ARTICLE 29 DATA PROTECTION WORKING PARTY

00264/10/EN
WP 169

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

Adopted on 16 February 2010

TABLE OF CONTENTS

Executive summary

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 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 a number of conclusions that have been summarized in paragraph IV of the opinion.

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.

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.

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

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 July 2002,

having regard to its Rules of Procedure,

has adopted the following opinion:

I. Introduction

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, 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.

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.

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.

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.

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.

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.

II. General observations and policy issues

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:

> *'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 processing are determined by national or Community laws or regulations the controller or the specific criteria for his nomination may be designated by national or Community 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

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

- "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".

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

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.

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"

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 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 questions "why is this processing taking place? Who initiated it?".

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

The concept of controller is a functional concept, intended to allocate responsibilities where the factual influence is, and thus 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, rules of thumb and practical presumptions are needed to guide and simplify the application of data protection law.

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 - legal and/or factual - circumstances from which factual influence normally can be inferred, unless other elements indicate the contrary.

---

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 explicit legal competence*. This is *inter alia* the case referred to in the second part of the definition, i.e. when the controller or the specific criteria for his 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. In some countries, the national law has provided that public authorities are responsible for processing of personal data within the context of their duties.

However, more frequent is the case where the law, rather than directly appointing the controller or setting out the criteria for his appointment, establishes a task or imposes a duty on someone to collect and process certain data. For example, this would be the case of 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 register with a view to fulfil them. In that case, it follows from the law who is the controller. More generally, the law may 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 processing of personal data in that context.

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.

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.

Example No. 1: Telecom operators

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.

3) *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.

It may be that a contract is silent on who is the controller, but contains sufficient elements to assign the responsibility of controller to a party that apparently exercises a dominant role in this respect. It may also be that the contract is more explicit as to 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 all circumstances, as this would simply allow parties to allocate responsibility where they think fit.

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.

[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.

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 the other hand, the Directive 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 determining the purposes and the means amounts to determining respectively the "why" and the "how" of certain 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.

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.

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.

Example No. 2: Mail marketing

Company ABC enters into contracts with different organisations to carry out its mail marketing campaigns and to run its payroll. It gives clear instructions (what marketing material to send out and to whom, and who to pay, what amounts, by what date etc). Even though the organisations have some discretion (including what software to use) their tasks are pretty clearly and tightly defined and though the mailing house may offer advice (e.g. advising against sending mailings in August) they are clearly bound to act as ABC instructs. Moreover, only one entity, the Company ABC, is entitled to use the data which are processed – all the other entities have to rely on the legal basis of Company ABC if their legal ability to process the data is questioned. In this case it is clear that the company ABC is the data controller and each of the separate organisations can be considered as a processor regarding the specific processing of data carried out on its behalf.

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.

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 of processing 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.

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]

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].

---

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.

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.

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

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).

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*".

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.

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.

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.

Example No. 5: Installing video-surveillance cameras

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.

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.

Example No. 6: Headhunters

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.

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.

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)

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.

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.

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.

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.

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. 13: Banks and information pools on defaulting customers

Several banks may establish a common "information pool" - where national law allows for these pools - whereby each of them contributes information (data) concerning defaulting customers and all of them have access to the total amount of information. Some legislations provide that all requests of data subjects, e.g. for access or deletion, need only to be made to one "entry-point", the provider. The provider is responsible for finding the correct controller and for organizing that due answers are given to the data subject. The identity of the provider is published in the Data Processing Register. In other jurisdictions, such information pools may be operated by separate legal entities as controller, while requests for subject access are handled by the participating banks acting as its intermediary.

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.

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

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.

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. Definition of processor

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.

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 …").

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".

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.

Example No. 16: Internet service providers of hosting 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).

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.

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.

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, 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* 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.

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.

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.

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

[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.

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).

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.

Example No. 19: Computer grids

Large scale research infrastructures are increasingly using distributed computing facilities, especially grids, to profit in terms of computing and storage capacity. Grids are installed in different research infrastructures established in different countries. A European grid may, for instance, consist of national grids, which in turn are under the responsibility of a national body. This European grid, however, may not have a central body, responsible for its functioning. Researchers using such a grid can not usually identify where their data are exactly being processed, and thus who is the responsible data processor (the case is even more complicated if there are grid infrastructures in third countries). Should a grid infrastructure use the data in an unauthorised manner, this party may be considered data controller, if it does not act on behalf of the researchers.

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.

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.

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.

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

- 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;

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

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.

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.

Sometimes, the complexity of processing operations may lead to put more focus on the 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