ARTICLE 29 DATA PROTECTION WORKING PARTY

0836-02/10/EN
WP 179

Opinion 8/2010 on applicable law

Adopted on 16 December 2010

Executive summary

This opinion clarifies the scope of application of Directive 95/46/EC, and in particular of its Article 4, which determines which national data protection law(s) adopted pursuant to the Directive may be applicable to the processing of personal data. The opinion also highlights some areas for possible further improvement.

Determining the application of EU law to the processing of personal data serves to clarify the scope of EU data protection law both in the EU/EEA and in a wider international context. A clear understanding of applicable law will help to ensure both legal certainty for controllers and a clear framework for individuals and other stakeholders. Furthermore, a correct understanding of the applicable law provisions should ensure that no lacunae or loopholes may be found in the high level of protection of personal data provided by Directive 95/46.

With regard to Article 4(1)a, the reference to "an" establishment means that the applicability of a Member State's law will be triggered by the location of an establishment of the controller in that Member State, and other Member States' laws could be triggered by the location of other establishments of that controller in those Member States. To trigger the application of the national law, the notion of the "context of activities" of the establishment is decisive. It implies that the *establishment* of the controller is involved in *activities* implying the processing of personal data, taking into consideration its degree of involvement in the processing activities, the nature of the activities and the need to guarantee effective data protection.

With regard to the "use of equipment" provision in Article 4(1)c, which may entail the application of the Directive to controllers not established in the EU/EEA territory, the opinion clarifies that it should apply in those cases where there is no establishment in the EU/EEA *which would trigger the application of Article 4(1)a* or where the processing *is not carried out in the context* of such an establishment. The opinion also notes that a broad interpretation of the notion of "equipment' - justified by its expression by "means" in other EU languages - may in some cases result in European data protection law being applicable where the processing in question has no real connection with the EU/EEA.

The opinion also provides guidance and examples with regard to: the other provisions of Article 4; the security requirements stemming from the law applicable pursuant to Article 17(3); the possibility for data protection authorities to use their powers to verify and intervene in a processing operation that is taking place on their territory even if the law applicable is the law of another Member State (Article 28(6).

The opinion also suggests that the wording used in the Directive and the consistency between the different parts of Article 4 would benefit from further clarification as a part of the revision of the general data protection framework.

In this perspective, simplifying the rules for determining applicable law would consist of a shift back to the country of origin principle: all establishments of a controller within the EU would then apply the same law - that of the main establishment - regardless of the territory in which they are located. However, this could only be acceptable if a comprehensive harmonisation of national legislation is reached, including harmonisation of security obligations.

Additional criteria could apply when the controller is established outside the EU, with a view to ensuring that a sufficient connection exists with EU territory, while avoiding that the EU territory is used to conduct illegal data processing activities by controllers established in third countries. The following criteria may be developed in this view: the targeting of individuals, resulting in the application of EU data protection law when the activity involving the processing of personal data is targeted at individuals in the EU; the application of the equipment criterion in a residual and limited form, which would address borderline cases (data about non EU data subjects, controllers having no link with EU) where there is a relevant data-processing infrastructure in the EU.

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

established by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 (OJ L 281, 23.11.1995, p. 31),

having regard to Articles 29 and 30 paragraphs 1(a) and 3 of that Directive,

having regard to its Rules of Procedure,

has adopted the following opinion:

I. Introduction

Defining the law applicable to the processing of personal data under Directive 95/46/EC ('Directive' or 'Directive 95/46') is a key issue for a number of reasons. Provisions on applicable law are crucial in determining the external scope of EU data protection law, in other words, to determine the extent to which EU data protection law is applicable to processing of personal data taking place wholly or partly outside the EU/EEA, but still having a relevant connection with the EU/EEA territory. However, rules on applicable law also determine the scope of data protection law within the EU/EEA, so as to avoid possible conflicts between and overlapping of the national laws of the EU/EEA Member States implementing the Directive[1].

Furthermore, a correct understanding of the applicable law provisions should ensure that no lacunae or loopholes arise in the high level of protection of personal data provided by Directive 95/46.

The Directive includes a number of provisions addressing applicable law issues, in particular Article 4, Article 17 and Article 28. These provisions define the national data protection law which applies pursuant to the Directive, and the authority which will be responsible for the enforcement of that law. It is important to bear in mind that there is an interaction between substantive law and jurisdiction. This is considered in further detail below.

It has been suggested that the implementation and interpretation of the Directive's provisions on applicable law are far from uniform throughout the European Union. The Commission's 'First report on the implementation of the Data Protection Directive' highlighted that the implementation of Article 4 of the Directive was "deficient in several cases, with the result that the kind of conflicts of law this Article seeks to avoid could arise"[2]. According to the technical annex to the report, which presents a detailed analysis of several national provisions, such a deficient transposition could be partly explained by the complexity of the provision itself.

Similarly, a study sponsored by the European Commission[3] highlights the ambiguity and divergent implementation of the applicable law rules in the Directive and recommends that "*better, clearer and unambiguous rules are desperately needed on applicable law*".

More recently, the Commission Communication "A comprehensive approach on personal data protection in the European Union" [4] mentions that "*The Commission will examine how to revise and clarify the existing provisions on applicable law, including the current determining criteria, in order to improve legal certainty, clarify Member States' responsibility for applying data protection rules and ultimately provide for the same*

---

1 Directive 95/46/EC also applies to the EFTA countries Norway, Iceland and Liechtenstein under the EEA agreement (cf. Decision of the EEA Joint Committee No 83/1999 of 25 June 1999 amending Protocol 37 and Annex XI (Telecommunication services) to the EEA Agreement; OJ L 296/41, of 23.11.2000).

2 First report on the implementation of the Data Protection Directive (95/46/EC), May 2003, p. 17. The report is available at http://ec.europa.eu/justice/policies/privacy/lawreport/report_en.htm

3 "Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments", January 2010, available at http://ec.europa.eu/justice/policies/privacy/studies/index_en.htm.

4 COM (2010) 609 final of 4.11.2010.

degree of protection of EU data subjects, regardless of the geographic location of the data controller".

The complexity of applicable law issues is also growing due to increased globalisation and the development of new technologies: companies are increasingly operating in different jurisdictions, providing services and assistance around-the-clock; the internet makes it much easier to provide services from a distance and to collect and share personal data in a virtual environment; cloud computing makes it difficult to determine the location of personal data and of the equipment being used at any given time.

It is thus crucial that the precise meaning of the provisions of the Directive dealing with applicable law are sufficiently clear to all involved in the implementation of the Directive as well as in the day-to-day application of national data protection laws in both the public and the private sector.

Therefore, the Working Party has decided to contribute to the clarification of some key provisions of the Directive and to deal with the concept of applicable law, much as it has done already with regard to the concept of personal data and the concepts of "controller" and "processor"[5]. In this opinion, the Working Party will also refer to the other opinions in which it has dealt with the issue of applicable law where it arises in relation to the specific topics covered by those opinions[6].

The final objective of the Working Party is to provide legal certainty in the application of EU data protection law. This entails, on the one hand, that data subjects are aware of which rules apply to protect their personal data, and on the other hand, that businesses as well as other private and public bodies know which data protection rules regulate their data processing.

Clarifying the concept of applicable law is of great importance, independently of possible amendments to the current provisions of the Directive in the future. Current provisions will remain valid until amended, and to the extent that they are not amended. Therefore clarification of the applicable law provisions will help to ensure better compliance with the Directive pending any amendment of the legislation. In addition, in preparing this opinion the Working Party has been able to draw on the experience of applying the current provisions with a view to providing guidance to the legislator to assist in any future revision of the Directive.

Finally, the provisions on determining applicable law with regard to data protection are designed to govern the application of the Directive within its own scope as defined in Article 3. As such, they will often interact with other areas of law without influencing them beyond its scope.[7]

---

5 Opinion 4/2007 on the concept of personal data (WP 136); Opinion 1/2010 on the concepts of "controller" and "processor" (WP 169). All opinions are available at: http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm

6 In particular, Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites (WP 56), Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT) (WP 128) and Opinion 1/2008 on data protection issues related to search engines (WP 148).

7 Although the Directive contains provisions on liability (Article 23) and sanctions (Article 24), general principles of civil or criminal law are in principle not affected, as mentioned in Recital 21 of the Directive. They would be affected only as far as necessary to foresee sanctions in case of violation of

II. General observations and policy issues

II.1. Brief history: from Convention 108 to Directive 95/46/EC

In 1981, the authors of Convention 108 drawn up under the auspices of the Council of Europe identified the risks posed by conflict of law issues, or the legal gap, that could result from the application of different national laws. However, that Convention did not include specific rules to address these problems: the fact that the Convention would provide for a "common core of substantive law" was considered to be the main guarantee that, even if different regulations subsist, the principles to be applied at the end would be the same, which would avoid differences in terms of level of protection.

The need for criteria to determine applicable law was addressed by the European Commission when preparing the Directive on data protection. In its initial proposal[8], the Commission identified the location of the data file as a primary determining factor, and the controllers' residence as the secondary determining factor when the file is located in a third country.

In the course of the discussion in European Parliament and in the Council of the EU, there was a shift from the criterion of the location of the file to the criterion of the establishment of the controller. The location of the means was identified as the second criterion when the controller is not established in the EU.

The Council supplemented these criteria and provided further indications with regard to the notion of establishment. The Commission's amended proposal[9] specified that the processing should take place "in the context of the activities of an establishment" of the controller, and took into account the possibility that the controller may have several establishments in different Member States. One major change concerned the fact that the main criterion to determine applicable law was not the place where the controller has its main establishment but where there was *an* establishment of the controller. The consequences of these amendments, in terms of distributive rather than uniform application of national law in case of multiple establishments, will be developed below.

II.2. Role of concepts

II.2.a) Context and strategic importance

Determining the application of EU law to the processing of personal data, as said before, serves to clarify the scope of EU data protection law both in the EU/EEA and in a wider international context. A clear understanding of applicable law will

---

data protection principles. In practice, national implementation of the Directive has led to different scenarios, including or not criminal sanctions. To mention another example, although the Directive contains provisions on the need for consent - see Article 2(h), Article 7(a) and Article 8(2)(a) - or the relevance of contractual obligations - see Article 7 (b) - it does not enter into contract law (e.g. conditions for concluding a contract, law applicable) or other aspects of civil law beyond its own provisions.

8 COM (1990) 314 - 2 of 18.07.1990, Proposal for a European Parliament and Council Directive concerning the protection of individuals in relation to the processing of personal data.

9 COM (1992) 422 final of 15.10.1992.

help to ensure both legal certainty for controllers and a clear framework for individuals concerned and other stakeholders.

The identification of applicable law is closely connected to the identification of the controller[10] and its establishment(s): the main consequence of this link is the reaffirmation of the responsibilities of the controller, and its representative if the controller is established in a third country.

As it will be elaborated below, this does not mean that there will always be one applicable law, especially if the controller has several establishments: the location of those establishments and the nature of their activities will also be decisive. But the clear connection between the applicable law and the controller can be a guarantee of effectiveness and enforceability, especially in a context in which it can be difficult, or sometimes impossible, to locate a file (as may be the case for cloud computing).

Clear guidelines as to applicable law rules should help address new developments: technological (internet; network based files/cloud computing) and commercial (multinational companies).

II.2.b) Scope of EU law and of national law within the EU/EEA

The main criteria in determining the applicable law are the location of the establishment of the controller, and the location of the means or equipment[11] being used when the controller is established outside the EEA. This means that neither the nationality or place of habitual residence of data subjects, nor the physical location of the personal data, are decisive for this purpose[12].

This induces a broad scope of application, with legal implications extending beyond the EEA territory: the Directive – and national laws of implementation – apply to the processing of personal data outside the EEA (where carried out in the context of activities of an establishment of the controller in the EEA), as well as to controllers established outside the EEA (when they use equipment in the EEA). As a consequence, the provisions of the Directive can be applicable to services with an international dimension such as search engines, social networks and cloud computing. These examples are developed below in the document.

Where personal data is processed by a data controller (X) whose only establishment is located in Member State A, the national law of Member State A will be the law applicable to the processing, regardless of where it is carried out.

10 See Opinion 1/2010 on the concepts of "controller" and "processor" (WP 169).

11 As explained below in III.2.b, the notion of "equipment" has been expressed in other EU languages by "means". This supports a broad interpretation of the notion of equipment and explains why the two notions are used in this document.

12 See in the same line Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market. An additional relevant factor is the location of the processor with regard to the law applicable to security measures (Article 17). However, this criterion is not decisive in itself and has to be applied in connection to the main criterion of the establishment of the controller.

Where X also has an establishment (Y) in Member State B, the national law applicable to the processing by Y will be the national law of Member State B, provided that the processing is carried out in the context of the activities of Y. If the processing by Y is carried out in the context of the activities of the establishment of X in Member State A, the law applicable to the processing will be the law of Member State A.

Where personal data is processed by a data controller that is not established in any Member State, the processing will fall within the scope of the national law of any Member State in which equipment (or means) used by the data controller to process the data is located. Examples of these different scenarios will be considered in the course of this opinion.

The purpose of this broad scope of application is primarily to ensure that individuals are not deprived of the protection to which they are entitled under the Directive, and, at the same time, to prevent circumvention of the law.

The Directive provides for criteria for determining both:
(i) whether European law – either jointly with the law of a third country or not – applies to a particular personal data processing activity; and
(ii) where European law applies to the processing, which Member States' national law applies to the processing.

It should also be noted that some processing activities within the EU are outside the scope of the Directive, but they may trigger the application of other EU legal instruments, such as the Framework Decision 2008/977/JHA on data protection in the framework of police and judicial cooperation in criminal matters[13], or Regulation 45/2001 on personal data processed by Community institutions and bodies[14], or other instruments on specific EU bodies or information systems (e.g. Europol, Eurojust, SIS, CIS, etc)[15]

II.2.c) Avoidance of lacunae and undue overlap

The purpose of clear criteria for determining the applicable law is to avoid both circumvention of Member States' national rules, and overlap of those rules. Whether one or several laws apply to the processing will depend on the number and the activities of the establishment(s) of the controller:

- If the controller has one establishment, there will be one law for the whole EU/EEA, depending on the location of this establishment.[16]

13 Council Framework Decision 2008/977/JHA of 27.11.2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (OJ L 350, 30.12.2008, p. 60).

14 Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p. 1).

15 Europol: Council Decision 2009/371/JHA, OJ L 121, 15.5.2009, p. 37); Eurojust: Council Decision 2002/187/JHA, OJ L 63, 6.3.2002, p. 1, amended by Council Decision 2009/426/JHA, OJ L 138, 4.6.2009, p. 14.

16 Except with regard to security measures, which will depend on the location of a possible processor, as provided for in Article 17(3) of the Directive.

- If there are several establishments: the application of national legislation will be distributed depending on the activities of each establishment.

Application of the criteria should prevent the simultaneous application of more national laws to the same processing activity.

II.2.d) Applicable law and jurisdiction in the context of the Directive

In the area of data protection, it is particularly important to distinguish the concept of *applicable law* (which determines the legal regime applicable to a certain matter) from the concept of *jurisdiction* (which usually determines the ability of a national court to decide a case or enforce a judgment or order). The applicable law and the jurisdiction in relation to any given processing may not always be the same.

The external scope of EU law is an expression of its capacity to lay down rules in order to protect fundamental interests within its jurisdiction. The provisions of the Directive also determine the scope of applicability of the national laws of the Member States, but they do not affect the jurisdiction of national courts to decide relevant cases before them. The provisions of the Directive do, however, refer to the territorial scope of the competence of the supervisory authorities that may apply and enforce the applicable law.

Although in most cases these two concepts – applicable law and competence of supervisory authorities – tend to coincide, usually resulting in Member State A's law being applied by Member State A's authorities, the Directive explicitly foresees the possibility of different arrangements. Article 28(6) implies that the national data protection authorities should be able to exercise their powers when the data protection law of another Member State applies to the processing of personal data carried out within their jurisdiction. The practical consequences of this issue will be further examined in a future opinion of the Working Party.

Such situations result in the handling of cross-border cases, and highlight the need for cooperation between DPAs, taking into account the enforcement powers of each DPA involved. This also illustrates the need for national law to properly implement the relevant provisions of the Directive, as this may be decisive for an effective cross-border cooperation and enforcement.

III. Analysis of provisions

The key provision on applicable law is Article 4, which determines which national data protection law(s) adopted pursuant to the Directive may be applicable to the processing of personal data.

III.1. Controller established in one or more Member States (Article 4(1)a)

The first situation addressed by Article 4(1) is where the controller has one or more establishments within the EU territory. In this case, Article 4(1)a provides that a Member State shall apply its national data protection law where *"[...] the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; 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"*.

It is useful to recall that the concept of 'controller' is defined in Article 2(d) of the Directive. This definition will not be analysed in this opinion, since it has already been clarified by the Article 29 Working Party in its Opinion on the concepts of "controller" and "processor"[17].

It is furthermore important to emphasise that an establishment need not have a legal personality, and also that the notion of establishment has flexible connections with the notion of control. A controller can have several establishments, joint controllers can concentrate activities within one establishment or different establishments. The decisive element to qualify an establishment under the Directive is the effective and real exercise of activities in the context of which personal data are processed.

a) "…an establishment of the controller on the territory of the Member State …"

The notion of establishment is not defined in the Directive. The preamble of the Directive indicates however that *"establishment on the territory of a Member State implies the effective and real exercise of activity through stable arrangements (and that) the legal form of (..) an establishment, whether simply branch or a subsidiary with a legal personality, is not the determining factor in this respect" (recital 19).*

Concerning the freedom of establishment under Article 50 TFEU (former Article 43 TEC) the European Court of Justice (ECJ) has considered that a stable establishment requires that "both human and technical resources necessary for the provision of particular services are permanently available". [18]

The strong emphasis put in the preamble of the Directive on "effective and real exercise of activity through stable arrangements" clearly echoes the "stable establishment" referred to by the Court of Justice at the time of the adoption of the Directive. Although it is not clear whether this and subsequent interpretations by the ECJ as regards the freedom of establishment under Article 50 TFEU could be fully applied to the situations covered by Article 4 of the Data Protection Directive, the interpretation of the Court in those cases can provide useful guidance when analysing the wording of the Directive.

This interpretation is used in the following examples:

- Where "effective and real exercise of activity" takes place, for example in an attorney's office, through "stable arrangements", the office would qualify as an establishment.

---

17 Opinion 1/2010 on the concepts of "controller" and "processor" (WP 169).

18 ECJ judgment of 4 July 1985, *Bergholz*, (Case 168/84, ECR [1985] p. 2251, paragraph 14) and judgment of 7 May 1998, *Lease Plan Luxembourg / Belgische Staat* (C-390/96, ECR [1998] p. I-2553). In the latter case the issue was to determine whether a company server, situated in a country different from the country of the service provider, could be considered a stable establishment. The purpose was to identify in which country VAT had to be paid. The judge refused to consider computer means as a virtual establishment (returning with this interpretation to a more "classical" notion of 'establishment', different from the one adopted in previous judgement of 17 July 1997, *ARO Lease / Inspecteur der Belastingdienst Grote Ondernemingen te Amsterdam* (C-190/95, ECR 1997 p. I-4383).

- A server or a computer is not likely to qualify as an establishment as it is simply a technical facility or instrument for the processing of information[19].

- A one-person office would qualify as long as the office does more than simply represent a controller established elsewhere, and is actively involved in the activities in the context of which the processing of personal data takes place.

- In any case, the form of the office is not decisive: even a simple agent may be considered as a relevant establishment if his presence in the Member State presents sufficient stability.

Example No. 1: publication for travellers

A company established in Member State A, in order to create a publication for travellers, is collecting data concerning the services provided by petrol stations in Member State B. The data are collected by an employee who, travelling throughout B, collects and sends photos and comments to his employer in A. In this case, data are collected in B (without an "establishment" there) and are processed in the context of the activities of the establishment in A: the applicable law is the law of A.

Article 4(1)a, referring to *an* establishment of *the controller* on the territory of the *Member State*, raises issues – other than the concept of establishment – that require clarification.

First of all, the reference to "an" establishment means that the applicability of a Member State's law will be triggered by the location of an establishment of the controller in that Member State, and other Member States' laws could be triggered by the location of other establishments of that controller in those Member States.

Even if the controller has its main establishment in a third country, just having one of his establishments in a Member State could trigger the applicability of the law of that country, provided that the other conditions of Article 4(1)a are fulfilled (see infra sub b). This is also confirmed by the second part of the provision, which explicitly foresees that where the same controller is established on the territory of several Member States, he should ensure that each of the establishments complies with the relevant applicable law.

b) "… processing is carried out in the context of the activities ..."

The Directive links the applicability of a Member State's data protection law to a processing of personal data. The concept of 'processing' has already been incidentally addressed by the Working Party in other opinions, which highlighted that different operations or sets of operations upon personal data may be carried out simultaneously or in different stages.[20] In the context of determining applicable law, this may well mean that different applicable laws may be triggered by different stages of processing personal data.

While the multiplication of applicable laws is therefore a serious risk, consideration should be given to the possibility that links at a macro level between the different processing activities could lead alternatively to the application of one single national law.

[19] Whether they qualify otherwise, for instance as 'equipment', will be discussed later on in the text.

[20] See, e.g. Opinion 1/2010 on the concepts of "controller" and "processor" (WP 169).

To determine whether one or several laws apply to the different stages of the processing, it is important to have in mind the global picture of the processing activities: a set of operations carried out in a number of different Member States but all intended to serve a single purpose might well result in the application of a single national law.

In such circumstances, the notion of "context of activities" – and not the location of data – is a determining factor in identifying the applicable law.

The notion of "context of activities" does not imply that the applicable law is the law of the Member State where the *controller* is established, but where an *establishment* of the controller is involved in *activities* relating to data processing.

Consideration of different scenarios might help to clarify what is meant by the notion of "context of activities" and its influence in determining the law applicable to different processing activities in a number of different countries.

a. Where a controller has an establishment in Austria and processes personal data in Austria in the context of the activities of that establishment, the applicable law would obviously be the law of Austria - that is, where the establishment is situated.

b. In the second scenario, the controller has an establishment in Austria, in the context of activities of which he processes personal data collected via its website. The website is accessible to users in various countries. The data protection law applicable will still be the law of Austria - that is, where the establishment is situated - independently of the location of users and of the data.

c. In the third scenario, the controller is established in Austria and outsources the processing to a processor in Germany. The processing in Germany is in the context of the activities of the controller in Austria. That is to say, the processing is carried out for the business purposes of, and on instructions from the Austrian establishment. Austrian law will be applicable to the processing carried out by the processor in Germany. In addition, the processor will be subject to the requirements of German law in relation to the security measures it is obliged to put in place in connection with the processing[21]. Such arrangements would require coordinated supervision by the German and Austrian DPAs.

d. In the fourth scenario, the controller established in Austria opens a representation office in Italy, which organizes all the Italian contents of the website and handles Italian users' requests. The data processing activities carried out by the Italian office are conducted in the context of the Italian establishment, so that Italian law would apply to those activities.

[21] Pursuant to Article 17(3) of Directive 95/46/EC the processor is bound by the obligations as defined by the law of the Member State in which the processor is established with regard to security measures. In case of conflict between the substantive security obligations of the law of the processor and the law of the controller, the *lex loci* (law of the processor) prevails. While the ultimate liability remains with the controller, the processor has to prove that he took all necessary steps according to his contract with the controller as well as the security obligations as defined by the law of the Member State in which the processor is established (see more under III.5).

Conclusions on the law applicable can only be drawn on the basis of a precise understanding of the notion "in the context of the activities". The following considerations should be taken into account to conduct this analysis:

The degree of involvement of the establishment(s) in the activities in the context of which personal data are processed is crucial. Here the issue is to check "who is doing what", i.e. which activities are being carried out by which establishment, so as to be able to determine whether the establishment is relevant in order to trigger the application of national data protection law. Where an establishment is processing personal data in the context of its own activities, the applicable law will be the law of the Member State in which that establishment is located. Where the establishment processes personal data in the context of the activities of another establishment, the applicable law will be that of the Member State in which the other establishment is located.

The nature of the activities of the establishments is a secondary element, but it will help in identifying the law applicable to each establishment: the question whether an activity involves data processing or not, and which processing is taking place in the context of which activity largely depends on the nature of these activities. Alternatively, the fact that different establishments may be involved in totally different activities, in the context of which personal data are being processed, will have an impact on the law applicable. Example 4 develops an illustration of these considerations.

The overall objective of the Directive should also be taken into consideration, as it aims at guaranteeing an effective protection to individuals, in a simple, workable and predictable way.

Example No. 2: Transfer of personal data in connection with factoring

An Italian utility company transfers information about its debtors to a French investment bank with a view to factoring the debts. The debts have arisen in relation to unpaid electricity bills. This transfer of debt information involves the transfer of customers' personal data to the French investment bank, specifically, to the branch office in Italy (that is to say, the establishment of the French bank in Italy).

The French investment bank is a data controller in respect of the processing operations that constitute the transfer and its Italian branch performs management and levying of the debt on its behalf. The data are processed by the data controller both in France and at the Italian branch office. The French data controller provides all Italian customers with an information notice on the above operation by way of the Italian branch.

The Italian branch is an establishment for the purposes of the Directive, and its activities consisting of processing personal data to inform customers of the arrangements will have to comply with Italian data protection legislation. Security measures within the Italian branch will also have to comply with the conditions of Italian data protection legislation, while the French controller will have to comply in parallel with French security obligations for data processed within its establishment in France. Data subjects, i.e. the debtors, may apply to the office of the Italian branch in order to exercise their data protection rights such as access, rectification, and erasure under Italian law.

A functional approach should be taken in the analysis of these criteria: more than the theoretical evaluation made by the parties about the law applicable, it is their practical behaviour and interaction which should be the determining factors: what is the true role of each establishment, and which activity is taking place in the context of which establishment?

Attention should be paid to the degree of involvement of each establishment, in relation to the activities in the context of which personal data are processed. An understanding of the notion of "in the context of" is therefore also useful in complex cases to split different activities carried out by different EU establishments of the same company.

Example No. 3: Collection of clients' data by shops

A chain of "prêt à porter" shops has its head office in Spain, and shops all over the EU. The collection of data relating to clients takes place in every shop, but the data are transferred to the Spanish head office where some activities related to the processing of data take place (analysis of clients' profiles, service to customers, targeted advertising).

Activities such as direct marketing of Europe-wide customers are directed exclusively by the head office in Spain. Such activities would qualify as taking place in the context of the activities of the Spanish establishment. Spanish law would therefore be applicable to these processing activities.

However, the individual shops remain responsible for the aspects of the processing of their customers' personal data which take place in the context of the shops' activities (for example, the collection of customers' personal information). To the extent that processing is carried out in the context of each shop's activities, such processing is subject to the law of the country where the shop in question is established.

A direct practical consequence of this analysis is that each shop must take necessary steps to inform individuals about the conditions of collection and further processing of their data under its own national legislation.

Clients may go directly to the DPA of their own country in case of complaint. If the complaint relates to direct marketing actions in the context of the activities of the Spanish head office, the local DPA would have to refer the case to the Spanish DPA.

It is thus possible that a single establishment may be involved in a number of different types of activities, and that different national laws may be applicable to the processing of data in the context of these different activities. In order to provide for a predictable and workable approach where there is a possibility of multiple laws applying to the various activities of a single establishment, a functional approach should be used, including consideration of the broader legal context.

Example No. 4: Human resources centralised database

Situations where the same database can be subject to different applicable laws do increasingly happen in practice. This is often the case in the field of human resources where subsidiaries/establishments in different countries centralise employee data in a single database. While this traditionally happens for reasons of economies of scale, it should not have an impact on the responsibilities of each establishment under local law. This is the case not only from a data protection perspective, but also in the context of

labour law and public order provisions.

If, for instance, data of the employees of an Irish subsidiary (which qualifies as establishment) were transferred to a centralised database in the UK, where data of employees of the UK subsidiary/establishment are also stored, two different data protection laws (Irish and UK) would apply.

The application of two different national laws is not simply a result of the data originating in two different Member States, but instead arises as the processing of the Irish employee data by the UK establishment takes place in the context of the activities of the Irish establishment in its capacity of employer.

This example illustrates the fact that it is not the place where data are sent or located which determines which national law will apply, the key factors are the nature and place of normal activities which determine the "context" in which the processing is carried out: human resource or client data are thus normally subject to the data protection law of the country where the activity - in the context of which the data are being processed - takes place. It also confirms that there is no direct correlation between applicable national law and jurisdiction, as national law may apply outside national jurisdiction.

To sum up, the criteria used to determine applicable law have an impact at different levels:

- First, they help determining whether EU data protection law is applicable to the processing at all;

- Second, where EU data protection law applies, the criteria will determine both
  (a) which Member State data protection law is applicable, and
  (b) in case of multiple establishments in different Member States, which Member State's data protection law will apply to which processing activity;

- Third, the criteria will assist where there is an extra-European dimension to the processing activities – as in the following illustration in which the controller is established outside the EEA.

Example No. 5: Internet service provider

An internet service provider (the data controller) has its headquarters outside the EU, e.g. in Japan. It has commercial offices in most Member States of the EU, and an office in Ireland dealing with issues connected with the processing of personal data, including in particular IT support. The controller is developing a data centre in Hungary, with employees and servers devoted to the processing and storage of data relating to the users of its services.

The controller in Japan also has other establishments in various Member States of the EU, with different activities:

- the data centre in Hungary is only involved in technical maintenance;

- the commercial offices of the ISP organise general advertising campaigns;

- the office in Ireland is the only establishment within the EU, with activities in the context of which personal data are effectively being processed (notwithstanding the input from the Japanese headquarters).

The activities of the Irish office trigger the application of EU data protection law: personal data are processed in the context of the Irish office's activities, therefore such processing is subject to EU data protection legislation.

The law applicable to processing carried out in the context of the Irish office's activities is Irish data protection legislation, regardless of whether the processing takes place in Portugal, Italy or any other Member State.

This means that, in this hypothesis, the data centre in Hungary would have to comply with Irish data protection law with regard to the processing of the personal data of the users of the service provider. This would be without prejudice however to the application of Hungarian law to a distinct processing of personal data by the Hungarian data centre, in relation to its own activities – for instance processing of personal data concerning the employees of the data centre.

For the commercial offices based in other Member States, if their activity is limited to general non-user-targeted advertising campaigns which do not involve the processing of users' personal data, they are not subject to EU data protection laws. However, if they decide to conduct a processing in the context of their activities involving the personal data of individuals in the country where they are established (such as sending targeted advertisements to users and possible future users for their own business purposes), they will have to comply with the local data protection legislation.

If no connection can be established between the processing of data and the Irish establishment (IT support is very limited and there is no involvement in the processing of personal data), other provisions of the Directive could still trigger the application of data protection principles, for example if the controller uses equipment in the EU. This is considered in chapter III.3 below.

III.2. Controller established where Member State's law applies by virtue of international public law (Article 4(1)b)

Article 4(1)b addresses the less common case in which a Member State's data protection law applies where "the controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law".

III.2.a) "… the controller is not established on the Member State's territory …"

The first condition should be construed as meaning, for reasons of consistency within Article 4(1) that the controller does not have on the Member State's territory any establishment that would trigger the applicability of Article 4(1)a (see also below, III.3.a). In other words, in the absence of a relevant establishment in the EU, no national data protection law could be identified pursuant to Article 4(1)a.

III.2.b) "…, but in a place where its national law applies by virtue of international public law…"

However, external criteria stemming from international public law may determine in specific situations the extension of the application of a national data protection law beyond the national boundaries. This may be the case where international public law or international agreements determine the law applicable in an embassy or a consulate, or the law applicable to a ship or airplane. In those cases where the controller is established in one of these specific places, the applicable national data protection law will be determined by international law.

It is however important to also highlight that national data protection law may not apply to foreign missions or international organisations on EU territory to the extent in which they have a special status under international law, either in general or via a headquarter agreement: such exemption would prevent the application of Article 4(1)a to the mission or international organisation.

Example No. 6: Foreign embassies

An EU Member State's embassy in Canada is subject to the national data protection law of that Member State, and not to the Canadian data protection law.

Any country's embassy in the Netherlands is not subject to the Dutch data protection law as any embassy has a special status under international law. A data security breach occurring in the context of the activities of that embassy would therefore not trigger the application of the Dutch data protection law and consequent enforcement measures.

A non-governmental organisation with offices in EU Member States would not, in principle, benefit from a similar exemption, unless explicitly provided for by an international agreement with the host country.

III.3. Controller not established on Community territory but processing data through equipment located in a Member State (Article 4(1)c)

Article 4(1)c strives to ensure the right to the protection of personal data provided by the EU Directive even where the controller is not established in EU/EEA territory but where the processing of personal data has a clear connection with such territory, as indicated in Recital 20[22].

Article 4(1)c establishes the application of a Member State's law where "*the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community*".

[22] Recital 20: "*Whereas the fact that the processing of data is carried out by a person established in a third country must not stand in the way of the protection of individuals provided for in this Directive; whereas in these cases, the processing should be governed by the law of the Member State in which the means used are located, and there should be guarantees to ensure that the rights and obligations provided for in this Directive are respected in practice*"

This provision is especially relevant in the light of the development of new technologies and in particular of the internet, which facilitate the collection and processing of personal data at a distance and irrespective of any physical presence of the controller in EU/EEA territory[23].

a) "… the controller is not established on Community territory …"

This provision becomes relevant when the controller has no presence in EU/EEA territory which may be considered as an establishment for the purposes of Article 4(1)a of the Directive, as analyzed above.

It is important to clarify the interpretation of the wording "is not established". It should be clear that Article 4(1)c applies only when Article 4(1)a is not applicable: i.e. when the controller does not have any establishment *that is relevant for the activities in question* in the EU/EEA. Therefore, the fact that a controller established outside the EU/EEA makes use of equipment in Member State A where it has no establishment would not trigger the applicability of that Member State's law, if the controller already has an establishment in Member State B and is processing the personal data in the context of the activities of that establishment. Both the processing in Member State A (where equipment is being used) and in Member State B (where there is the establishment) will be subject to Member State B law. This was made clear by the Working Party in its opinion on data protection issues related to search engines[24].

On the other hand, Article 4(1)c will apply where the controller has an "irrelevant" establishment in the EU. That is to say, the controller has establishments in the EU but their activities are *unrelated to the processing of personal data*. Such establishments would not trigger the application of Article 4(1)a.

This means that, since there should be no lacunae or inconsistency in the application of the provisions of the Directive, the application of the "equipment" criterion need not be prevented by an irrelevant establishment: it could be prevented by the existence of an establishment only to the extent that this establishment processed personal data in the context of the same activities.

A corollary of this interpretation is that a company with diverse activities could trigger the application of both Articles 4(1)a and 4(1)c if it used equipment and had establishments in different contexts. In other words, a controller established outside the EU/EEA and using equipment in the EU would have to comply with Article 4(1)c even if it had an establishment in the EU, as long as this establishment processed personal data *in the context of other activities*. This establishment would trigger the application of Article 4(1)a for these specific activities.

An opportunity to better clarify the scope of Article 4(1)c and what is meant by "the controller is not established on Community territory" may arise during the revision of the data protection framework, in line with the spirit of the Directive and the wording of its Recital 20. The preamble of the Directive clearly states that the objective is to protect individuals and avoid gaps in the application of the principles. For this reason the

---

[23] See the Working Party's Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites (WP 56).

[24] Article 29 Working Party Opinion 1/2008 on data protection issues related to search engines (WP 148)

Working Party considers that Article 4(1)c should apply in those cases where there is no establishment in the EU/EEA *which would trigger the application of Article 4(1)a* or where the processing *is not carried out in the context* of the activities of such an establishment.

> b) "… and for purposes of processing personal data makes use of equipment, automated or otherwise situated on the territory of the Member State …"

The crucial element which determines the applicability of this Article and thus of a Member State's data protection law is the use of equipment situated on the territory of the Member State.

The Working Party has already clarified that the concept of "making use" presupposes two elements: some kind of activity of the controller and the clear intention of the controller to process personal data[25]. Therefore, whilst not any use of equipment within the EU/EEA leads to the application of the Directive, it is not necessary for the controller to exercise ownership or full control over such equipment for the processing to fall within the scope of the Directive.

It has to be noted that there is a difference between the word used in the English version of Article 4 (1) c 'equipment', and the word used in other language versions of Article 4 (1) c, which are more akin to the English word 'means'. The terminology used in other language versions of Article 4 (1) c is also consistent with the wording of Article 2 (d) defining the controller: the person who decides about the purposes and the "means" of the processing.

In view of these considerations, the Working Party understands the word "equipment" as "means"[26]. It also notes that according to the Directive this could be "automated or otherwise".

This leads to a broad interpretation of the criterion, which thus includes human and/or technical intermediaries, such as in surveys or inquiries. As a consequence, it applies to the collection of information using questionnaires, which is the case, for instance, in some pharmaceutical trials.

There is a question whether outsourcing activities, notably by processors, carried out in the EU/EEA territory on behalf of controllers established outside EEA may be considered as "equipment". The broad interpretation advocated above leads to a positive answer, provided they are not acting in the context of the activities of an establishment of the controller in the EEA - in which case Article 4(1)a would apply. However, account should be taken of the sometimes undesirable consequences of such an interpretation, as developed below in III.4: if controllers established in different countries over the world have their data processed in a Member State of the EU, where the database and the processor are located, those controllers will have to comply with the data protection law of that Member State.

---

25 WP56, op. cit.

26 It should also be recalled that the English language text of the Directive in previous versions (for instance, in the amended proposal of 1992 - COM (92) 422 final) also used the term "means", even though this was modified in the course of the negotiations, at quite a late stage, to the term "equipment", as can be seen in the text of the common position of March 1995.

A case-by-case assessment is needed whereby the way in which the equipment is actually used to collect and process personal data is assessed. On the basis of this reasoning, the Working Party recognized the possibility that personal data collection through the computers of users, as for example in the case of cookies or Javascript banners, trigger the application of Article 4(1)c and thus of EU data protection law to service providers established in third countries[27].

This interpretation of the "use of equipment" provision favours a wide scope of application. However, as mentioned, it also highlights some consequences which are not satisfactory, when the result is that European data protection law is applicable in cases where there is a limited connection with the EU (e.g. a controller established outside the EU, processing data of non-EU residents, only using equipment in the EU). There is an obvious need for more clarity and for further conditions to the application of this criterion, in order to bring more certainty in the future data protection framework. This point will be developed below in the concluding part of this document.

As another illustration, the extent to which telecommunication terminals or parts of them should be considered as equipment is not obvious. The fact that the tool is designed or used primarily in order to collect or further process personal data can be considered as an indicator in this respect. However, the fact that a controller knowingly collects personal data, even incidentally, by using some equipment in the EU, also triggers the application of the Directive.

Example 7: Geo-location services

A company located in New-Zealand uses cars globally, including in EU Member States, to collect information on Wi-Fi access points (including information about private terminal equipment of individuals) in order to provide a geo-location service to its clients. Such activity involves in many cases the processing of personal data.

The application of the Data Protection Directive will be triggered in two ways:
- First, the cars collecting Wi-Fi information while circulating on the streets can be considered as equipment, in the sense of Article 4(1)c;
- Second, while providing the geo-location service to individuals, the controller will also use the mobile device of the individual (through dedicated software installed in the device) as equipment to provide actual information on the location of the device and of its user.

Both the collection of information with a view to provide the service, and the provision of the geo-location service itself, will have to comply with the provisions of the Directive.

Example No. 8: Cloud computing

Cloud computing, where personal data are processed and stored on servers in several places around the world, is a complex example of the application of the provisions of the Directive. The exact place where data are located is not always known and it can change in time, but this is not decisive to identify the law applicable. It is sufficient that the controller carries out processing in the context of an establishment within the EU,

[27] WP56, op. cit., p. 10 f.

or that relevant means is located on EU territory to trigger the application of EU law, as provided in Article 4(1)c of the Directive.

The first decisive step will be to identify who is the controller, and which activities take place at which level. Two perspectives can be identified:

The user of the cloud service is a data controller: for instance, a company uses an agenda service on-line to organise meetings with clients. If the company uses the service in the context of the activities of its establishment in the EU, EU law will be applicable to this processing of data via the agenda on-line on the basis of Article 4(1)a. The company should make sure that the service provides for adequate data protection safeguards, notably with regard to the security of personal data stored on the cloud. It will also have to inform its clients of the purpose and conditions of use of their data.

The cloud service provider can also in some circumstances be a data controller: this would be the case when it provides for an agenda on-line where private parties can upload all their personal appointments and it offers added value services such as synchronisation of appointments and contacts. If the cloud service provider uses means in the EU, it will be subject to EU data protection law on the basis of Article 4(1)c. As demonstrated below, the application of the Directive would not be triggered by means used for transit purposes only, but it would be triggered by more specific equipment e.g. if the service uses calculating facilities, runs java scripts or installs cookies with the purpose of storing and retrieving personal data of users. The cloud service provider will then have to provide users with information on the way data are being processed, stored, possibly accessed by third parties, and to guarantee appropriate security measures to protect the information.

Example No. 9: A controller publishes country-by-country lists of paedophiles

A controller established in one EU/EEA Member State publishes country-by-country lists of persons suspected of or sentenced for criminal offences involving minors. With regard to the right to the protection of personal data of listed persons, the applicable law – according to which the lawfulness of this processing should be assessed – is the national data protection law of the Member State where the controller is established.

It is irrelevant for the determination of applicable data protection law whether the controller uses equipment in other Member States (such as internet servers with different top-level domain names, including .fr, .it, .pl, etc.), or whether it directly targets citizens from other EU countries (for example, by publishing country-specific lists of names in the language of those countries) in processing data for this purpose.

The supervisory authority of the Member State of establishment may in any case be called by other supervisory authorities to cooperate, by acting on complaints lodged by individuals located in other Member States.

Of course, different connection criteria and thus applicable laws could be applied in other areas of law, such as for example to file a suit for defamation according to criminal or civil law.

c) "…unless used only for purposes of transit through Community territory …"

The application of the national law of an EU Member States is excluded when the equipment used by the controller and located within the Member State is used only in order to ensure transit through Union territory, such as for example in the case of telecommunication networks (cables) or postal services which only ensure that communications transit through the Union in order to reach third countries.

As this is an exception to the equipment criterion, it should be subject to a narrow interpretation. It should be noted that the effective application of this exception is becoming infrequent: in practice, more and more telecommunication services merge pure transit and added value services, including for instance spam filtering or other manipulation of data at the occasion of their transmission. The simple "point to point" cable transmission is disappearing gradually. This should also be kept in mind when reflecting on the revision of the data protection framework.

d) "… must designate a representative established on the Member State's territory …" (Article 4(2))

The Directive imposes an obligation on the controller to designate 'a representative' in the territory of the Member State whose law is applicable by virtue of the controller's use of equipment in that Member State to process personal data. This is "without prejudice to legal actions which could be initiated against the controller himself".

In this last case, the question of enforcement against a representative raises practical issues, as shown by Member States' experience. This would be the case if for instance the only representative of the controller within the EU is a law firm. There is no uniform answer in national implementing provisions to the question whether the representative can be held responsible and sanctioned, on a civil or criminal basis, on behalf of the controller. The nature of the relationship between the representative and the controller is decisive here. In some Member States, the representative substitutes for the controller, also with regard to enforcement and sanctions, while in others it has a simple mandate. Some national laws explicitly foresee fines applicable to the representatives[28], while in other Member States this possibility is not envisaged[29].

Harmonisation is needed in this respect at European level, with the objective of giving more effectiveness to the role of the representative. In particular, data subjects should be able to exercise their rights against the representative, without prejudice to legal actions which could be initiated against the controller himself.

III.4. Considerations on the practical consequences of the application of Article 4(1)c

A decisive aspect of the application of Article 4(1)c relates to its practical consequence for the data controller. While located outside the EU/EEA, he will have to apply the

[28] Belgian data protection law of 8 December 1992, O.J. 18 March 1993; Dutch Act of 6 July 2000 regarding the protection of personal data, Bulletin of Acts, Orders and Decrees (Staatsblad) No. 302, 20 July 2000. See also the Greek legislation (Article 3 par. 3.b in combination with Article 21 par. 1 of Law 2472/1997).

[29] The French legislation 78/17 of 6 January 1978, for instance, does not foresee such type of fines on representatives.

principles of the Directive if he uses equipment located in the EU territory for personal data processing operations. It could be questioned whether the principles will only be applicable to the part of the processing taking place in the EU, or to the controller as such, for all the stages of the processing, even those taking place in a third country. These questions have particular significance in network environments such as cloud computing, or in the context of multinational companies.

Let us consider, for example, the implications for controllers established in different countries over the world, having their data processed in France, where the database and the processing equipment are located. If the different controllers make use of infrastructure in France, Article 4(1)c is applicable and all controllers would have to comply with French law. This may have undesirable consequences in terms of economic impact and enforceability.

Practical reasons would push for a mitigation of the application of the "equipment/means" criteria, but this is counterbalanced by the fact that data protection principles aim at the protection of a fundamental right. Limiting the rights of individuals to some parts of the processing of their data does not seem admissible. Nor would it be acceptable to reduce the scope of protection to persons residing in the EU, since the fundamental right to protection of personal data is enjoyed regardless of nationality or residence. Consequently, the criterion of Article 4(1)c results in the principles of the Directive being applicable to the controller as such, for all the stages of the processing, even those taking place in a third country.

The application of the Directive to a controller for the whole processing should be supported as long as the link with the EU is effective and not tenuous (such as by almost inadvertent, rather than intentional, use of equipment in a Member State).

A more specific connecting factor, taking the relevant "targeting" of individuals into account, as a complement to the "equipment/means" criteria could be useful in terms of legal certainty, as further developed in the conclusions. Such a criterion is not new and has been used in other contexts in the EU[30], and by the United States' legislation on the protection of children on-line[31]. This is also the case in some national laws transposing Directive 2000/31/EC on electronic commerce[32], stating that providers not established in the EEA will fall within the scope of these national laws when they target services specifically to their territory.

The application of a similar criterion for the data protection legislation in the EU could be reflected upon during future discussions on the revision of the data protection framework.

---

30 Cf. Article 15(1)c of Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (OJ L 12, 16.1.2001, p.1), and for its interpretation, see the Conclusions of Advocat General Trstenjak, 18 May 2010, in C-144/09, *Hotel Alpenhof* .

31 The application of the COPPA can indeed be triggered either by the location of a publisher in the US, or by the fact that US children are targeted by the website: foreign-based websites and online services must comply with COPPA if they are directed to, or knowingly collect or disclose personal information from, children in the United States. See 16 CFR 312.2, available at http://www.ftc.gov/os/1999/10/64fr59888.pdf, p. 59912.

32 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') OJ L 178 , 17.7.2000, p.1

Another practical consequence of the application of Article 4(1)c concerns the interaction between this provision and Articles 25 and 26 of the Directive. The fact that the controller established outside the EU/EEA uses equipment on EU/EEA territory - and must therefore comply with all relevant provisions of the Directive - would also entail the possible application of Articles 25 and 26. However, it may be difficult in practice to determine exactly the implications of such a scenario.

For instance, if a controller X based outside the EEA collects personal data through the use of equipment located on EU territory (for instance through the use of cookies or via a processor), he has to comply with the Directive for all stages of the processing. There is a certain parallel here with the situation where a controller established in the EEA transfers personal data to a processor outside the EEA: in this case as well, the controller and the processor established outside EEA territory will be bound by the Directive. However, the way in which these principles are implemented in practice, in accordance with the adequacy requirements of Articles 25 and 26 of the Directive, in an Article 4(1)c scenario involving a controller established outside the EEA, is not totally clear. The Working Party considers that the existing tools regulating the conditions for transfers should be further reflected upon so as to better cover this situation.

III.5. Law applicable to security measures (Article 17(3))

Article 17(3) establishes that the contract or the legal act binding the processor to the controller should also ensure compliance with the security measures "*defined by the law of the Member State in which the processor is established*".

The reason behind this principle is to ensure uniform requirements within one Member State with regard to security measures, and facilitate enforcement. It should be noted however that in a European perspective, security requirements diverge considerably depending on Member States: some provide for very detailed rules while others have just copied the general wording of the Directive. Where national laws are general and their wording is taken from the Directive, this will not have any practical consequences. It would not be a problem for a processor to comply with more detailed obligations imposed on him by the controller according to its national law, or alternatively for a controller to accept more detailed requirements according to the law of the processor. Only in cases where detailed rules are different or even in conflict, Article 17(3) decides in favour of the law of the processor[33]. However, it seems advisable that further harmonisation of security obligations should be included in the scope of discussion on the revision of the data protection framework.

III.6. Competence and cooperation of supervisory authorities (Article 28(6))

As mentioned above (see para. II.2.e) Article 28(6) aims at bridging the possible gap between applicable law and supervisory jurisdiction, which may arise in the area of data protection within the internal market.

Pursuant to this provision, national data protection authorities are competent to supervise the implementation of the data protection legislation on the territory of the Member State

[33] This should avoid the appointment of a data processor in another country with lower obligations being regarded as a violation of the obligations of the data controller.

where they are established. But if the law of another Member State were applicable on its territory, the enforcement powers of the DPA would not be limited: the applicable law criteria of the Directive foresee the possibility that a DPA is empowered to verify and intervene on a processing operation that is taking place on its territory even if the law applicable is the law of another Member State.

III.6.a) "…supervisory authority is competent, whatever national law applicable…"

This provision makes a national supervisory authority competent to always act within the limits of its territorial jurisdiction, irrespective of whether the law applicable is its national data protection law or the data protection law of another Member State.

III.6.b) "…to exercise its powers on the territory of its own Member State…"

Also, when a data protection law of another Member State is applicable, the supervisory authority will be in a position to fully exercise on its territory all powers conferred to it by its national legal system. This includes investigative powers, powers of intervention, power to engage in legal proceedings, power to impose sanctions.

Where several DPAs are involved, including the DPA of the location and the DPAs whose law is applicable, it is essential that cooperation is organised, and that the role of each DPA is clear. Several questions should therefore be addressed, including notably:

- procedural issues, such as the identification of the lead authority, and the way it will cooperate with the other DPAs;
- the scope of competences to be exercised by each DPA. In particular, how far will the DPA of the location exercise its powers with regard to the application of the material principles and the sanctions? Should it limit the use of its powers to the verification of facts, can it take provisional measures of enforcement or even definitive measures? Can it give its own interpretation of the provisions of the law applicable, or is it the prerogative of the DPA of the Member State whose law is applicable? It should be noted in this regard that not all national laws foresee the possibility to impose sanctions on all stakeholders.[34]

A high level of harmonisation of the supervisory powers conferred to supervisory authorities pursuant to Article 28 of the Directive is an essential condition to guarantee that cross-border data protection compliance is ensured in an effective and non-discriminatory way. This issue deserves further analysis, and the Working Party will provide guidance in this regard in a separate paper.

Example No. 10: Intra-EU cross-border processing of personal data

Processing activities are taking place in the UK, but in the context of the activities of an establishment of the controller located in Germany. This will have the following consequences:

- German law will be applicable to the processing in the UK;

- The UK DPA needs to have the power to inspect the premises in the UK, and establish findings, to be transmitted to the German DPA;

[34] The Greek law for instance provides for sanctions only on data controllers and their representatives and not on processors.

- The German DPA should be able to impose a sanction on the controller established in Germany on the basis of the findings of the UK DPA.

As an additional element, if the establishment in the UK is a processor, security aspects of the processing are subject to the requirements of UK data protection law. This then leads to the question how the requirements of that law could be properly enforced.

III.6.c) "…mutual cooperation to the extent necessary for performance of duties…"

Supervisory authorities have an obligation to cooperate ("shall"), but at the same time this obligation is limited to what is necessary in order to perform their duties. Therefore, requests for cooperation should be related to the exercise of their competences and usually relate to cases with cross-border relevance.

The provision refers in particular to the exchange of "all useful information", which could relate for example to information on the relevant provisions and legal instruments applicable to the specific case. However, cooperation is likely to take place also at different levels: handling cross-border complaints, collecting evidence for other DPAs, or imposing sanctions.

The issue is even more acute in an international context, with data controllers operating worldwide, and it calls for improvements in terms of enforcement cooperation. Initiatives such as the 'Global Privacy Enforcement Network (GPEN)', involving data protection authorities from various continents, are a necessary and welcome step in this perspective.

Example No. 11: Social network having its headquarters in a third country and an establishment in the EU

A social network platform has its headquarters in a third country and an establishment in a Member State. The establishment defines and implements the policies relating to the processing of personal data of EU residents. The social network actively targets residents of all EU Member States, which constitute a significant portion of its customers and revenues. It also installs cookies on EU users' computers.

In this case, the applicable law will be, pursuant to Article 4(1)a, the data protection law of the Member State where the company is established within the EU. The issue of whether the social network makes use of equipment located in other Member States' territory is irrelevant, since all processing takes place in the context of the activities of the single establishment and the Directive excludes the cumulative application of Articles 4(1)a and 4(1)c.

However, the supervisory authority of the Member State where the social network is established in the EU will - pursuant to Article 28(6) – have a duty to cooperate with other supervisory authorities, in order for example to deal with requests or complaints coming from residents of other EU countries.

Example No. 12: European e-health platform

A platform is set up at European level in order to facilitate the processing of cross-border handling of patient records. The platform allows for the exchange of patients summary data sets, medication records and prescriptions in order to facilitate healthcare services when travelling abroad.

While the platform facilitates the exchange of information, there will still be in each Member State one or several establishments in the context of which activities patients' data are processed. For instance, if a Bulgarian resident travelling to Portugal needs urgent treatment, his record will be processed via the platform by Portuguese medical services under Portuguese data protection law. If the patient wished to claim redress once back in Bulgaria with regard to the processing of his data by the Portuguese controller, he would first lodge his claim with the Bulgarian DPA. The Bulgarian DPA will then collaborate with the Portuguese DPA to establish the facts and check whether there has been an infringement under Portuguese legislation.

If the European Commission intervenes in the functioning of the platform by organising personal data flows and guaranteeing the security of the system, it may also be considered as processing personal data, which would trigger the application of Regulation (EC) 45/2001. In this example, if the Bulgarian citizen complained about a security breach involving his medical data, the Bulgarian DPA would collaborate with the EDPS in order to identify the conditions and consequences of the breach.

IV. Conclusions

This opinion aims at clarifying the scope of application of Directive 95/46/EC, and in particular Article 4 of the Directive. However, it also highlights some areas for possible further improvement. The main findings in these two respects are summarised below.

IV.1. Clarifying current provisions

Determining the application of EU law to the processing of personal data serves to clarify the scope of EU data protection law both in the EU/EEA and in a wider international context. A clear understanding of applicable law will help to ensure both legal certainty for controllers and a clear framework for individuals and other stakeholders. Furthermore, a correct understanding of the applicable law provisions should ensure that no lacunae or loopholes may be found in the high level of protection of personal data provided by Directive 95/46.

The key provision on applicable law is Article 4, which determines which national data protection law(s) adopted pursuant to the Directive may be applicable to the processing of personal data.

Pursuant to Article 4(1)a, a Member State must apply its national data protection law where the processing is carried out in the context of an establishment of the controller on the territory of the Member State. Key to the identification of a relevant establishment for the purposes of Article 4(1)a is whether the organisation in question conducts the

effective and real exercise of activities. Furthermore, the reference to "an" establishment means that the applicability of a Member State's law will be triggered by the location of an establishment of the controller in that Member State, and other Member States' laws could be triggered by the location of other establishments of that controller in those Member States.

The notion of "context of activities" – and not the location of data – is a determining factor in identifying the scope of the applicable law. The notion of "context of activities" implies that the applicable law is not the law of the Member State where the *controller* is established, but where an *establishment* of the controller is involved in *activities* implying the processing of personal data. In this context, the degree of involvement of the establishment(s) in the activities, in the context of which personal data is processed, is crucial. In addition, the nature of the activities of the establishments and the need to guarantee effective protection of individuals' rights should be considered. A functional approach should be taken in the analysis of these criteria: more than the theoretical indication by the parties of the law applicable, it is their practical behaviour and interaction which should be decisive.

Article 4(1)b addresses the less common case in which a Member State's data protection law applies where "the controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law". External criteria stemming from international public law will determine in specific situations the extension of the application of a national data protection law beyond the national boundaries, as for example in the case of embassies or ships.

Article 4(1)c strives to ensure the right to the protection of personal data provided by the EU Directive even where the controller is not established in EU/EEA territory but where the processing is in some way connected with the EU/EEA. To ensure consistency within Article 4 and to avoid gaps in the application of data protection law, the Working Party considers that the application of Article 4(1)c should not be prevented by the existence of an establishment of the controller on Community territory where that establishment is not a relevant establishment for the purposes of Article 4(1)a. Instead, the "use of equipment" provision in Article 4(1)c should apply in those cases where there is no establishment in the EU/EEA *which would trigger the application of Article 4(1)a* or where the processing *is not carried out in the context* of such an establishment.

The crucial element which determines the applicability of Article 4(1)c and thus of a Member State's data protection law is the use of equipment situated on the territory of the Member State. The concept of "making use" presupposes two elements: some kind of activity of the controller and the clear intention of the controller to process personal data. Therefore, whilst not any use of equipment within the EU/EEA leads to the application of the Directive, it is not necessary for the controller to exercise ownership or full control over such equipment for the processing to fall within the scope of the Directive.

With regard to the notion of "equipment', its expression by "means" in other EU languages would lead to a broad interpretation of the criteria, favouring a wide scope of application. Such an interpretation may in some cases result in European data protection law being applicable where the processing in question has no real connection with the EU/EEA. In any case, the processing of personal data by a controller established outside the EU/EEA, through equipment in the EU/EEA, triggers the application of the Directive

pursuant to Article 4(1)c, which means that all other relevant provisions of the Directive will be applicable as well.

The application of the national law of a Member State is excluded when the equipment used by the controller and located within the Member State is used only in order to ensure transit through Community territory, such as for example in the case of telecommunication networks (cables) or postal services which only ensure that communications transit through the Community in order to reach third countries.

Article 4(2) imposes an obligation on the controller to designate a representative in the territory of the Member State whose law is applicable by virtue of the controller's use of equipment in that Member State to process personal data. In this last case, the enforcement against a representative can be a challenge.

Article 17(3) establishes that the contract or the legal act binding the processor to the controller should also provide that the processor is required to comply with the security measures "*defined by the law of the Member State in which the processor is established*". The reason behind this principle is to ensure uniform requirements within one Member State with regard to security measures, and facilitate enforcement.

Article 28(6) aims at bridging the possible gap between applicable law and supervisory jurisdiction, which may arise in the area of data protection within the internal market, by establishing that a DPA should be able to use its powers to verify and intervene in a processing operation that is taking place on its territory even if the law applicable is the law of another Member State.

IV.2. Improving current provisions

While the indications and examples developed above should contribute to enhancing legal certainty and protection of individuals' rights when defining the law applicable to the processing of personal data, some shortcomings were identified during their development.

The wording used in the Directive and the consistency between the different parts of Article 4 would benefit from further clarification as a part of the revision of the general data protection framework. The Working Party has identified a need for such further clarification in several areas:

a. There is a need to address the inconsistencies in the wording used in Articles 4(1)a and 4(1)c with regard to "establishment", and the notion that the controller is "not established" in the EU. To be consistent with Article 4(1)a which uses the criterion of "establishment", Article 4(1)c should apply in all cases where there is no *establishment* in the EU *which would trigger the application of Article 4(1)a* or where the processing *is not carried out in the context* of the activities of such an establishment.

b. Some clarification would also be useful with regard to the notion of "context of activities" of the establishment. The Working Party has emphasised the need to assess the *degree of involvement* of the establishment(s) in the activities in the context of which personal data are processed, or in other words to check "who is doing what" in which establishment. This criterion is interpreted taking into account

the preparatory works of the Directive and the objective set out at the time to keep a distributive approach of national laws applicable to the different establishments of the controller within the EU. The Working Party considers that Article 4(1)a as it stands now leads to a workable but sometimes complex solution, which seems to argue in favour of a more centralised and harmonised approach.

c. The change envisaged in order to simplify the rules for determining applicable law would consist of a shift back to the country of origin principle: all establishments of a controller within the EU would then apply the same law regardless of the territory in which they are located. In this perspective, the location of the main establishment of the controller would be the first criterion to be applied. The fact that several establishments exist within the EU would not trigger a distributed application of national laws.

d. This could only be acceptable however, if there are no significant differences between the laws of Member States. Any effective application of the country of origin principle would otherwise result in 'forum shopping' in favour of Member States whose legislation is considered as more permissive towards data controllers. This could obviously also harm data subjects. Legal certainty for data controllers and for data subjects would only be guaranteed if a comprehensive harmonisation of national legislation is reached, including harmonisation of security obligations. The Working Party therefore supports a strong harmonisation of data protection principles, also as a condition for a possible shift to the country of origin principle.

e. Additional criteria should apply when the controller is established outside the EU, with a view to ensuring that a sufficient connection exists with EU territory, and to avoid EU territory being used to conduct illegal data processing activities by controllers established in third countries. The two following criteria may be developed in this view:

   - The targeting of individuals, or "service oriented approach": this would involve the introduction of a criterion for the application of EU data protection law, that the activity involving the processing of personal data is targeted at individuals in the EU. This would need to consist of substantial targeting based on or taking into account the effective link between the individual and a specific EU country. The following examples illustrate what targeting could consist of: the fact that a data controller collects personal data in the context of services explicitly accessible or directed to EU residents, via the display of information in EU languages, the delivery of services or products in EU countries, the accessibility of the service depending on the use of an EU credit card, the sending of advertising in the language of the user or for products and services available in the EU. The Working Party notes that this criterion is already used in the field of consumer protection: applying it in a data protection context would bring additional legal certainty to controllers as they would have to apply the same criterion for activities which often trigger the application of both consumer and data protection rules**.**

   - The criterion of the equipment/means: this criterion has shown to have undesirable consequences, such as a possible universal application of EU law. Nonetheless, there is a need to prevent situations where a legal gap

would allow the EU being used as a data haven, for instance when a processing activity entails inadmissible ethical issues. The equipment/means criterion could therefore be kept, in a fundamental rights perspective, and in a residual form. It would then only apply as a third possibility, where the other two do not: it would address borderline cases (data about non EU data subjects, controllers having no link with EU) where there is a relevant infrastructure in the EU, connected with the processing of information. In this latter case, it might be an option to foresee that only certain data protection principles – such as legitimacy or security measures – would apply. This approach, which obviously would be subject to further development and refinement, would probably solve most of the problems in the current Article 4(1)c.

f. As a last recommendation, the Working Party calls for more harmonisation in the obligation of controllers established in third countries to appoint a representative in the EU, with the objective of giving more effectiveness to the role of the representative. In particular, the extent to which data subjects should be able to effectively exercise their rights against the representative should be clarified.

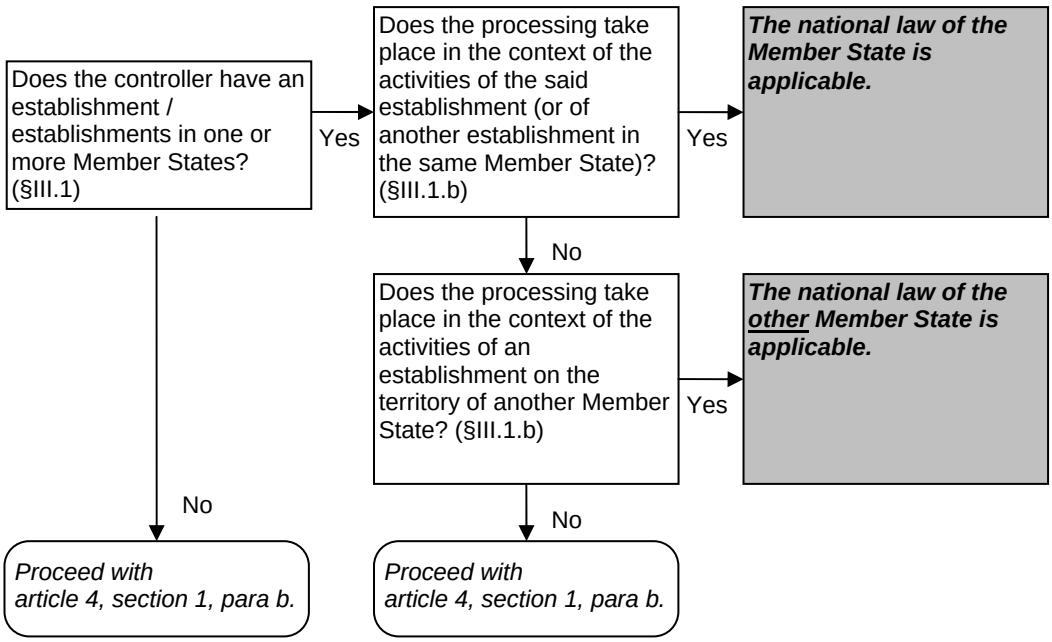
Done in Brussels, on 16 December 2010

For the Working Party,

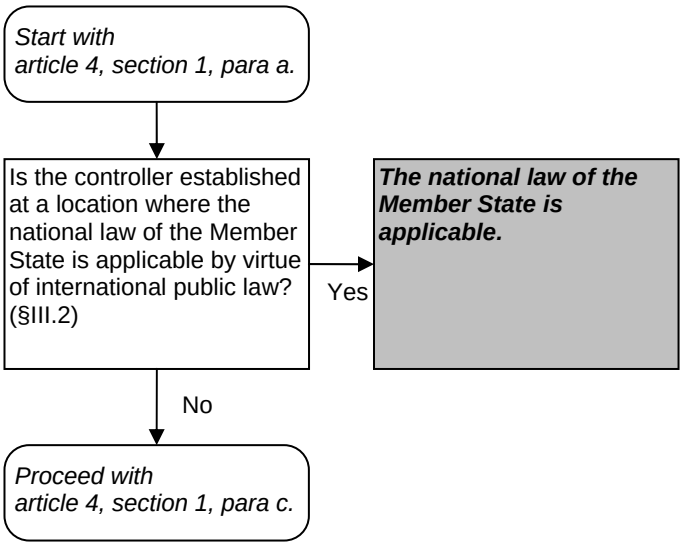
The Chairman
Jacob KOHNSTAMM

ANNEX

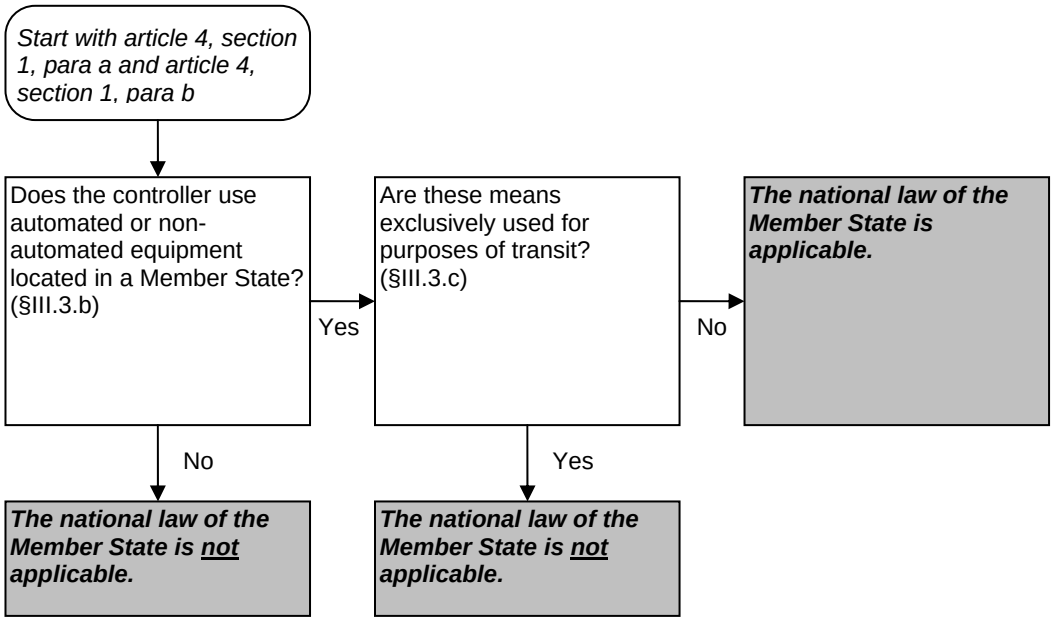
Article 4(1)a



Article 4(1)b



Article 4(1)c


Start with article 4, section 1, para a and article 4, section 1, para b
Does the controller use automated or non-automated equipment located in a Member State? (§III.3.b)
Yes
Are these means exclusively used for purposes of transit? (§III.3.c)
No
The national law of the Member State is applicable.
No
The national law of the Member State is not applicable.
Yes
The national law of the Member State is not applicable.