract must say that the processor needs to ensure that anyone it allows to process the personal data is committed to confidentiality. This may occur either via a specific contractual agreement, or due to statutory obligations already in place.

120. The broad concept of "persons authorised to process the personal data" includes employees and temporary workers. Generally speaking, the processor should make the personal data available only to the employees who actually need them to perform tasks for which processor was hired by the controller.

121. The commitment or obligation of confidentiality must be "appropriate", i.e. it must effectively forbid the authorised person from disclosing any confidential information without authorisation, and it must be sufficiently broad so as to encompass all the personal data processed on behalf of the controller as well as the details concerning the relationship.

1.3.3 The processor must take all the measures required pursuant to Article 32 (Art. 28(3)(c) GDPR)

122. Article 32 requires the controller and the processor to implement appropriate technical and organisational security measures. While this obligation is already directly imposed on the processor whose processing operations fall within the scope of the GDPR, the duty to take all measures required pursuant to Article 32 still needs to be reflected in the contract concerning the processing activities entrusted by the controller.

123. As indicated earlier, the processing contract should not merely restate the provisions of the GDPR. The contract needs to include or reference information as to the security measures to be adopted**, an obligation on the processor to obtain the controller's approval before making changes**, and a regular review of the security measures so as to ensure their appropriateness with regard to risks, which may evolve over time. The degree of detail of the information as to the security measures to be included in the contract must be such as to enable the controller to assess the appropriateness of the measures pursuant to Article 32(1) GDPR. Moreover, the description is also necessary in order to enable the controller to comply with its accountability duty pursuant to Article 5(2) and Article 24 GDPR as regards the security measures imposed on the processor. A corresponding obligation of the processor to assist the controller and to make available all information necessary to demonstrate compliance can be inferred from Art. 28.3 (f) and (h) GDPR.

124. The level of instructions provided by the controller to the processor as to the measures to be implemented will depend on the specific circumstances. In some cases, the controller may provide a clear and detailed description of the security measures to be implemented. In other cases, the controller may describe the minimum security objectives to be achieved, while requesting the processor to propose implementation of specific security measures. In any event, the controller must provide the processor with a description of the processing activities and security objectives (based on the controller's risk assessment), as well as approve the measures proposed by the processor. This could be included in an annex to the contract. The controller exercises its decision-making power over

the main features of the security measures, be it by explicitly listing the measures or by approving those proposed by the processor.

1.3.4 The processor must respect the conditions referred to in Article 28(2) and 28(4) for engaging another processor (Art. 28(3)(d) GDPR).

125. The agreement must specify that the processor may not engage another processor without the controller's prior written authorisation and whether this authorisation will be specific or general. In case of general authorisation, the processor has to inform the controller of any change of sub-processors under a written authorisation, and give the controller the opportunity to object. It is recommended that the contract set out the process for this. It should be noted that the processor's duty to inform the controller of any change of sub-processors implies that the processor actively indicates or flags such changes toward the controller.[46] Also, where specific authorisation is required, the contract should set out the process for obtaining such authorisation.

126. When the processor engages another processor, a contract must be put in place between them, imposing the same data protection obligations as those imposed on the original processor or these obligations must be imposed by another legal act under Union or Member State law. This includes the obligation under Article 28(3)(h) to allow for and contribute to audits by the controller or another auditor mandated by the controller.[47] The processor is liable to the controller for the other processors' compliance with data protection obligations (for further details on the recommended content of the agreement see section1.6 below).

1.3.5 The processor must assist the controller for the fulfilment of its obligation to respond to requests for exercising the data subject's rights (Article 28(3) (e) GDPR).

127. While ensuring that data subjects requests are dealt with is up to the controller, the contract must stipulate that the processor has an obligation to provide assistance "by appropriate technical and organisational measures, insofar as this is possible". The nature of this assistance may vary greatly "taking into account the nature of the processing" and depending on the type of activity entrusted to the processor. The details concerning the assistance to be provided by the processor should be included in the contract or in an annex thereto.

128. While the assistance may simply consist in promptly forwarding any request received, in some circumstances the processor will be given more specific, technical duties, especially when it is in the position of extracting and managing the personal data.

129. It is crucial to bear in mind that, although the practical management of individual requests can be outsourced to the processor, the controller bears the responsibility for complying with such requests. Therefore, the assessment as to whether requests by data subjects are admissible and/or the requirements set by the GDPR are met should be performed by the controller, either on a case-by-case basis or through clear instructions provided to the processor in the contract before the start of the processing. Also, the deadlines set out by Chapter III cannot be extended by the controller based on the fact that the necessary information must be provided by the processor.

[46] In this regard it is, by contrast, e.g. not sufficient for the processor to merely provide the controller with a generalized access to a list of the sub-processors which might be updated from time to time, without pointing to each new sub-processor envisaged. In other words, the processor must actively inform the controller of any change to the list (i.e. in particular of each new envisaged sub-processor).

[47] See also EDP Opinion 14/2019 on the draft Standard Contractual Clauses submitted by the DK SA (Article 28(8) GDPR), 9 July 2019, at paragraph 44.

~~may help to better understand the relations between the parties[19]. Therefore, also in this case a functional approach shall be applied, analysing the factual elements of the relations between the different subjects and the way purposes and means of the processing are determined. In case a controller/processor relation appears to exist, these parties are obliged to conclude a contract according to the law (cf. Article 17 of the Directive).~~

1.3.6 The processor must assist the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 (Art. 28(3)(f) GDPR).

130. It is necessary for the contract to avoid merely restating these duties of assistance: **the agreement should contain details as to how the processor is asked to help the controller meet the listed obligations**. For example, procedures and template forms may be added in the annexes to the agreement, allowing the processor to provide the controller with all the necessary information.

131. The type and degree of assistance to be provided by the processor may vary widely "*taking into account the nature of processing and the information available to the processor".* The controller must adequately inform the processor as to the risk involved in the processing and as to any other circumstance that may help the processor meet its duty.

132. Moving on to the specific obligations, the processor has, first, a duty to assist the controller in meeting the obligation to adopt adequate technical and organisational measures to ensure security of processing.[48] While this may overlap, to some extent, with the requirement that the processor itself adopts adequate security measures, where the processing operations of the processor fall within the scope of the GDPR, they remain two distinct obligations, since one refers to the processor's own measures and the other refers to the controller's.

133. Secondly, the processor must assist the controller in meeting the obligation to notify personal data breaches to the supervisory authority and to data subjects. The processor must notify the controller whenever it discovers a personal data breach affecting the processor's or a sub-processor's facilities / IT systems and help the controller in obtaining the information that need to be stated in the report to the supervisory authority.[49] The GDPR requires that the controller notify a breach without undue delay in order to minimize the harm for individuals and to maximize the possibility to address the breach in an adequate manner. Thus, the processor's notification to the data controller should also take place without undue delay.[50] The EDPB recommends that there is a specific time frame of notification (e.g. number of hours) and the point of contact for such notifications be provided in the contract.[51] The contract should finally specify how the processor shall notify the controller in case of a breach.

134. Furthermore, the processor must also assist the controller in carrying out data protection impact assessments when required, and in consulting the supervisory authority when the outcome reveals that there is a high risk that cannot be mitigated.

135. The duty of assistance does not consist in a shift of responsibility, as those obligations are imposed on the controller. For instance, although the data protection impact assessment can in practice be carried out by a processor, the controller remains accountable for the duty to carry out the assessment[52] and the processor is only required to assist the controller "where necessary and upon request."[53] As a

~~*Plurality of processors*~~

~~It increasingly happens that processing of personal data is outsourced by a controller to several data processors. These processors may have a direct relationship with the data controller, or be sub-contractors to which the processors have delegated part of the processing activities entrusted to them.~~

These complex (multi-level or diffused) structures of processing personal data are increasing with new technologies and some national laws explicitly refer to them. Nothing in the Directive prevents that on account of organizational requirements, several entities may be designated as data processors or (sub-)processors also by subdividing the relevant tasks. However, all of them are to abide by the instructions given by the data controller in carrying out the processing.

[48] Article 32 GDPR.
[49] Article 33(3) GDPR.
[50] For more information, see the Guidelines on Personal data breach notification under Regulation 2016/679, WP250rev.01, 6 February 2018, p. 13-14.
[51] See also EDP Opinion 14/2019 on the draft Standard Contractual Clauses submitted by the DK SA (Article 28(8) GDPR), 9 July 2019, at paragraph 40.
[52] Article 29 Data Protection Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP 248 rev.01, p. 14
[53] Recital 95 GDPR.

The strategic issue here is that - with a plurality of actors involved in the process - the obligations and responsibilities stemming from data protection legislation should be clearly allocated and not dispersed along the chain of outsourcing/subcontracting. In other words, one should avoid a chain of (sub-)processors that would dilute or even prevent effective control and clear responsibility for processing activities, unless the responsibilities of the various parties in the chain are clearly established.

In this perspective, in the same line as described above in paragraph III.1.b - while it is not necessary that the controller defines and agrees on all the details of the means used to pursue the envisaged purposes - it would still be necessary that he is at least informed of the main elements of the processing structure (for example, subjects involved, security

[19] However, in some cases, the existence of a written contract can constitute a necessary condition to automatically qualify as a processor in certain contexts. In Spain, for example, the report on call- centres defines as processors all call centres in third countries, as long as they are complying with the contract. This is the case even if the contract has been drafted by the processor and the controller merely "adheres" to it.

result, the controller is the one that must take the initiative to perform the data protection impact assessment, not the processor.

1.3.7 On termination of the processing activities, the processor must, at the choice of the controller, delete or return all the personal data to the controller and delete existing copies (Art. 28(3)(g) GDPR).

136. The contractual terms are meant to ensure that the personal data are subject to appropriate protection after the end of the "provision of services related to the processing": it is therefore up to the controller to decide what the processor should do with regard to the personal data.

137. The controller can decide at the beginning whether personal data shall be deleted or returned by specifying it in the contract, through a written communication to be timely sent to the processor. The contract or other legal act should reflect the possibility for the data controller to change the choice made before the end of the provision of services related to the processing. The contract should specify the process for providing such instructions.

138. If the controller chooses that the personal data be deleted, the processor should ensure that the deletion is performed in a secure manner, also in order to comply with Article 32 GDPR. The processor should confirm to the controller that the deletion has been completed within an agreed timescale and in an agreed manner.

139. The processor must delete all existing copies of the data, unless EU or Member State law requires further storage. If the processor or controller is aware of any such legal requirement, it should inform the other party as soon as possible.

1.3.8 The processor must make available to the controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller (Art. 28(3)(h) GDPR).

140. The contract shall include details on how often and how the flow of information between the processor and the controller should take place so that the controller is fully informed as to the details of the processing. For instance, the relevant portions of the processor's records of processing activities may be shared with the controller. The processor should provide all information on how the processing activity will be carried out on behalf of the controller. Such information should include information on the functioning of the systems used, security measures, retention of data, data location, transfers of data, access to data and recipients of data, sub-processors used, etc.

141. Further details shall also be set out in the contract regarding the ability to carry out and the duty to contribute to inspections and audits by the controller or another auditor mandated by the controller. The parties should cooperate in good faith and assess whether and when there is a need to perform audits on the processor's premises. Likewise, specific procedures should be established regarding the processor's and the controller's inspection of sub-processors (see section 1.6 below).

1.4 Instructions infringing data protection law

142. According to Article 28(3), the processor must immediately inform the controller if, in its opinion, an instruction infringes the GDPR or other Union or Member State data protection provisions.

~~measures, guarantees for processing in third countries, etc), so that he is still in a position to be in control of the data processed on his behalf.~~

143. Indeed, the processor has a duty to comply with the controller's instructions, but it also has a general obligation to comply with the law. An instruction that infringes data protection law seems to cause a conflict between the aforementioned two obligations.

144. Once informed that one of its instructions may be in breach of data protection law, the controller will have to assess the situation and determine whether the instruction actually violates data protection law.

145. The EDPB recommends the parties to negotiate and agree in the contract the consequences of the notification of an infringing instruction sent by the processor and in case of inaction from the controller in this context. One example would be to insert a clause on the termination of the contract if the controller persists with an unlawful instruction.

1.5 Processor determining purposes and means of processing

~~It shall also be considered that, while the Directive imposes liability on the controller, it does not prevent national data protection laws from providing that, in addition, also the processor should be considered liable in certain cases.~~

146. If the processor infringes the Regulation by determining the purposes and means of processing, it shall be considered as a controller in respect of that processing (Article 28(10) GDPR).

1.6 Sub-processors

~~Some criteria may be helpful in determining the qualification of the various subjects involved:~~

147. Data processing activities are often carried out by a great number of actors, and the chains of subcontracting are becoming increasingly complex. The GDPR introduces specific obligations that are triggered when a processor intends to engage another player, thereby adding another link to the chain.

148. Although the chain may be quite long, the controller retains its pivotal role in determining the purpose and means of processing. Article 28(2) GDPR stipulates that the processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor must inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes. In both cases, the processor must obtain the controller's authorisation in writing before any personal data processing is entrusted to the sub-processor. In order to make the assessment and the decision whether to authorise subcontracting, a list of intended sub-processors (including per each: their locations, what they will be doing and proof of what safeguards have been implemented) will have to be provided to the data controller by the processor[54].

149. The prior written authorisation may be specific, i.e. referring to a specific sub-processor for a specific processing activity and at a specific time, or general. This should be specified in the contract or other legal act that governs the processing.

150. In cases where the controller decides to accept certain sub-processors at the time of the signature of the contract, a list of approved sub-processors should be included in the contract or an annex thereto. The list should then be kept up to date, in accordance with the general or specific authorisation given by the controller.

151. If the controller chooses to give its **specific authorisation**, it should specify in writing which sub-processor and what processing activity it refers to. Any subsequent change will need to be further

authorised by the controller before it is put in place. If the processor's request for a specific authorisation is not answered to within the set timeframe, it should be held as denied. The controller

- ~~Level of prior instructions given by the data controller, which determines the margin of manoeuvre left to the data processor;~~

- ~~Monitoring by the data controller of the execution of the service. A constant and careful supervision by the controller to ensure thorough compliance of the processor with instructions and terms of contract provides an indication that the controller is still in full and sole control of the processing operations;~~

[54] This information is needed, so that the controller can comply with the accountability principle in Article 24 and with provisions of Articles 28(1), 32 and Chapter V of the GDPR.

should make its decision to grant or withhold authorisation taking into account its obligation to only use processors providing "sufficient guarantees" (see section 1.1 above).

152. Alternatively, the controller may provide its **general authorisation** to the use of sub-processors (in the contract, including a list with such sub-processors in an annex thereto), which should be supplemented with criteria to guide the processor's choice (e.g., guarantees in terms of technical and organisational measures, expert knowledge, reliability and resources)[55]. In this scenario, the processor needs to inform the controller in due time of any intended addition or replacement of sub-processor(s) so as to provide the controller with the opportunity to object.

153. Therefore, the main difference between the specific authorisation and the general authorisation scenarios lies in the meaning given to the controller's silence: in the general authorisation situation, the controller's failure to object within the set timeframe can be interpreted as authorisation.

154. In both scenarios, the contract should include details as to the timeframe for the controller's approval or objection and as to how the parties intend to communicate regarding this topic (e.g. templates). Such timeframe needs to be reasonable in light of the type of processing, the complexity of the activities entrusted to the processor (and the sub-processors) and the relationship between the parties.

155. Regardless of the criteria suggested by the controller to choose providers, the processor remains fully liable to the controller for the performance of the sub-processors' obligations (Article 28(4) GDPR).

156. Furthermore, when a processor intends to employ an (authorised) sub-processor, it must enter into a contract with it that imposes the same obligations as those imposed on the first processor by the controller or the obligations must be imposed by another legal act under EU or Member State law. The whole chain of processing activities needs to be regulated by written agreements.

157. Imposing the "same" obligations should be construed in a functional rather than in a formal way: it is not necessary for the contract to include exactly the same words as those used in the contract between the controller and the processor, but it should ensure that the obligations in substance are the same. This also means that if the processor entrusts the sub-processor with a specific part of the processing, to which some of the obligations cannot apply, such obligations should not be included "by default" in the contract with the sub-processor, as this would only generate uncertainty.

2 CONSEQUENCES OF JOINT CONTROLLERSHIP

2.1 Determining in a transparent manner the respective responsibilities of joint controllers for compliance with the obligations under the GDPR

158. Article 26(1) of the GDPR provides that joint controllers shall in a transparent manner determine and agree on their respective responsibilities for compliance with the obligations under the Regulation.

159. Joint controllers thus need to set "who does what" by deciding between themselves who will have to carry out which tasks in order to make sure that the processing complies with the applicable

[55] This duty of the controller stems from the accountability principle in Article 24 and from the obligation to comply with provisions of Articles 28(1), 32 and Chapter V of the GDPR.

obligations under the GDPR in relation to the joint processing at stake. In other words, a distribution of responsibilities for compliance is to be made as resulting from the use of the term "*respective*" in Article 26(1).

160. The objective of these rules is to ensure that where multiple actors are involved, especially in complex data processing environments, responsibility for compliance with data protection rules is clearly allocated in order to avoid that the protection of personal data is reduced, or that a negative conflict of competence lead to loopholes whereby some obligations are not complied with by any of the parties involved in the processing. It should be made clear here that all responsibilities have to be allocated according to the factual circumstances in order to achieve an operative agreement.

161. More specifically, Article 26(1) specifies that the determination of their respective responsibilities (i.e. tasks) for compliance with the obligations under the GDPR is to be carried out by joint controllers "*in particular*" as regards the exercising of the rights of the data subject and the duties to provide information referred in Articles 13 and 14, 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.

162. It is clear from this provision that joint controllers need to define who respectively will be in charge of answering to requests when data subjects exercise their rights granted by the GDPR and of providing information to them as required by Articles 13 and 14 of the GDPR. However, the use of the terms "*in particular*" indicates that the obligations subject to the allocation of responsibilities for compliance by each party involved as referred in this provision are non-exhaustive. It follows that the distribution of the responsibilities for compliance among joint controllers is not limited to the topics referred in Article 26(1) but extends to other controller's obligations under the GDPR. Indeed, joint controllers need to ensure that the whole joint processing fully complies with the GDPR.

163. In this perspective, the compliance measures and related obligations joint controllers should consider when determining their respective responsibilities, in addition to those specifically referred in Article 26(1), include amongst others without limitation:

- Implementation of general data protection principles (Article 5)
- Legal basis of the processing[56] (Article 6)
- Security measures (Article 32)
- Notification of a personal data breach to the supervisory authority and to the data subject[57] (Articles 33 and 34)
- Data Protection Impact Assessments (Articles 35 and 36)[58]

[56] Although the GDPR does not preclude joint controllers to use different legal basis for different processing operations they carry out, it is recommended to use, whenever possible, the same legal basis for a particular purpose.

[57] Please also see EDPB guidelines on Personal data breach notification under Regulation 2016/679, WP250.rev.01 which provide that joint controllership will include "*determining which party will have responsibility for complying with the obligations under Articles 33 and 34. WP29 recommends that the contractual arrangements between joint controllers include provisions that determine which controller will take the lead on, or be responsible for, compliance with the GDPR's breach notification obligations*"(p.13).

[58] Please also see EDPB guidelines on DPIAs, WP248.rev01 which provide the following: "*When the processing operation involves joint controllers, they need to define their respective obligations precisely. Their DPIA should set out which party is responsible for the various measures designed to treat risks and to protect the rights and*

- The use of a processor (Article 28)
- Transfers of data to third countries (Chapter V)
- Organisation of contact with data subjects and supervisory authorities

164. Other topics that could be considered depending on the processing at stake and the intention of the parties are for instance the limitations on the use of personal data for another purpose by one of the joint controllers. In this respect, both controllers always have a duty to ensure that they both have a legal basis for the processing. Sometimes, in the context of joint controllership, personal data are shared by one controller to another. As a matter of accountability, each controller has the duty to ensure that the data are not further processed in a manner that is incompatible with the purposes for which they were originally collected by the controller sharing the data.[59]

165. Joint controllers can have a certain degree of flexibility in distributing and allocating obligations among them as long as they ensure full compliance with the GDPR with respect of the given processing. The allocation should take into account factors such as, who is competent and in a position to effectively ensure data subject's rights as well as to comply with the relevant obligations under the GDPR. The EDPB recommends documenting the relevant factors and the internal analysis carried out in order to allocate the different obligations. This analysis is part of the documentation under the accountability principle.

166. The obligations do not need to be equally distributed among the joint controllers. In this respect, the CJEU has recently stated that "*the existence of joint responsibility does not necessarily imply equal responsibility of the various operators involved in the processing of personal data*"[60].

167. However, there may be cases where not all of the obligations can be distributed and all joint controllers may need to comply with the same requirements arising from the GDPR, taking into account the nature and context of the joint processing. For instance, joint controllers using shared data processing tools or systems both need to ensure compliance with notably the purpose limitation principle and implement appropriate measures to ensure the security of personal data processed under the shared tools.

168. Another example is the requirement for each joint controller to maintain a record of processing activities or to designate a Data Protection Officer (DPO) if the conditions of Article 37(1) are met. Such requirements are not related to the joint processing but are applicable to them as controllers.

2.2 Allocation of responsibilities needs to be done by way of an arrangement

2.2.1 Form of the arrangement

169. Article 26(1) of the GDPR provides as a new obligation for joint controllers that they should determine their respective responsibilities "*by means of an arrangement between them*". The legal form of such

freedoms of the data subjects. Each data controller should express his needs and share useful information without either compromising secrets (e.g.: protection of trade secrets, intellectual property, confidential business information) or disclosing vulnerabilities" (p.7).

[59] Each disclosure by a controller requires a lawful basis and assessment of compatibility, regardless of whether the recipient is a separate controller or a joint controller. In other words, the existence of a joint controller relationship does not automatically mean that the joint controller receiving the data can also lawfully process the data for additional purposes which are beyond the scope of joint control.

[60] Judgment in *Wirtschaftsakademie*, C-210/16, ECLI:EU:C:2018:388, paragraph 43.

arrangement is not specified by the GDPR. Therefore, joint controllers are free to agree on the form of the arrangement.

170. In addition, the arrangement on the allocation of responsibilities is binding upon each of the joint controllers. They each agree and commit *vis-à-vis* each other on being responsible for complying with the respective obligations stated in their arrangement as their responsibility.

171. Therefore, for the sake of legal certainty, even if there is no legal requirement in the GDPR for a contract or other legal act, the EDPB recommends that such arrangement be made in the form of a binding document such as a contract or other legal binding act under EU or Member State law to which the controllers are subject. This would provide certainty and could be used to evidence transparency and accountability. Indeed, in case of non-compliance with the agreed allocation provided in the arrangement, its binding nature allows one controller to seek the liability of the other for what was stated in the agreement as falling under its responsibility. Also, in line with the accountability principle, the use of a contract or other legal act will allow joint controllers to demonstrate that they comply with the obligations imposed upon them by the GDPR.

172. The way responsibilities, i.e. the tasks, are allocated between each joint controller has to be stated in a clear and plain language in the arrangement[61]. This requirement is important as it ensures legal certainty and avoid possible conflicts not only in the relation between the joint controllers but also vis-à-vis the data subjects and the data protection authorities.

173. To better frame the allocation of responsibilities between the parties, the EDPB recommends that the arrangement also provide general information on the joint processing by notably specifying the subject matter and purpose of the processing, the type of personal data, and the categories of data subjects.

2.2.2. Obligations towards data subjects

174. The GDPR provides several obligations of joint controllers towards data subjects:

The arrangement shall duly reflect the respective roles and relationships of the joint controllers *vis-à-vis* the data subjects

175. As a complement to what is explained above in section 2.1 of the present guidelines, it is important that the joint controllers clarify in the arrangement their respective role, "*in particular*" as regards the exercise of the rights of the data subject and their duties to provide the information referred to in Articles 13 and 14. Article 26 of the GDPR stresses the importance of these specific obligations. The joint controllers must therefore organise and agree on how and by whom the information will be provided and how and by whom the answers to the data subject's requests will be provided. Irrespective of the content of the arrangement on this specific point, the data subject may contact either of the joint controllers to exercise his or her rights in accordance with Article 26(3) as further explained below.

176. The way these obligations are organised in the arrangement should "*duly*", i.e. accurately, reflect the reality of the underlying joint processing. For example, if only one of the joint controllers communicates with the data subjects for the purpose of the joint processing, such controller could be in a better position to inform the data subjects and possibly to answer their requests.

[61] As stated in recital 79 of the GDPR *"(...) the responsibility and liability of controllers and processors, also in relation to the monitoring by and measures of supervisory authorities, requires a clear allocation of the responsibilities under this Regulation, including where a controller determines the purposes and means of the processing jointly with other controllers*".

The essence of the arrangement shall be made available to the data subject

177. This provision is aimed to ensure that the data subject is aware of the "*essence of the arrangement*". For example, it must be completely clear to a data subject which data controller serves as a point of contact for the exercise of data subject rights (notwithstanding the fact that he or she can exercise his or her rights in respect of and against each joint controller). The obligation to make the essence of the arrangement available to data subjects is important in case of joint controllership in order for the data subject to know which of the controllers is responsible for what.

178. What should be covered by the notion of "*essence of the arrangement*" is not specified by the GDPR. The EDPB recommends that the essence cover at least all the elements of the information referred to in Articles 13 and 14 that should already be accessible to the data subject, and for each of these elements, the arrangement should specify which joint controller is responsible for ensuring compliance with these elements. The essence of the arrangement must also indicate the contact point, if designated.

179. The way such information shall be made available to the data subject is not specified. Contrary to other provisions of the GDPR (such as Article 30(4) for the record of processing or Article 40(11) for the register of approved codes of conduct), Article 26 does not indicate that the availability should be "*upon request*" nor "*publicly available by way of appropriate means*". Therefore, it is up to the joint controllers to decide the most effective way to make the essence of the arrangement available to the data subjects (e.g. together with the information in Article 13 or 14, in the privacy policy or upon request to the data protection officer, if any, or to the contact point that may have been designated). Joint controllers should respectively ensure that the information is provided in a consistent manner.

The arrangement may designate a contact point for data subjects

180. Article 26(1) provides the possibility for joint controllers to designate in the arrangement a contact point for data subjects. Such designation is not mandatory.

181. Being informed of a single way to contact possible multiple joint controllers enables data subjects to know who they can contact with regard to all issues related to the processing of their personal data. In addition, it allows multiple joint controllers to coordinate in a more efficient manner their relations and communications *vis-à-vis* data subjects.

182. For these reasons, in order to facilitate the exercise of data subjects' rights under the GDPR, the EDPB recommends joint controllers to designate such contact point.

183. The contact point can be the DPO, if any, the representative in the Union (for joint controllers not established in the Union) or any other contact point where information can be obtained.

Irrespective of the terms of the arrangement, data subjects may exercise their rights in respect of and against each of the joint controllers.

184. Under Article 26(3), a data subject is not bound by the terms of the arrangement and may exercise his or her rights under the GDPR in respect of and against each of the joint data controllers.

185. For example, in case of joint controllers established in different Member States, or if only one of the joint controllers is established in the Union, the data subject may contact, at his or her choice, either the controller established in the Member State of his or her habitual residence or place of work, or the controller established elsewhere in the EU or in the EEA.

186. Even if the arrangement and the available essence of it indicate a contact point to receive and handle all data subjects' requests, the data subjects themselves may still choose otherwise.

187. Therefore, it is important that joint controllers organise in advance in their arrangement how they will manage answers to requests they could receive from data subjects. In this respect, it is recommended that joint controllers communicate to the other controllers in charge or to the designated contact point, the requests received in order to be effectively handled. Requiring data subjects to contact the designated contact point or the controller in charge would impose an excessive burden on the data subject that would be contrary to the objective of facilitating the exercise of their rights under the GDPR.

2.3 Obligations towards data protection authorities

- ~~Visibility/image given by the controller to the data subject, and expectations of the data subjects on the basis of this visibility.~~

188. Joint controllers should organise in the arrangement the way they will communicate with the competent supervisory data protection authorities. Such communication could cover possible consultation under Article 36 of the GDPR, notification of a personal data breach, designation of a data protection officer.

189. It should be recalled that data protection authorities are not bound by the terms of the arrangement whether on the issue of the qualification of the parties as joint controllers or the designated contact point. Therefore, the authorities can contact any of the joint controllers to exercise their powers under Article 58 with respect to the joint processing.

~~Example No. 20: Call centres~~

~~A data controller outsources some of its operations to a call centre and instructs the call centre to present itself using the identity of the data controller when calling the data controller's clients. In this case the expectations of the clients and the way the controller presents himself to them through the outsourcing company lead to the conclusion that the outsourcing company acts as a data processor for (on behalf of) the controller.~~

- ~~Expertise of the parties: in certain cases, the traditional role and professional expertise of the service provider play a predominant role, which may entail its qualification as data controller.~~

~~Example No. 21: Barristers~~

~~A barrister represents his/her client in court, and in relation to this mission, processes personal data related to the client's case. The legal ground for making use of the necessary information is the client's mandate. However, this mandate is not focused on processing data but on representation in court, for which activity such professions have traditionally their own legal basis. Such professions are therefore to be regarded as independent 'controllers' when processing data in the course of legally representing their clients.~~

~~In a different context, a closer assessment of the means put in place to reach the purposes may also be determining.~~

Example No. 22: "Lost and found" website

A 'lost and found' website was presented as being merely a processor as it would be those who post lost items who would determine the content and thus, at a micro level, the purpose (e.g. finding a lost brooch, parrot etc). A data protection authority rejected this argument. The website was set up for the business purpose of making money from allowing the posting of lost items and the fact that they did not determine which specific items were posted (as opposed to determining the categories of items) was not crucial as the definition of "data controller" does not expressly include the determination of content. The website determines the terms of posting etc and is responsible for the propriety of content.

Although there could have been a tendency to generally identify outsourcing as the task of a processor, nowadays situations and assessments are often much more complex. Sometimes, the complexity of processing operations may lead to put more focus on the

Example No. 23: Accountants

The qualification of accountants can vary depending on the context. Where accountants provide services to the general public and small traders on the basis of very general instructions ("Prepare my tax returns"), then – as with solicitors acting in similar circumstances and for similar reasons – the accountant will be a data controller. However, where an accountant is employed by a firm, and subject to detailed instructions from the in-house accountant, perhaps to carry out a detailed audit, then in general, if not a regular employee, he will be a processor, because of the clarity of the instructions and the consequent limited scope for discretion. However, this is subject to one major caveat, namely that where they consider that they have detected malpractice which they are obliged to report, then, because of the professional obligations they owe they are acting independently as a controller.

margin of manoeuvre of those entrusted with the processing of personal data, e.g. when the processing entails a specific privacy risk. Introducing new means of processing may lead to favouring the qualification as data controller rather than data processor. These cases may also lead to a clarification – and appointment of the controller – explicitly provided for by law.

Example No. 24: Processing for historical, scientific and statistical purposes

National law may introduce, with regard to processing of personal data for historical, scientific and statistical purposes, the notion of intermediary organization to designate the body in charge of transforming non-encoded data into encoded data, so that the controller of the processing for historical, scientific and statistical purposes would not be able to re-identify the data subjects.

If several controllers of initial processing operations transmit data to one or more third parties for further processing for historical, scientific and statistical purposes, the data are first encoded by an intermediary organization. In this case the intermediary organization may be considered as controller pursuant to specific national regulations, and it is subject to all resulting obligations (relevance of the data, informing the data subject, notification etc.). This is justified by the fact that when data from different sources are brought together, there is a particular threat to data protection, justifying the intermediary organization's own responsibility. Consequently, it is not simply considered as processor but fully regarded as controller pursuant to national law.

In the same line, the autonomous decision-making power left to the various parties involved in the processing is relevant. The case of clinical drug trials shows that the relationship between sponsor companies and external entities entrusted to carry out the trials depends on the discretion left to the external entities in respect of data processing. This entails that there may be more than one controller, but also more than one processor or person in charge of the processing.

Example No. 25: Clinical drug trials

The pharmaceutical company XYZ sponsors some drug trials and selects the candidate trial centres by assessing the respective eligibility and interests; it draws up the trial protocol, provides the necessary guidance to the centres with regard to data processing and verifies compliance by the centres with both the protocol and the respective internal procedures.

Although the sponsor does not collect any data directly, it does acquire the patients' data as collected by trial centres and processes those data in different ways (evaluating the information contained in the medical documents; receiving the data of adverse reactions; entering these data in the relevant database; performing statistical analyses to achieve the trial results). The trial centre carries out the trial autonomously – albeit in compliance with the sponsor's guidelines; it provides the information notices to patients and obtains their consent as also related to processing of the data concerning them; it allows the sponsor's collaborators to access the patients' original medical documents to perform monitoring activities; and it handles and is responsible for the safekeeping of those documents. Therefore, it appears that responsibilities are vested in the individual actors. Against this background, in this case both trial centres and sponsors make important determinations with regard to the way personal data relating to clinical trials are processed. Accordingly, they may be regarded as joint data controllers. The relation between the sponsor and the trial centres could be interpreted differently in those cases where the sponsor determines the purposes and the essential elements of the means and the researcher is left with a very narrow margin of manoeuvre.

III.3. Definition of third party

The concept of "third party" was not laid down by Convention 108, but was introduced by the amended Commission proposal further to an amendment proposed by the European Parliament. According to the explanatory memorandum, the amendment was reworded in order to make clear that third parties do not include the data subject, the controller and any person authorized to process the data under the controller's direct authority or on his behalf, as is the case with the processor. This means, that "*persons working for another organization, even if it belongs to the same group or holding company, will generally be third parties*" while on the other hand "*branches of a bank processing customer's accounts under the direct authority of their headquarters would not be third parties*".

The Directive uses "third party" in a way which is not dissimilar to the way in which this concept is normally used in civil law, where third party is usually a subject which is not part of an entity or of an agreement. In the data protection context, this concept should be interpreted as referring to any subject who has no specific legitimacy or authorization - which could stem, for example, from its role as controller, processor, or their employee - in processing personal data.

The Directive uses this concept in many provisions, usually with a view to establish prohibitions, limitations and obligations for the cases where personal data might be processed by other parties which in origin were not supposed to process certain personal data.

Against this background, it can be concluded that a third party receiving personal data - either lawfully or unlawfully - would in principle be a new controller, provided that the other conditions for the qualification of this party as controller and the application of the data protection legislation are met.

Example No. 26: Unauthorised access by an employee

An employee of a company in carrying out his tasks gets to know personal data to which he is not authorized to have access. In this case, this employee should be considered as "third party" vis-à-vis his employer, with all the resulting consequences and liabilities in terms of lawfulness of communication and processing of data.

IV. Conclusions

The concept of data controller and its interaction with the concept of data processor play a crucial role in the application of Directive 95/46/EC, since they determine who shall be responsible for compliance with data protection rules, how data subjects can exercise their rights, which is the applicable national law and how effective Data Protection Authorities can operate.

Organisational differentiation both in the public and in the private sector, the development of ICT as well as the globalisation of data processing increase complexity in the way personal data are processed and call for clarifications of these concepts, in order to ensure effective application and compliance in practice.

The concept of controller is autonomous, in the sense that it should be interpreted mainly according to Community data protection law, and functional, in the sense that it is intended to allocate responsibilities where the factual influence is, and thus based on a factual rather than a formal analysis.

The definition in the Directive contains three main building blocks: the personal aspect ("*the natural or legal person, public authority, agency or any other body*"); the possibility of pluralistic control ("*which alone or jointly with others*"); and the essential elements to distinguish the controller from other actors ("*determines the purposes and the means of the processing of personal data*").

The analysis of these building blocks leads to the following main outcomes:

- The capacity to "*determine* the purposes and the means " may stem from different legal and/or factual circumstances: an explicit legal competence, when the law appoints the controller or confers a task or duty to collect and process certain data; common legal provisions or existing traditional roles that normally imply a certain responsibility within certain organisations (for example, the employer in relation to data of its employees); factual circumstances and other elements (such as contractual relations, actual control by a party, visibility towards data subjects, etc).

  If none of these categories is applicable, the appointment of a controller should be considered as "null and void". Indeed, a body which has neither legal nor factual influence to determine how personal data are processed cannot be considered as a controller.

  Determining the "purpose" of processing triggers the qualification of (*de facto*) controller. Instead, the determination of the "means" of processing can be delegated by the controller, as far as technical or organisational questions are concerned. However, substantial questions which are essential to the core of lawfulness of processing - such as data to be processed, length of storage, access, etc. - are to be determined by the controller.
- The *personal* aspect of the definition refers to a broad series of subjects, which can play the role of controller. However, in the strategic perspective of allocating responsibilities, preference should be given to considering as controller the company or body as such rather than a specific person within the company or the body. It is the company or the body which shall be considered ultimately responsible for data processing and the obligations stemming from data protection legislation, unless there are clear elements indicating that a natural person shall be responsible, for example when a natural person working within a company or a public body uses data for his or her own purposes, outside the activities of the company.
- The possibility of *pluralistic control* caters for the increasing number of situations where different parties act as controllers. The assessment of this joint control should mirror the assessment of "single" control, by taking a substantive and functional approach and focusing on whether the purposes and the essential elements of the means are determined by more than one party.

The participation of parties in the determination of purposes and means of processing in the context of joint control may take different forms and does not need to be equally shared. This opinion provides many examples of different kinds and degrees of joint control. Different degrees of control may give rise to different degrees of responsibility and liability, and "joint and several" liability can certainly not be assumed in all cases. Furthermore, it is well possible that in complex systems with multiple actors, access to personal data and exercise of other data subjects' rights can be ensured also at different levels by different actors.

This opinion also analyzes the concept of processor, the existence of which depends on a decision taken by the controller, who can decide either to process data within his organization or to delegate all or part of the processing activities to an external organization. Therefore, two basic conditions for qualifying as processor are on the one hand being a separate legal entity with respect to the controller and on the other hand processing personal data on his behalf. This processing activity may be limited to a very specific task or context or may accommodate a certain degree of discretion about how to serve the controller's interests, allowing the processor to choose the most suitable technical and organizational means.

Furthermore, the role of processor does not stem from the nature of an actor processing personal data but from its concrete activities in a specific context and with regard to specific sets of data or operations. Some criteria may be helpful in determining the qualification of the various actors involved in the processing: the level of prior instruction given by the data controller; the monitoring by the data controller of the level of the service; the visibility towards data subjects; the expertise of the parties; the autonomous decision-making power left to the various parties.

The residual category of "third party" is defined as any actor who has no specific legitimacy or authorization - which could stem, for example, from its role as controller, processor, or their employee - in processing personal data.

* * *

The Working Party recognises the difficulties in applying the definitions of the Directive in a complex environment, where many scenarios can be foreseen involving controllers and processors, alone or jointly, with different degrees of autonomy and responsibility.

In its analysis, it has emphasized the need to allocate responsibility in such a way that compliance with data protection rules will be sufficiently ensured in practice. However, it has not found any reason to think that the current distinction between controllers and processors would no longer be relevant and workable in that perspective.

The Working Party therefore hopes that the explanations given in this opinion, illustrated with specific examples taken from the daily experience of data protection authorities, will contribute to effective guidance on the way to interpret these core definitions of the Directive.

Done in Brussels, on 16 February 2010

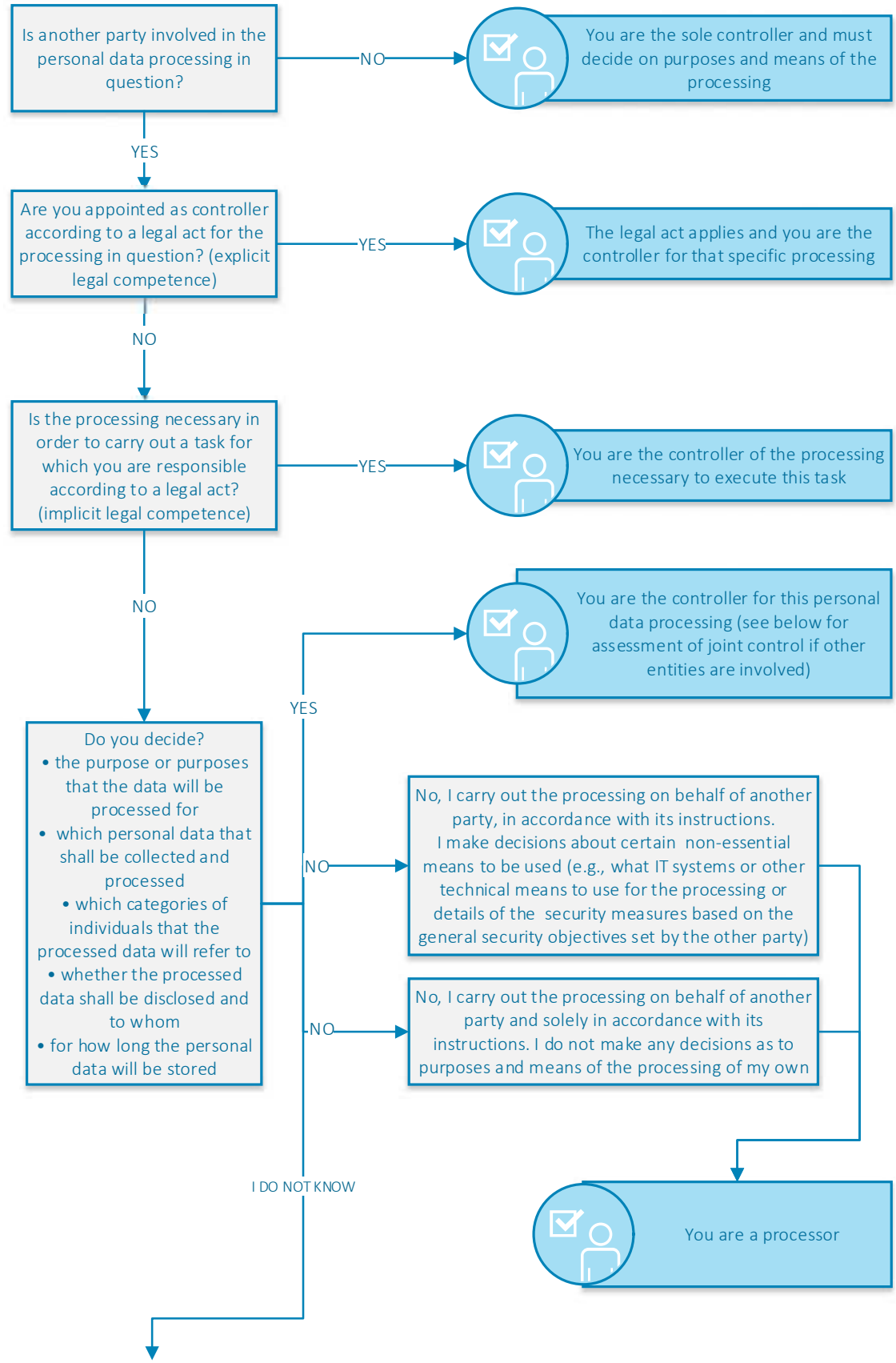
For the Working Party,

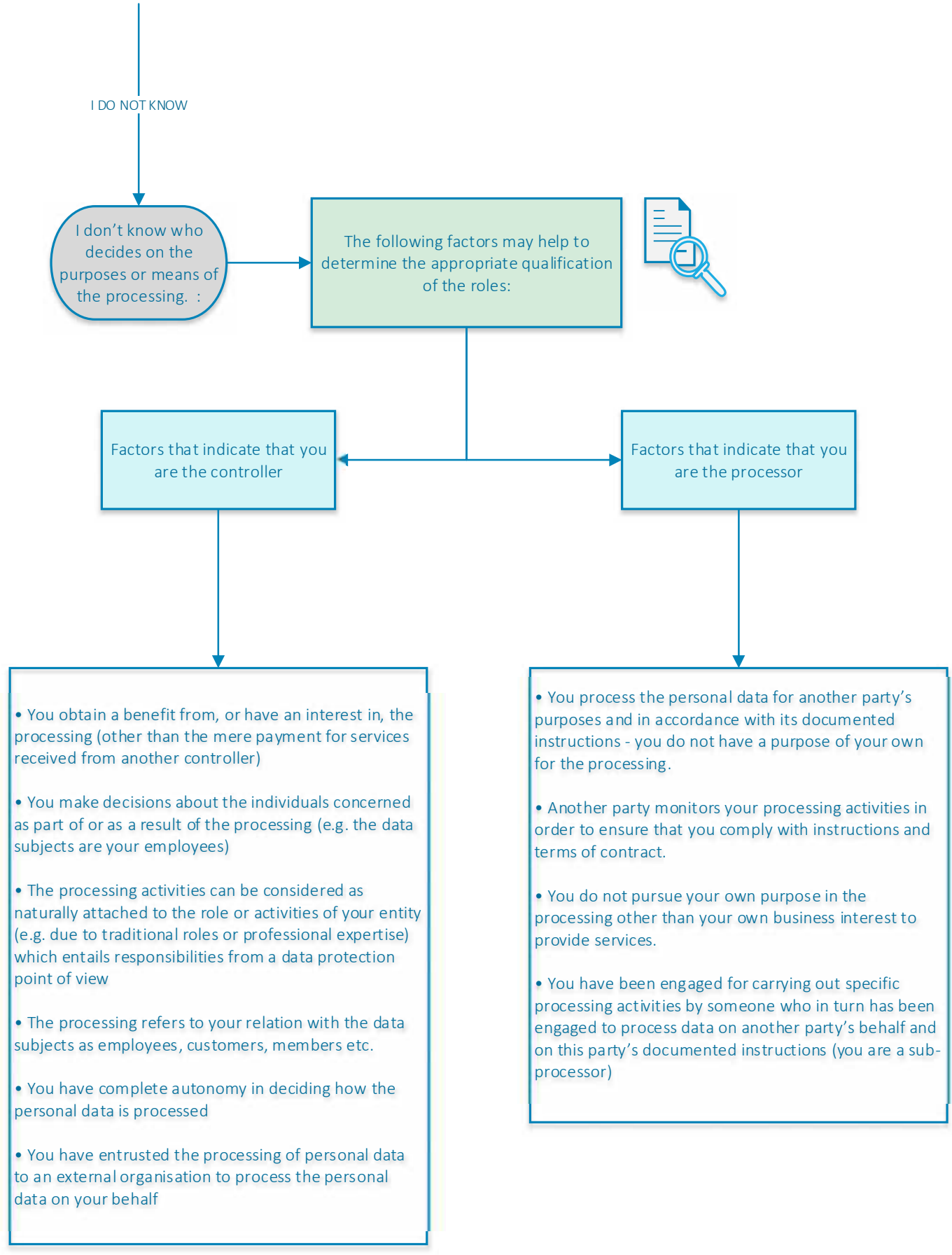
The Chairman

Jacob KOHNSTAMM

Annex I – Flowchart for applying the concepts of controller, processor and joint controllers in practice

Note: in order to properly assess the role of each entity involved, one must first identify the specific personal data processing at stake and its exact purpose. If multiple entities are involved, it is necessary to assess whether the purposes and means are determined jointly, leading to joint controllership.




I DO NOT KNOW
I don't know who decides on the purposes or means of the processing. :
The following factors may help to determine the appropriate qualification of the roles:
Factors that indicate that you are the controller
Factors that indicate that you are the processor
• You obtain a benefit from, or have an interest in, the processing (other than the mere payment for services received from another controller)
• You make decisions about the individuals concerned as part of or as a result of the processing (e.g. the data subjects are your employees)
• The processing activities can be considered as naturally attached to the role or activities of your entity (e.g. due to traditional roles or professional expertise) which entails responsibilities from a data protection point of view
• The processing refers to your relation with the data subjects as employees, customers, members etc.
• You have complete autonomy in deciding how the personal data is processed
• You have entrusted the processing of personal data to an external organisation to process the personal data on your behalf
• You process the personal data for another party's purposes and in accordance with its documented instructions - you do not have a purpose of your own for the processing.
• Another party monitors your processing activities in order to ensure that you comply with instructions and terms of contract.
• You do not pursue your own purpose in the processing other than your own business interest to provide services.
• You have been engaged for carrying out specific processing activities by someone who in turn has been engaged to process data on another party's behalf and on this party's documented instructions (you are a sub-processor)

Joint controllership - If you are the controller and other parties are involved in the personal data processing: