Back to basics: when does EU data protection law apply?

Lokke Moerel*

Abstract

- Discusses the key concepts of the main default rule for the applicability of EU data protection law, and provides for a uniform interpretation thereof based on the legislative history of the Data Protection Directive.
- Discusses the differences in the manner in which the rules on applicability are implemented in the Member States and the resulting divergent interpretations by the national Data Protection Authorities.
- Evaluates the present position of the Article 29 Working Party in the SWIFT opinion (which seems contrary to the legislative history of the Directive).
- Recommends that the European legislator revise the applicability regime of the Directive.

Introduction

It is much debated when the data protection laws of the EU Member States apply in international situations. In the previous issue of this journal,[1] I discussed whether the EU Data Protection Directive 95/46/EC[2] (the 'Directive') applies to the processing of personal data of EU citizens by non-EU websites. This required discussion of the long arm reach of the Directive as it applies to the use by foreign data controllers of processing 'equipment' located within the EU. In the present contribution, the main default rule is discussed as it applies 'to the processing of personal data in the context of the activities of an establishment of the controller on the territory of the Member State'.

The rules of applicability of the Directive are extraordinarily complex. The lack of guidance in the Directive on key concepts of applicable law and jurisdiction has lead to unacceptable differences in the manner in which this provision is implemented in the Member States. Also, the opinions of the Article 29 Working Party have taken conflicting interpretations of the law. As a consequence, the national Data Protection Authorities are very much left to their own devices to decide when to apply their data protection law, and in practice do so in a divergent manner, which causes widespread confusion within the international business community. Given the substantial obligations of controllers under the Directive, there is no greater uncertainty than not knowing to which data protection laws your data processing is subject. The Directive thus fails to meet its broader legal purpose to operate as a single market measure.[3] In this publication, an attempt is made to provide a uniform interpretation of the main applicability rule based on the legislative history of the Directive. Suggestions are also made as to which key concepts require further guidance from the Article 29 Working Party and what amendments to the Directive should be considered.

The Directive applies 'to the processing of personal data in the context of the activities of an establishment of the controller on the territory of

* ICT Partner at De Brauw Blackstone Westbroek, Amsterdam, the Netherlands and researcher at TILT (Tilburg Institute for Law, Technology and Society), Tilburg, the Netherlands. This publication draws on two earlier publications in Dutch on the interpretation by the Dutch DPA of Article 4 of the Dutch Data Protection Act, 'Back to Basics: wanneer is de Wet bescherming Persoonsgegevens van toepassing?' (2008) 3 *Computerrecht*, at 81 and 'Art. 4 Wbp revisited'; naschrift De nieuwe WP Opinie inzake Search Engines', (2008) 6 *Computerrecht* 291. E-mail: lokke.moerel@debrauw.com.

1 Lokke Moerel, 'The long arm reach: does the Data Protection Directive apply to processing of personal data of EU citizens by websites worldwide?' (2010) 1 International Data Privacy Law, Advance Access published 2 November 2010, doi: 10.1093/idpl/ipq004.

2 Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281/31 ('Data Protection Directive').

3 The legal basis for the Directive is Article 95 (currently Article 114 TFEU) of the Consolidated Version of the Treaty establishing the European Community, [2002] OJ C 325 ('EC Treaty'). See further Recitals 1–9 of the Directive (n 3).

the Member State'.[4] This provision has been implemented by some Member States by providing that their national data protection law applies only if the data controller is established on their territory. Also, some data protection authorities (DPAs) and authors apply the provision in this manner. At first glance this appears to be a perfectly legitimate interpretation of the Directive, but it creates a gap in the legal protection of personal data. As is often the case, it is necessary to review the full legislative history of a directive in order to determine the correct application. In this case, the outcome is surprising. The Directive seems to declare a national data protection law already applicable if the data processing takes place in the context of the activities of an establishment of a controller that is located on its territory. The controller itself does not have to be established in the Member State in question. This leads to a much wider scope of application of the national data protection laws. Further, in its SWIFT Opinion,[5] the Article 29 Working Party ('WP 29')[6] also applies the national data protection law of the Member State of the controller to data processing by establishments of such controller in other Member States (thereby sidelining the national data protection law of the establishments in the other Member States). This position of the WP 29 is probably designed to preclude an unnecessary cumulative application of the national EU data protection laws. However, it will become apparent that this interpretation by the WP 29 does not solve the problem of the cumulative application of national data protection laws, but rather creates gaps in the legal protection of personal data. Although the attempt of the WP 29 to avoid cumulative application of the EU data protection laws is very commendable, this result will only be achieved if the so-called 'country of origin' principle is also introduced into EU data protection law, which should be done by European legislation and not via the short-cut of opinions of the WP 29. In its first evaluation of the Directive in 2003,[7] the European Commission recognized the lack of clarity of Article 4 of the Directive, but announced that it would first make it a priority to ensure the correct implementation of Article 4 of the Directive in all Member States, before considering amendments. In December 2009, the WP 29 has also acknowledged the problem of the lack of clarity of Article 4 and the many different interpretations of it, and announced that it is writing an opinion on the concept of applicable law, which will include recommendations for future legal framework revisions (in response to the revision of the Directive launched by the Commission on 1 July 2009).[8] The Commission seems to have moved on as well and announced in November 2010[9] that it will indeed revise and clarify the applicability rule. In this paper an attempt is made to provide a uniform interpretation of the applicability rule based on the legislative history of the Data Protection Directive and (read in conjunction with my previous publication) the suggestion is made that a 'true' country of origin principle for data protection be introduced.

Outline

The key provision for the applicability of the EU data protection laws is Article 4(1)(a) of the Directive. In the second main section of this paper looks closely at Article 4(1)(a), starting with an explanation of the meaning of this provision based on the legislative history of the Directive before reviewing each of the key concepts of this provision. There then follows a summary comparison of the various national implementation laws and in the next two sub-sections I discuss some deviating opinions on the interpretation

4 Article 4(1)(a) Directive.

5 Article 29 Working Party, 'Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)' (WP 128, 22 November 2006) ('SWIFT Opinion').

6 The WP 29 was designated as an advisory body to the European Commission under Article 29 of the Directive, among other things to promote a clear interpretation of the Directive. Although the WP 29 has no more than an advisory function, the chairmen of the national supervisory authorities of all EU Member States are its members, and the recommendations of the WP 29 are, in practice, closely followed by the national supervisory authorities.

7 See Commission of the European Communities, First report on the implementation of the Data Protection Directive (95/46/EC), 15 March 2003, COM/2003/265 final, at 17 ('First Report on the Directive').

8 See Article 29 Working Party, 'The Future of Privacy, Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data' (WP 168, 1 December 2009), at paras 26–28. ('WP The Future of Privacy'). The advice of the WP 29 to revise and clarify the applicability rule has already been adopted by the European Commission. See European Commission, 'Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, A comprehensive approach on personal data protection in the European Union', COM(2010) 609/3 (4 November 2010), at paras 2.2.1.and 2.2.3 ('EC Communication on the revised Directive').

9 See European Commission, 'Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, A comprehensive approach on personal data protection in the European Union' COM(2010) 609/3 (4 November 2010), at paras 2.2.1.and 2.2.3 ('EC Communication on the revised Directive').

of Article 4(1)(a) including the WP 29 Opinion on Non-EU Based Websites.[10] To understand the scope of this provision, knowledge is also required of Article 4(1)(c) of the Directive, which is discussed in the next sub-section. In the third main section I discuss a number of international cases to illustrate the differences in interpretation and this is followed by a section considering the SWIFT Opinion, which concerns the situation where the processing of personal data takes place by an establishment in a Member State that acts as a processor for a controller in a third country. My conclusions are presented in the final section.

Article 4(1)(a) of the Directive

Article 4(1)(a) of the Directive contains the key provision for the application of EU data protection law:

1. Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:

(a) 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.

The legislative history

The country of origin principle

In order to understand the legislative history of the Directive knowledge of the so-called 'country of origin principle' is required. Around the time the Directive was adopted, the European legislators introduced the country of origin principle for various areas of law, most notably for cross-border television broadcasting services[11] and for e-commerce services.[12] According to the country of origin principle, the Member States each apply their own law to the services provided by service providers established on their territory (ie these services are governed by the law of their 'country of origin'). The other Member States must allow these services and may not apply further regulations.[13] This prevents the cumulative application of the different national laws to cross-border services within the EU. Application of the country of origin principle is considered justified in a European context if a certain area of law has been extensively harmonized within the EU.[14] Given the purpose of the Data Protection Directive (full harmonization of data protection law within the EU),[15] introduction of the country of origin principle for data protection law as well would have been the obvious choice. We will see that this was indeed the original proposal of the European legislator, but that this principle was abandoned in the final Directive.

'Being established' v 'having an establishment'

To understand the legislative history, it is of particular relevance to recognize that application of the country of origin principle results in a sole place of establishment of the service provider in respect of the service involved. If a provider of e-commerce services has more than one place of business in the EU (ie more than one establishment), such provider is considered 'established' for purposes of application of the country of origin principle in the Member State where the service provider has its centre of activities for that particular service (ie has its primary establishment).[16] The same applies to broadcasting services.[17] The European Court of Justice (ECJ) has developed a body of case law

10 Article 29 Working Party, '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, 30 May 2002), at 6 ('Opinion on Non-EU Based Websites').

11 Directive 89/552/EEC of the European Parliament and of the Council of 3 October 1989 on the coordination of certain provisions laid down by law, regulation, or administrative action in Member States concerning the provision of audiovisual media services [1989] OJ L 298/ 23 ('Television without Frontiers Directive') as recently amended by Directive 2007/65/EC of the European Parliament and of the Council of 11 December 2007 (renaming the Television without Frontiers Directive as the 'Audiovisual Media Services Directive'). The implementation date of the Audiovisual Media Services Directive expired on 19 December 2009.

12 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 [2000] OJ L 178/1 ('E-commerce Directive'). See EML Moerel, 'The country of origin principle in the E-commerce Directive: the expected "one stop shop"?', [2001] CTLR, at 184.

13 See Article 2 and 2a and Recitals 10–14 Television without Frontiers Directive (n 11) and Article 3 and Recital 5 E-commerce Directive (n 12).

14 Note however that the E-commerce Directive itself harmonized no more than five selected topics and this also in a very limited way. This means that Member States are forced to allow certain information society services which comply with the applicable rules in the country-of-origin, even though those rules have not been harmonized.

15 See Recital 8 of the Data Protection Directive (n 2), indicating that the purpose of the Directive was full harmonization with the exception of specific discretionary powers in a limited number of areas. See also Case C-101/01 *Bodil Lindqvist* [2003] ECR I-12971, paras 95–96.

16 See Recital 13 of the E-commerce Directive (n 12).

17 Article 2(3) Television without Frontiers Directive (n 11) provides a set of factors to determine which of multiple establishments involved in a certain broadcasting service should be considered to have 'effective

to apply these criteria.[18] Relevant here is that the concept of 'being established' for purposes of the country of origin principle (which refers to the primary establishment for purposes of the country of origin principle) is a different concept from the concept of 'having an establishment' (which is the basis for the applicability rule of the Directive). The latter concept includes the primary establishment but especially refers to secondary establishments like subsidiaries, branches, and agencies.[19] We will see that as a consequence the applicability rule of the Directive may lead to more than one applicable law. The concept of 'having an establishment' has been extensively discussed in my previous publication.[20]

The various stages of the legislative history

The Directive has had two draft versions, namely the Original Proposal,[21] and the Amended Proposal[22] (published together with an Explanatory Memorandum of the Commission).[23]

The three versions (ie the two draft versions and the final version) of the Directive show substantial differences especially as regards Article 4(1)(a) and the corresponding Recitals. The European legislators changed the connecting factor for the applicable law in each of the consecutive drafts, as a result of which the legal commentaries on Article 4 deviate according to the version of Article 4(1)(a) they relate to. Also the Explanatory Memorandum is often cited for explanatory purposes of the final Directive, while this Memorandum relates to the Amended Proposal, which adopted a different connecting factor than that used in the Final Directive.

The Original Proposal: incorporating the country of origin principle

Article 4(1) of the Original Proposal read as follows:

1. Each Member State shall apply this Directive to:

(a) all files located in its territory;

(b) the controller of a file resident in its territory who uses from its territory a file located in a third country whose law does not provide an adequate level of protection, unless such use is only sporadic.

In the Initial Proposal the connecting factor for choosing the applicable national law was the location of the data file (ie based on territorial jurisdiction). In order to avoid circumvention of the applicability of EU data protection law, a transfer of the data file to a non-member country was not supposed to prevent the protection of EU privacy laws attaching to the data. This provision was also supposed to prevent cumulation of applicable laws. The Member State where the data file was located had the obligation to ensure the data processing was in accordance with EU law; the other Member States could not exercise supervision as the protection was considered sufficient to permit the free flow of data. Those familiar with the Television without Frontiers Directive and the E-commerce Directive recognize this language, which is used by the European legislator to express the country of origin principle.

The Amended Proposal: still the country of origin principle

Article 4(1) Amended Proposal reads as follows:

1. Each Member State shall apply the national provisions adopted under this Directive to all processing of personal data:

(a) of which the controller *is established* in its territory or is within its jurisdiction;

(b) of which the controller is not established in the territory of the Community, where for the purpose of processing personal data he makes use of means, whether or not automatic, which are located in the territory of that Member State.

control' over the relevant service (ie should be considered the 'primary establishment' for purposes of application of the country of origin principle).

18 See for an overview of the case law Oliver Castendyk, Egbert Dommering and Alexander Scheuer, *European Media Law* (Kluwer Law International, Alphen aan den Rijn 2008) 847–66.

19 Pursuant to Article 43 EC Treaty (currently Article 49 TFEU), companies have the 'freedom of establishment' in the EU. This entails the right to set up and establish a primary establishment and the right to set up and manage secondary establishments such as subsidiaries, branches, and agencies. The freedom of establishment entails that nationals of a Member State may also set up and manage secondary establishments on behalf of companies that have their primary establishment in another Member State. Most case law of the ECJ in respect of Article 43 EC Treaty relates to the latter issue.

20 Moerel (n 1) at para. IV.2. See further the section entitled 'National implementations below.

21 Proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data, COM (1990) 314—2, 1990/0287/COD ('Initial Proposal').

22 Amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data ('Amended Proposal'), COM (92) 422 final—SYN 287, 15 October 1992.

23 This Explanatory Memorandum is not available anymore on the website of the European Commission. It can be retrieved from the Archive of European Integration of the University of Pittsburgh at <http://aei.pitt.edu/10375> last accessed 6 January 2011.

Relevant here is that the phrase in italics 'is established' concerns the primary establishment and is still in line with the country of origin principle. In the Explanatory Memorandum[24] of the Amended Proposal, the Commission gives the purposes of Article 4(1)(a) as follows:

> [the intention of Article 4(1)(a) is] to avoid two possibilities:
>
> – that the data subject might find himself outside any system of protection, and particularly that the law might be circumvented in order to achieve this;
> – that the same processing operation might be governed by the laws of more than one country.

Thus, the Commission considered the location of the data file no longer to be an adequate rationale, and the new connecting factor became the place of establishment of the controller.

The Explanatory Memorandum further shows that it was still the intention of the European legislator to introduce the country of origin principle for the EU data protection laws:[25]

> Under the Directive the protection provided is to follow the same lines in all Member States, and will thus be equivalent throughout the Community; and paragraph 2 accordingly prevents Member States from restricting the free flow of data in the fields covered by the Directive on grounds relating to the protection of data subjects.

The final version: cumulation of applicable laws

Article 4(1)(a) of the final version of the Directive reads as follows:

1. Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:
   (b) 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.

The changes in the final Directive compared with the Amended Proposal could not be more drastic. The country of origin principle apparently was not politically viable and was abandoned, and the Member States were each allowed to apply their own law (therefore making possible the cumulation of applicable laws). The drafters also detected a further gap in protection, since the controller itself could relocate outside the EU and thus avoid the applicability of the EU data protection laws. As a consequence the wording of Article 4(1)(a) and the corresponding Recitals was changed drastically.

To cover the possible circumvention of the EU laws by relocating the corporate seat of the controller, the connecting factor in Article 4(1)(a) first sentence was changed from the Member State where the 'controller is established' (ie the primary establishment) into 'establishment of the controller in a Member State' (so that the presence of a secondary establishment would be sufficient for the law to apply). Furthermore, the processing has to take place in 'the context of the activities of such establishment', in order to cover the possibility of a circumvention of EU data protection laws by relocating the processing itself to a country outside the EU. Finally, a second sentence was added to Article 4(1)(a) to express the cumulation principle.

Theoretically, the first sentence of Article 4(1)(a) of the Directive leaves open the possibility that the controller must be located in the territory of a Member State.[26] However, if that indeed had been the intention of the European legislator, the provision would simply have stated that the law of the Member State where the controller is established shall apply (as the provision read in the Amended Proposal). In any event, the second sentence of Article 4(1)(a) shows unequivocally that the intention was that the law of the Member State where the establishment is located applies. The second sentence states that a controller with more than one establishment in the EU must ensure that the establishments concerned comply with the national law applicable (pursuant to the first sentence). In other words, each of these establishments must comply with the obligations laid down in the national law of the Member State in which such establishment is located. This does not entail that the controller itself must be established in the territory of the relevant Member

24 Explanatory Memorandum (n 23), at 13.

25 Ibid., at 9.

26 The Dutch DPA bases its interpretation that the Dutch Data Protection Act only applies if the controller is established in the Netherlands on an isolated reading of this first sentence of Article 4(1)(a) of the Data Protection Directive. This sentence is then interpreted as referring to 'an establishment on the territory of the member state of the controller' (in other words, the establishment must be located on the territory of the Member State where the controller is established). This interpretation is untenable in the light of the second sentence.

States (just that its establishment is established there). This interpretation is confirmed by Recital 19 of the Directive, which states:

> whereas, when a single controller is established on the territory of several Member States, particularly by means of subsidiaries, he must ensure, in order to avoid any circumvention of national rules, that each of the establishments fulfils the obligations imposed by the national law applicable to its activities.

This leads to the conclusion that, in the final version of the Directive, the country of origin principle is abandoned,[27] and the laws of more Member States may apply to a processing of data (cumulation of applicable laws). The relevant connecting factor is whether a processing activity 'takes place in the context of the activities of an establishment of a controller in a Member State'. The controller itself no longer needs to be established in a Member State, nor is it required that the processing itself takes place with a Member State.

This interpretation is also the prevailing opinion in legal commentary[28] and is further confirmed by the leading commentary on the Directive of Dammann and Simitis (see the next sub-section), by the First Implementation Report on the Directive (discussed in the subsequent sub-section7), and recently also by the WP 29 in its Opinion on Search Engines (discussed thereafter in the following sub-section). There are also, however, a number of authors and DPAs who hold a different view. Most notably, the Dutch DPA[29] has recently published an article defending the position that Article 4(1)(a) provides that the connecting factor for the applicability is the place of establishment of the parent company of the controller and further-more contains a conflict rule indicating only one applicable law. The counter-arguments brought forward by these authors and the Dutch DPA are discussed in the footnotes and further the sub-section entitled 'Divergent opinions'.

Commentary Dammann and Simitis

The commentary of Dammann and Simitis[30] confirms the interpretation taken in this publication (translations by the author):

> The directive does not take into account the 'person involved' (his domicile or nationality), but the controller of the processing and then not the place of establishment of the parent company of the controller, but the place of establishment of an establishment of the controller in the context of which the processing activities take place. The directive herewith creates a decentralization which to a large extent results in the territoriality principle, ie what is decisive is the place of the processing. As a rule this has the result that also the persons involved can rely on their own well-known law for maintaining their own rights.

Dammann and Simitis are of the opinion that the second sentence of Article 4(1)(a) provides for an independent obligation on the part of the controller who has establishments in other Member States to ensure that these establishments indeed do comply with their own national data protection laws:[31]

> If a controller of a data processing [activity] has one or more establishments in another Member State, the Directive also applies to these establishments; the Member State in which she [the controller] is established should oblige her to 'take the necessary measures to ensure that each of these establishments complies with the requirements imposed on such establishment by applicable national law' (sub 1(a), second sentence). This provision extends further than the title of Article 4 'applicable law', it also imposes material obligations. This material obligation can be enforced against the controller by the supervising authority on the basis of Article 28(3), whereby on the basis of the territorially limited authority of the supervisory authorities, which is not changed by Article 4, cooperation between the supervisory authorities of other Member States are required pursuant to Article 28(6).

27 See Peter P Swire, 'Of Elephants, Mice, and Privacy: International Choice of Law and the Internet' (1998) 32 International Lawyer 991, 1007. Swire notes that under an interpretation whereby the Directive would apply only one applicable law to an act of data processing (based on stressing the singular in the term 'national law applicable' in Article 4(1)(a) Directive), the Directive would require a substantial new jurisprudence on how to select that unique law in the huge range of circumstances to which the Directive applies. He takes this as an indication that this interpretation was not the intention of the legislators.

28 See Christopher Kuner, *European Data Protection Law: Corporate Compliance and Regulation* (2nd edn Oxford University Press, Oxford 2007) 117–18; Lokke Moerel (n 1), at 81; MBJ Thijssen, 'Grensoverschrijdend gegevensbeschermingsrecht' (Cross-border data protection law) (2005) Privacy & Informatie 110; PH Blok, 'Privacybescherming in alle staten' (Privacy protection; a problem everywhere) (2005) Computerrecht 299 and 300; the commentaries on Article 4(1) of JMA Berkvens in *Wet bescherming persoonsgegevens; Leidraad voor de praktijk*, supplement 3 (Kluwer, Alphen aan den Rijn 2002); H de Vries in *T&C Telecommunicatierecht* (Kluwer, Alphen aan den Rijn 2009) 559–60; G-J Zwenne and Ch Erents, 'Reikwijdte Wbp; enige opmerkingen over de uitleg van art. 4, eerste lid, Wbp' (2009) Privacy & Informatie 60.

29 This publication is written on behalf of the Dutch DPA by its international coordinator MAH Fonteijn-Bijnsdorp, 'Art. 4 Wbp revisited': enkele opmerkingen inzake de toepasselijkheid van de Wet bescherming persoonsgegevens' (2008) Computerrecht 287–291.

30 Ulrich Dammann and Spiros Simitis, *EG-Datenschutzrichtlinie* (Nomos Verlagsgesellschaft, Baden Baden 1997) 127–8.

31 Insofar as I can see, this obligation has not been implemented in any of the data protection laws of the Member States.

First Report on the implementation of the Directive

That the Directive does not incorporate a country of origin principle[32] but is based on the principle of cumulation of laws is also confirmed by the Commission in its First Report on the implementation of the Directive.[33] Based on a survey of the various national implementation provisions of Article 4(1)(a) (the 'Technical Analysis'),[34] the Commission concludes that Article 4 has not been uniformly implemented and that as a result conflicts of law arise that the Directive sought to avoid. In other words, due to a lack of harmonization in the EU, controllers have to comply with divergent national laws, leading to conflicts of law which would have been avoided if Article 4 were uniformly implemented throughout the EU. The Commission further indicates in the Report that it will not introduce a country of origin principle,[35] but will first ensure the correct implementation of Article 4 of the Directive:[36]

> As regards the country of origin rule, the Directive already allows for the organisation of processing under a single data controller, which means complying only with the data protection law of the controller's country of establishment. This of course does not apply where a company has chosen to exercise its right of establishment in more than one Member State.
>
> The Commission's priority is, however, to secure the correct implementation by the Member States of the existing provision . . .'

Where the Commission in the First Report gives a more or less correct reflection of the applicability rule of Article 4(1)(a), the applicability rule as presented in the Technical Analysis (stating that the first ground for applicability is the place of establishment of the controller) seems to be incorrect.[37]

Opinion on Search Engines

After some diverging opinions (which will be discussed below), the Working Party 29 recently found its voice in its Opinion on Search Engines.[38] Where the earlier opinions contained references to the country of origin principle,[39] these are abandoned and the Opinion on Search Engines confirms that the data protection laws also apply in the event the controller is established outside the EU, as long as such foreign controller has an establishment within the EU and the processing takes place 'in the context of the activities of such establishment':[40]

> Where the search engine service provider is a non EEA-based controller, there are two cases in which Community data protection law still applies. . . . When applied to a particular search engine whose headquarters are located outside of the EEA, the questions needs to be answered whether the processing of user data involves establishments on the territory of a Member State . . .
>
> It is the search engine service provider that is responsible for clarifying the degree of involvement of establishments in the territory of Member States when processing personal data. If a national establishment is involved in the processing of user data, Article 4(1)(a) of the Data Protection Directive applies.'

Review of the key concepts of Article 4(1)(a)

Given the complexity of the key concepts of the provision of Article 4(1)(a), it is necessary to review each of these concepts below.

Controller (and processor)

Article 2 of the Directive provides that the 'controller' is 'the natural or legal person, public authority, agency or any other body, which alone or jointly with others determines the purposes and means of the processing of personal data'. From the definition it follows that it is possible to have multiple controllers for the same processing (so called co-controllers).[41] A 'processor' is 'the natural or legal person or any other body which processes personal data on behalf of the controller'.

32 This is also confirmed by the fact that data protection laws are excluded from the scope of applicability of the E-Commerce Directive (n 12) (and therewith from applicability of the country of origin principle). See Article 1(5) E-commerce Directive.

33 See European Commission, First report on the implementation of the Data Protection Directive (95/46/EC), 15 March 2003, COM/2003/265 final ('First Report on the Directive'). Pursuant to Article 33 of the Directive, the Commission has to report at regular intervals on the implementation of the Directive and, if necessary, provide suitable proposals for amendment.

34 Analysis and impact study on the implementation of Directive EC 95/46 in Member States, attached to the First Report on the Directive ('Technical Analysis').

35 As part of the evaluation process several companies and organizations have proposed to also introduce the 'home country control principle' to privacy law. See, for instance, JHJ Terstegge, 'Home Country Control—Improving Privacy Compliance and Supervision', [2002] P&I at 257–9 ('Home Country Control').

36 See First Report on the Directive (n 33), at 17.

37 Technical Analysis (n 34) 6. On behalf of the Dutch DPA, Fonteijn-Bijnsdorp (n 29) 288, quotes this passage from the Technical Analysis and indicates that these are the words of the European Commission which support the interpretation that Article 4(1)(a) provides for the place of establishment of the controller as the main ground for applicability. However, such interpretation cannot be based on an isolated citation from an underlying fact finding report which was commissioned by the Commission from a third party.

38 Opinion 1/2008 on data protection issues related to search engines (WP 148 4 April 2008). ('Opinion on Search Engines').

39 See for quote the discussion of Opinion WP 29 on Non-EU Based Websites.

40 'Opinion 1/2008 on data protection issues related to search engines' (WP 148 of 4 April 2008) ('Opinion on Search Engines'). See also more recently 'Opinion 1/2010 on the concepts "controller" and "processor"' (WP 169 of 16 February 2010) 5 ('Opinion on concepts of controller and processor').

41 The concept of co-controllership is under dispute in France as the definition does not incorporate the wording 'alone or jointly with others'. See also Kuner (n 28) 70.

Although at first sight the Directive provides a clear distinction between controllers and processors, this distinction cannot be easily made in respect of many complex joint processing situations within multinational companies. In this publication I will sometimes refer to the common example of a complex joint processing activity which exists within many multinational companies. Most multinationals process their worldwide employee or customer data in central systems.[42] In most cases the central HR systems or Customer Relationship Management (CRM) systems are operated by the parent company which therefore processes such employee (or customer) data on behalf of its subsidiaries. At first sight this would qualify the parent as a data processor for each of its subsidiaries.

In practice, however, most of the time it is the parent company that determines centrally which software and other systems will be implemented to perform the central processing, which employees of which group companies have access to the central system, and—last but not least—which data are to be included and processed in the central system. The decision about which data are to be included and processed is often prompted by the need of the parent company itself for certain information or reports from these central databases for management information purposes. As a consequence, not only are employee data included that are strictly necessary for the performance of that employment agreement (for the payment of salaries, etc.), but also information for so-called worldwide 'succession planning', 'tracking of high potentials', participation in worldwide 'share option schemes', etc. Inclusion of these data is more in the interest of the parent company than in the interest of the individual subsidiaries. Furthermore, because of the structure of their organizations, hierarchically the managers of employees of foreign subsidiaries are often found at the parent company (or at other intermediate holding companies). Employees of the parent company then, for all these purposes, have access to the data of the (other) group companies in the central systems. In this case it is difficult to argue that the central processing by the parent company of the employee data of group companies takes place only on behalf of the subsidiaries. In most cases, the parent company will even be primarily responsible for the aggregate data processing in the central system, and the relevant group companies are only jointly responsible with the parent for that part of the central system that concerns their employee data. In such cases, one cannot but conclude that the parent qualifies as the controller for the central system as a whole, and the respective subsidiaries qualify as joint controllers for their respective parts of the central processing.[43]

Can a branch qualify as a controller?

Some DPAs[44] are of the opinion that a branch office can also qualify as a controller. The fact that a branch is not a separate legal entity is not a decisive factor in establishing whether there is a person in a particular place who is competent to determine the purposes of a particular processing. 'Control' for data protection purposes is a very different concept than control under corporate law.[45] In this view a branch could qualify as a controller in its own right.[46] How this should be reconciled with the legal obligations subsequently imposed on such controller (like notification) is unclear. Only formal (legal) persons can have rights and obligations. In the case of a branch this would be the parent entity (to avoid one natural person within the branch being personally accountable for the processing of its employer). Any claim could only result in legal liability if it were brought against the legal entity controlling (under corporate law) the controller (under data protection law). Thus legal certainty would be best served if only the formal (legal) person being responsible for the processing at hand could qualify as a controller. In Case II discussed below it is shown why this properly fits with the interpretation of Article 4(1)(a) Directive as advocated in this publication. In its recent Opinion on the concepts of controller and processor,[47] the WP 29 seems to confirm this by first indicating that for the purposes of defining the concept of controller, 'it is important

42 In this publication, a central system refers to an IT system that is implemented in one location and to which all group companies worldwide have access. This is a development of the last five to ten years. Before this the group companies each had their own systems that at best were linked to one another.

43 The WP 29 in its recent Opinion on concepts of controller and processor (n 41) does not discuss this common example.

44 For instance the Dutch DPA, see Fonteijn-Bijnsdorp (n 29) 289. This despite the fact that the legislative history of the Dutch Data Protection Act clearly indicates that a controller is the formal legal entity that is responsible for the processing in order for those involved to be aware against which (legal) person they may exercise their rights. See Explanatory Memorandum to the Act, 25 892, no. 3, 55

45 See also Kuner, (n 28), para. 2.23.

46 The Dutch DPA, for instance, applies this view to subsequently conclude that the relevant branch is established in the Netherlands and that therefore the Dutch data protection law applies.

47 See n 40, p. 15–16.

to stay as close as possible to the practice established both in the private and public sector by other areas of law' and that 'preference should be given to consider as controller the company . . . as such', so as 'to provide data subjects with a more stable and reliable reference entity for the exercise of their rights under the Directive'.

Establishment of the controller

There must be an 'establishment' of the controller. This concept has been extensively discussed previously.[48] In short, an establishment is considered to be 'the effective and real exercise of activity through stable arrangements' whereby the 'the legal form of such an establishment, whether simply a branch or a subsidiary with a legal personality, is not the determining factor in this respect'.[49]

Establishment of the controller on the territory of a Member State

There must be an 'establishment of the controller in the territory of a Member State'. This element does not require further discussion. It has just been shown that a review of the legislative history of the Directive yields the interpretation that the national data protection laws already apply if an establishment of the controller is established in a Member State. For this purpose, the controller itself need not be established in a Member State.

In the context of the activities of an establishment

The national data protection laws only apply when the data processing takes place 'in the context of the activities of an establishment'. The Directive does not say that the data processing must be carried out by the establishment in a Member State. On the contrary, the European legislators meant to abstract from the location where the data processing takes place. If location were be decisive, this would easily facilitate by-passing national laws, for instance by relocating the servers to another jurisdiction.[50] It is, therefore, very possible for data processing to take place in the context of the activities of an establishment in a Member State, but that the data processing itself to be carried out by a third party outside this Member State (whether in another EU Member State or outside the EU). This underlines the long-arm reach of the Directive.

In today's context this has become a matter of course. For instance, a foreign parent company often processes data centrally for its EU group companies. If that processing takes place in the context of the activities of these EU companies (for instance, the foreign parent company has a central HR system which also processes the employee data of its EU group companies), the EU data protection laws will apply to those parts of the central processing which relate to the respective employees of the EU subsidiaries.

In its recent Opinion on Search Engines, the WP 29 has given some guidance when processing activities by a US search engine can be considered 'to be carried out in the context of the activities of its establishment in the EU':

> However, a further requirement is that the processing operation is carried out 'in the context of the activities' of the establishment. This means that the establishment should also play a relevant role in the particular processing operation. This is clearly the case, if:
>
> – an establishment is responsible for relations with users of the search engine in a particular jurisdiction;
> – a search engine provider establishes an office in a Member State (EEA) that is involved in the selling of targeted advertisements to the inhabitants of that state;
> – the establishment of a search engine provider complies with court orders and/or law enforcement requests by the competent authorities of a Member State with regard to user data.'[51]

National implementations

The laws implementing the Directive in the Member States are (more or less) based on the principle that the law of that Member State already applies if a foreign controller has an establishment in the relevant Member State.[52] Careful reading of them shows, however, many deviations concerning key concepts of Article 4(1)(a).

48 Moerel (n 1), at para. IV.2.

49 Recital 19 to the Directive.

50 Recital 18 of the Directive (n 2). This is also the position of the WP 29, see for instance Opinion on Non-EU Based Websites (n 10) 6, fn 17.

51 Opinion on Search Engines (n 38) 10.

52 All texts of the laws referred to are unofficial English translations, to be found at <www.mofoprivacy.com> last accessed 6 January 2011. That a different interpretation of Article 4(1)(a) leads to a very different interpretation of the various national implementation laws is shown by a recent research study commissioned by the Commission: Douwe Korff, New Challenges to Data Protection Study—Working Paper No. 2: Data Protection Laws in the EU: The Difficulties in Meeting the Challenges Posed by Global Social and Technical Developments (15 January 2010). European Commission DG Justice, Freedom and Security Report. Available at SSRN: <http://ssrn.com/abstract=1638949> 27–9, last accessed 6 January 2011.

The German implementation[53] applies for instance also 'to a data controller not located in an EU Member State or in another EEA Contracting State that collects, processes, or uses personal data in Germany'. The UK implementation[54] applies to data processed by a data controller who is established in the United Kingdom and the data are processed in the context of that establishment. The law defines those established in the United Kingdom as 'any person who maintains in the United Kingdom an office, branch or agency through which he carries on any activity'. The Irish[55] and French[56] implementations are more or less similar to that of the UK.

The Dutch Data Protection Act implements the first sentence of Article 4(1)(a) and demonstrates the same ambiguity.[57] The legislative history of Article 4(1) of the Dutch Act, however, makes clear that the Dutch legislators follow the European legislators, and the Act already applies if an establishment of a controller is established in the Netherlands.[58] The Belgian and Portuguese laws are similar to the Dutch provision (and therefore require study of the legislative history to determine whether their legislators have followed the European legislators or not).[59] The Italian provision applies 'where a processing is performed by any entity established . . . in the State's territory' and thereby applies both to controllers and establishments of foreign controllers in its territory.[60] The Spanish implementation provision provides that Spanish law applies 'when the processing is carried out as part of the activities of an establishment pertaining to the data controller, whenever the establishment is in Spanish territory'.[61] This seems to imply that the controller itself can be established in another country. However, the provision provides that the law also applies if this subsection is not applicable, but the data processor is located in Spain.[62] This seems to imply that the first provision only applies if the controller itself is established on Spanish territory. Clearly deviating from all other implementation provisions are those of Sweden, Norway, and Finland, which provide that their implementation laws apply only if the data controller is established on their territory.[63] These provisions seem an incorrect implementation of the applicability rule of the Directive. Apparently, however, these countries take a broad view of when a company may be considered to be 'established on their territory'. For instance in Finland, a company may already be considered established on its territory if a non-EU controller transmits advertising into Finland.[64] Also Finnish data protection law may therefore apply to a non-EU controller, an end-result which is more similar to a correct implementation and application of Article 4(1)(a), than expected at face value of the Finnish implementation provision. Greek data protection law expands the scope of the Directive's rule, by providing that Greek law also applies to data controllers outside the EU who process personal data of persons on Greek Territory,[65] and the data protection law of Denmark, which provides that Danish law applies to data processing carried out on behalf of a controller established in Denmark if the collection of data takes place for the purpose of processing in a third country.[66]

Opinion WP 29 on Non-EU Based Websites

It is also important to consider the WP 29 Opinion on Non-EU Based Websites,[67] which predates the Opinion on Search Engines and deviates substantially from it. The Opinion on Non-EU Based Websites has confused many DPAs and authors alike and some of its reasoning has found its way into other official documents of the European Commission.[68] The Opinion has also been quoted in a publication by the Dutch DPA in support of its interpretation that Article 4(1)(a) leads to the application of the law of one of the Member States only rather than to a cumulation of applicable laws.[69]

53 Sec 1(5) of the Bundesdatengeschutzgezetz.

54 Sec 5(1) and (3) of the UK Data Protection Act 1998.

55 Sec 3B sub (a) and (b) of the Irish Data Protection Acts 1988 and 2003.

56 Article 5(I)(1°) of Loi n° 78–17 du 6 janvier 1987 relative à l'informat aux fichiers et aux libertés.

57 Article 4(1) Wet Bescherming Persoonsgegevens.

58 See n 28 for an overview of Dutch literature confirming this. See further n 29 for contrary opinions.

59 Article 3bis of Loi relative à la protection de la vie privée à l'egard des traitement de données à caractère personnel and Article 3 sub (a), (b) and (c) of the Lei 67/ 98 da Protecção de Dados Pessoais.

60 Section 5 sub (1) and (2) Codice in materia di protezione dei dati personali.

61 Article 3(1)(a) of the Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/ 1999, de 13 de diciembre, de protección de datos de carácter personal.

62 Ibid.

63 Section 4 of the Swedish Personal Data Act 1998 (Personuppgiftslag (1998: 204); Section 4 of the Norwegian Personal Data Act (LOV 2000–04–14 nr 31: Lov om behandling av personopplysninger); and Section 4 of the Finnish Personal Data Act (523/1999) (Henkilötietolaki 22.4.1999/523).

64 Kuner (n 28) 84, mentions an unpublished case where McDonald's was found to be 'established' in Finland based on advertising that was transmitted into the country from abroad via cable television. This is not in conformity with the Directive.

65 See Article 3(3)(b) of the Greek Data Protection Act.

66 See Article 4(1) Danish Data Protection Act.

67 Opinion on Non-EU Based Websites (n 10).

68 Most notably the Commission's First Report on the Directive (n 33) para. 4.4.1 and Korff (n 52) 21–2 (dating after WP Opinion on Search Engines).

69 Fonteijn-Bijnsdorp (n 29) 168.

The confusion starts where the WP 29 attempts to reconcile the possibility for the cumulative application of multiple laws under the Directive with the country of origin principle. In short, according to the WP 29, the country of origin principle has been introduced into data protection legislation, so that if the controller is established in the territory of the EU, the law of the establishment of the controller applies. If the controller chooses to 'establish' itself in more than one Member State (ie has establishments in other Member States) it will have to comply with the law of all those (other) Member States in which it is 'established'. From this point of view the Directive does not contain an exception to the country of origin principle, but merely constitutes a strict application of it. The explanation the WP 29 gives is, however, an incorrect interpretation of the country of origin principle as the European legislator usually has in mind. Both the Television without Frontiers Directive and the E-Commerce Directive make clear that if a service provider has more than one place of business in the EU, such service provider is considered to be 'established' for purposes of application of the country of origin principle in the Member State where the provider of e-commerce services has its centre of activities or the media service provider is considered to have effective control. Application of the country of origin principle therefore results in no more than one place of establishment for the service involved, whereas with respect to data protection legislation each and every one place of establishment (even if it is no more than a branch office) qualifies as a place of establishment. Below is included an example for the purposes of clarification:

E-commerce Directive

A Dutch parent company provides a website for the online sale of products throughout the EU, also for its EU subsidiaries. The centre of activities regarding the provision of the online services is in the Netherlands. In line with the country of origin principle the website is governed solely by Dutch law.

Data Protection Directive

A Dutch parent company processes the company's employee data in a central HR system located in the Netherlands, and also for its EU subsidiaries. The centre of activities regarding the provision of services by the parent company is in the Netherlands. However, the law of the establishments (the EU group companies) governs that part of the central database that concerns the employee data of the relevant subsidiary. As a result, there is a host of applicable laws.

See the Opinion on Non-EU Based Websites for this creative turn regarding the application of the national data protection laws:[70]

> As the directive addresses the issue of applicable law and establishes a criterion for determining the law on substance that should provide the solution to a case, the directive itself fulfils the role of so-called 'rule of conflict' and no recourse to other existing criteria of international private law is necessary.
>
> In order to find an answer, the directive uses the criterion or <connection factor> of the '*place of establishment of the controller*" or, in other words, the country of origin principle typically applied in the Internal Market. This means concretely:
>
> When the processing is carried out in the context of the activities of an establishment of the controller on the territory of one Member State, the protection law of this Member State applies to the processing.
>
> When the same controller is established on the territory of several Member States, each of the establishments must comply with the obligations laid down by the respective law of each of the Member States for the processing carried out by them in the course of their activities. It is not an exception to the country of origin principle. It is merely its strict application: where the controller chooses not to have only one, but several establishments, he does not benefit from the advantage that complying with one law is enough for his activities throughout the whole Internal Market. This controller then faces the parallel application of the respective national laws to the respective establishments.

Another problematic aspect of the reasoning of the WP 29 is that the starting point that the controller 'has spread out over more than one establishment' appears to imply that each of the controller's establishments itself would be a controller (this would be in line with the country of origin principle). The point is, however, that these establishments very often do not qualify as a controller while the data processing takes place 'within the context of the activities of that establishment' (for a number of cases see below). The application principle of the Directive (that the data processing must take place in the context of the activities of the establishment) entails that the law of the country of the establishment (and not therefore of the controller) applies. This cannot be reconciled with the country of origin principle, which would lead to applicability of the law of the country of establishment of the controller.

70 Opinion on Non-EU Based Websites (n 10), at 6.

Divergent opinions

Some commentators interpret Article 4(1)(a) as leading to the applicability of the law of the Member State where the controller is established.[71] Some quote in support of this interpretation the Explanatory Memorandum of the Commission[72] (see above), where the Commission gives as the second rationale for the applicability rule of Article 4(1)(a) 'to avoid that one and the same data processing would be governed by the law of more than one country'. As noted above, this Memorandum was published in respect of the Amended Proposal, therefore at the time the country of origin principle was still contained in the proposed Directive, a point these commentators have overlooked.[73] It is further striking that the Dutch DPA in a recent publication (dating after the WP Opinion on Search Engines) still defends the position that Dutch data protection law only applies if the controller is established in the Netherlands.[74] The main arguments of the Dutch DPA are discussed in the footnotes.[75]

Article 4(1)(c) Directive

To fully understand the scope of applicability of the Directive, knowledge of Article 4(1)(c) is required.[76] In short, this provision underlines the long-arm approach of the Directive[77] by providing that a national data protection law also applies in the event that the:

> controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated in the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.

The European legislator wished to ensure that even in the event the controller has no establishment in the EU at all, EU data protection laws will nevertheless apply if the actual data processing takes place in a Member State by means of use of the equipment. Relevant here is that some DPAs[78] apply Article 4(1)(c) despite the fact that the controller does have an establishment within the EU. They consider the branch or subsidiary to (also) qualify as 'equipment'. In its recent Opinion on Search Engines,[79] the WP 29 explicitly indicated that in those cases Article 4(1)(a) takes precedence over Article 4(1)(c).[80]

Cases

Because the above may be somewhat abstract, several cases will now be discussed involving an international situation (with a foreign controller and establishment in the EU), in order to clarify what results the established difference in interpretation of Articles 4(1)(a) and (c) of the Directive may lead to. In some cases, the different interpretations lead to the same outcome via different routes. In other instances the outcomes are diametrically opposed. Each time I will apply the rule of Article 4(1)(a) as advocated in this article (Opinion 1) and then the deviating opinion as, for instance, advocated by the Dutch DPA
(Opinion 2)

71 See Lee A Bygrave, 'Determining Applicable Law Pursuant to European Data Protection Legislation', <http://folk.uio.no/lee/oldpage/articles/Applicable_law.pdf> 8 (under reference to the concept of establishment under the E-Commerce Directive (n 12) and the Television without Frontiers Directive (n 11)) last accessed 6 January 2011; Jeroen Terstegge's comment on article 4(1) Directive in *Concise European IT Law* (Kluwer Law International, Alphen aan den Rijn 2004) 39–41 (which is diametrically opposed to the interpretation of article 4(1) given in his earlier publication 'Home Country Control' (n 35) 257–9); Bing, 'Data protection, jurisdiction and the choice of law' [1999] 65 Privacy Law and Policy Reporter 5–7 (referring to the concept of establishment under the E-Commerce Directive (n 12) and the Television without Frontiers Directive (n 11)); Fonteijn-Bijnsdorp (n 29) 288; T Hooghiemstra and S Nouwt, *Tekst en Toelichting Wet Bescherming Persoonsgegevens* (Text and explanation Personal Data Protection Act) (SDU 2007), Explanation to Article 4, at 61: 'The key point of the Dutch Personal Data Protection Act is the place of establishment of the controller'; JEJ Prins and JMA Berkvens, *Privacyregulering in theorie en praktijk* (Privacy regulation in theory and practice), (Series Recht en Praktijk, part 75) (Kluwer, Alphen aan den Rijn 2007) 101: 'The consequence of the above is that, as to the question which body of law applies, the place of establishment of the controller of the processing is considered essential'; Korff (n 52) 21–2.

72 Explanatory Memorandum (n 23) 13.

73 See Bygrave (n 71) 7–8. Bygrave gives as an explanation for the second rationale that at the time the Directive was drafted, it was the assumption and hope of the drafters of the Directive that the national privacy laws would be in harmony, as a result of which the applicability of more EU national laws would not be a problem, and only now is it apparent that the considerable margin that Member States have been given in implementing the Directive has lead to substantial disharmony. Despite this comment, however, he still takes as the main rule the application of the law of the Member State where the controller is established; Bing (n 71) 9. Korff (n 52) 21–2, this still under reference to WP Opinion on Non-EU Based Websites (n 10) 6, while at that time the WP Opinion on Search Engines (n 38) was already issued.

74 Fonteijn-Bijnsdorp (n 29).

75 See n 44, n 71, n 26 and n 94.

76 See Moerel (n 1).

77 See also Recital 20 of the Directive (n 2).

78 In particular the French and Dutch DPA. See Fonteijn-Bijnsdorp (n 29) 291, note 28.

79 See Opinion on Search Engines (n 38) 11: 'a Member State cannot apply its national law to a search engine established in the EEA, in another jurisdiction, even if the search engine makes use of equipment. In such cases, the national law of the Member State in which the search engine is established applies.'

80 See in a different context also Kuner (n 28) 122: 'a corporate subsidiary should not be considered to be "equipment" of the non-EU company'. He considers this might be different if the subsidiary is a branch office only. The latter does not seem correct.

Case I: US parent with a branch in the Netherlands

A US parent company has a branch office in the Netherlands. The Dutch branch processes the data of persons employed at the branch. Who is the controller, the US parent or the Dutch branch? As explained in above, the term 'controller' refers to the person who in a formal-legal sense controls the processing as a result of which those involved are aware of the legal persons against which they may exercise their rights. As the Dutch branch is not incorporated, it therefore cannot qualify as a controller. The US parent has control over the data processing in a formal-legal sense and therefore qualifies as the controller. Does Dutch data protection law apply?

Opinion 1

The processing of data of Dutch employees is carried out 'in the context of the activities of the Dutch establishment'. As the controller, the US parent must comply with the obligations laid down in Dutch data protection law.

Opinion 2

Dutch data protection law does not apply: Article 4(1)(a) Directive does not apply because the controller (the US parent) is not established in the Netherlands. Article 4(1)(c) and also does not apply because the US controller does have an establishment in the Netherlands (in Section 2.6 we saw that this provision only applies if a controller outside the EU has no establishment in one of the Member States).

In order to fill this 'gap', some DPAs sometimes apply the fiction that the US parent is 'established' in the Netherlands as a controller because it has an establishment in the Netherlands.[81] Other creative solutions are that the branch itself is considered the controller and as this branch is established in the Netherlands, so that Dutch data protection law applies.[82] In the section above on the controller (and processor) we saw that this is not a correct interpretation. Some DPAs also just apply Article 4(1)(c), considering the branch 'equipment' in the Member State.[83] In the section entitled 'Article 4(1)(c) of the Directive' above we saw that this also is not a correct interpretation. These creative turns are unnecessary if the criterion of Article 4(1)(a) of the Directive is applied in line with the Directive.

81 In some Member States this fiction is even implemented in their data protection law (see for instance UK, Irish, and French law, discussed in the section entitled 'National implementations').

Case II: the US central database

A US parent company has a subsidiary (a separate legal entity) in the Netherlands. The US parent has a central database located in the US that processes both employee and customer data of the Dutch subsidiary. The US parent processes more data than necessary for the purposes of the Dutch establishment and also determines the means used to process the data. The US parent qualifies as a joint controller in respect of the Dutch employee and customer data in the central system.

Opinion 1

The US parent processes the Dutch employee and customer data also 'within the context of the activities of its Dutch establishment'. The Dutch data protection law applies to this part of the processing. Both controllers (the US parent and the Dutch establishment) must comply with the obligations under Dutch data protection law.

Opinion 2

Dutch data protection law will also apply. The Dutch subsidiary is viewed as a joint controller with regard to the Dutch employee and customer data processed in the central database. Because one of the joint controllers (the Dutch subsidiary) is established in the Netherlands, the Dutch subsidiary must comply with the obligations laid down in Dutch data protection law with respect to that part of the database which concerns the Dutch employees and customers.

The main difference here is that in the second opinion the US parent falls outside the ambit of Dutch data protection law. The creative turn possible in Case I (the US parent is 'established' in the Netherlands because it has a branch office in the Netherlands) does not work here because the subsidiary is a separate legal entity. If the interpretation in line with the Directive is followed, the US parent would also be governed directly by Dutch data protection law. In view of the fact that the processing is undertaken by the US parent in the USA (as a result of which the Dutch subsidiary does not have actual control over the processing), the first interpretation is to be preferred from an enforcement perspective.

82 See Fonteijn-Bijnsdorp (n 29) 289.

83 Ibid., at 291 (note 28).

Case III: the US share option plan

A US parent company introduces a company-wide share option plan. Under this plan, the US parent grants share options to a very select group of employees of its worldwide subsidiaries, including its Dutch subsidiary. For this purpose the US parent processes certain assessment data of the employees and further the data necessary to grant (and later exercise) the share options. The controller for the processing is the US parent. The US parent determines the means and the purpose of the processing. The subsidiaries in question have no power of decision in the matter whatsoever. Their role is limited to providing certain data to the US parent.

Opinion 1

Insofar as the US parent processes data of Dutch employees in the context of the share option plan, these data are also 'processed in the context of the activities of the Dutch establishment', as the remuneration of the Dutch employees in respect of their work for the Dutch establishment is involved. Dutch data protection law is applicable to the processing of these employee data by the US parent (ie the US parent is directly subject to Dutch data protection law).

Opinion 2

Dutch Data Protection law is not applicable because the controller is not established in the Netherlands.[84] Because the controller does have an establishment in the Netherlands, Article 4(1)(c) is also not applicable. As a consequence the transfer requirements also do not apply. This result does not appear desirable from the perspective of the Directive to protect individuals. Possibly, DPAs will resolve this by using a broad definition of 'controller', by qualifying the Dutch subsidiary to be a joint controller insofar as the data of Dutch employees are processed in the context of this share option plan. This creative turn is unnecessary if the interpretation in accordance with the Directive is used. Furthermore, when an interpretation in accordance with the Directive is used, the US parent is directly subject to Dutch Data Protection law. If the interpretation of some DPAs is used, only the Dutch subsidiary is subject to Dutch Data Protection law. The first interpretation is therefore to be preferred from an enforcement perspective.

84 Incidentally, in the past the former Dutch Data Protection Commissioner (at present the EU Data Protection Supervisor) Mr Peter Hustinx, repeatedly indicated that the Dutch Personal Data Protection Act is certainly applicable to the processing of data of employees in the context of international share option plans.

Case IV: US parent institutes worldwide whistleblower hotline

A US parent opens a call centre located in the USA for employees of all its companies to file complaints. The US parent is obliged to do so under the US Sarbanes–Oxley legislation. Is Dutch data protection law applicable to the personal data processed in the context of complaints by or about employees of its Dutch subsidiary? The US parent is the controller of this data processing (it determines the purpose and means of the processing).

Opinion 1

The whistleblower line also has an independent purpose for the Dutch establishment (the Dutch subsidiary independently benefits from the complaints procedure, such whistleblower facility being required under Dutch corporate governance requirements).[85] The data concerning complaints relating to the Dutch subsidiary are thus also processed in the context of the activities of the Dutch establishment. The US parent is directly subject to Dutch data protection law insofar as personal data of Dutch employees are processed.

Opinion 2

Dutch data protection law should not be applicable, since the controller is established outside of the Netherlands. Because the controller does have an establishment in the Netherlands, Article 4(1)(c) of the Directive is also not applicable.[86] Dutch data protection law is therefore not applicable to the transfer of the data by the Dutch employees to the US parent. Again, the DPAs may possibly resolve this by using a broad definition of controller by qualifying the Dutch subsidiary as a joint controller insofar as complaints are submitted by or about Dutch employees. In case of a correct interpretation this is unnecessary and moreover the US parent company would be directly subject to Dutch data protection law, instead of (only) the Dutch establishment (which has no control over the processing whatsoever).

Case V: US call centre for product support

A US parent offers call centre services, offering customers of its worldwide subsidiaries an opportunity to submit questions about products brought onto the

85 Dutch Corporate Governance Code, to be found at <http://www.commissiecorporategovernance.nl/Corporate_Governance_Code> last accessed 6 January 2011.

86 The French DPA applies (the French equivalent of) Article 4(1)(c) in this context, with the argument that the telephones (the means) are located in France.

market by those subsidiaries. The Dutch establishment has access to the information of the US call centre, insofar as complaints of Dutch customers are involved. The information is necessary for the Dutch establishment for purposes of repairs or replacement of returned products. The US parent is the controller for the processing of the data that takes place in the context of the call centre (it determines the purpose and means).

Opinion 1

The data are processed by the US parent also in the context of the activities of the Dutch establishment (which is responsible for repairs and replacements). This involves support by telephone for the products that would otherwise have been provided by the Dutch establishment itself. Since the data are necessary for activities of the Dutch establishment, it must be concluded that the data are also processed in the context of the activities of this establishment. The US parent is directly subject to Dutch data protection law.

Opinion 2

Dutch data protection law will not apply to the processing of the data of Dutch customers because the controller is not established in the Netherlands. Because the controller does have an establishment in the Netherlands, Article 4(1)(c) of the Directive is also not applicable. Again the DPAs may possibly resolve this by using a broad definition of controller or by qualifying the Dutch subsidiary as a joint controller insofar as support is requested by Dutch customers. In cases of interpretation in accordance with the Directive, this is unnecessary and moreover the US parent company would be directly subject to Dutch data protection law.

A question that comes up is: what if the call centre data are not available in the Dutch establishment? Should the conclusion therefore be that these data are not processed 'also in the context of the Dutch establishment'?[87] The answer is: it depends. Possibly the handling of complaints has been organized in such a way that it is not necessary to provide the Dutch establishment with these data, whereas the complaints-handling is still to such an extent linked to the products brought onto the market by the Dutch establishment that processing should indeed be deemed to take place in the context of the Dutch activities. According to the criteria formulated by the WP 29 in its Opinion on Search Engines, the answer could be 'yes', if the Dutch establishment would be 'responsible for the relations with the Dutch customers' and is 'involved in the targeted advertisement for the relevant service in its jurisdiction'. This is without doubt a grey area. In my view, however, such processing should be seen as a separate activity. The support activity is then apparently an activity that can be performed by an independent third party.[88] In that case processing does not take place 'also in the context of the activities of the Dutch establishment'.

The SWIFT Opinion

How does all of the foregoing relate to the SWIFT Opinion? In the SWIFT Opinion, the WP 29 concluded that the headquarters of the Society for Worldwide Interbank Financial Telecommunication (SWIFT) is established in Belgium and qualifies as the controller in respect of all processing activities of SWIFT in the EU (including the data processing in SWIFT's messages operating centre located in the Netherlands and its sales offices in various other Member States).[89] The WP 29 subsequently applied Belgian law to all processing activities on behalf of SWIFT anywhere in the EU, including data processing in the Dutch operating centre and in its sales offices in various other Member States. This amounts *de facto* to application of the country of origin principle (also applying the law of the controller to the data processing which takes place in the context of the activities of a branch in another Member State). Rumour has it that the Opinion was taken on a far from unanimous basis.[90]

Background to the SWIFT Opinion

SWIFT supplies messaging services for financial transactions between financial institutions (processing more than twelve million messages on a daily basis). The information processed by SWIFT concerns messages on the financial transactions of hundreds of thousands EU

87 In the affirmative Blok (n 28) 299.

88 An example of this is the maintenance of washing machines. There are enough parties in the market that offer maintenance for all brands. If such a third party processes data of Dutch customers with a Miele washing machine, this processing does not take place 'partly in the context of the activities of the Dutch Miele distributor'. The services in question are fully independent. In my view the same should apply if another company belonging to the Miele group carries out this maintenance.

89 SWIFT Opinion (n 5).

90 See for the earlier opinion of the Belgium DPA: Advice No. 37/2007 of the Belgian DPA dated 27 September 2006, at <www.privacycommission.be> last accessed 6 January 2011. See for the position of the Dutch DPA for example: 'Verslag van het onderzoek naar gegevensverstrekking door banken aan de Amerikaanse autoriteiten', bijlage bij 'Onderzoek naar directe gegevensverstrekking aan de VS en antwoorden op kamervragen inzake SWIFT', nader rapport 27–06-2007', at <www.rijksoverheid.nl> last accessed 6 January 2011.

citizens that contain without question their personal data. SWIFT is established in Belgium. SWIFT Belgium makes use of an operating centre in the Netherlands, where all data transmissions are processed. This operating centre is a branch office of SWIFT Belgium as are the various sales offices. The WP 29 considers SWIFT Belgium as the controller for the data processing by all branches because the critical decisions regarding this processing are taken by SWIFT Belgium. The WP 29 subsequently declared Belgian law applicable to all processing in the EU:[91]

> The head office of SWIFT is located in La Hulpe, Belgium. SWIFT also has two operating centers (one in Europe and one in the US, which is a complete mirror). In addition, SWIFT has several sales offices in the UK, France, Germany, Italy, Spain, etc. The critical decisions on the processing of personal data and transfer of data to the US were decided by the head office in Belgium. As a consequence, the processing of personal data by SWIFT is subject to Belgian law, implementing the Directive, regardless of where the data processing takes place.

The WP 29 does not assess in any way whether the processing of personal data by the Dutch operating centre takes place (also) in the context of the activities of (i) the sales offices or (ii) the operating centre itself. For instance the Dutch operating centre has as its only purpose the processing of the millions of messages, which constitutes the primary business activity of SWIFT. The WP 29 therefore, in fact, simply applies the country of origin principle here (applicable is the law of the controller). As explained above, this seems untenable as a starting position. The European legislators explicitly rejected introduction of the country of origin principle under EU data protection law.

The establishment acts as processor for a foreign controller

In the SWIFT case, the Dutch operating centre acted as a processor on behalf of the controller SWIFT Belgium. Some DPAs take the position that in the event an establishment on their territory acts as a processor for a controller in another Member State, the law of the controller applies to the processing ('processor follows controller'). Support for this view is found by some DPAs in the Technical Analysis attached to the European Commission's report on the Data Protection Directive:[92]

> None of the laws explicitly specify that they do *not* apply to processing on their territory if the processing takes place in the context of the activities of an establishment of a controller in another Member State, or to processing by a controller who has its main office on their territory but when processing takes place in the context of an establishment of that controller in another Member State.

If this quote is read properly, I do not think that the Commission[93] intended to say that if an establishment acts as a processor for a controller in another Member State, the law of the controller is always exclusively applicable. The quote uses the concept of 'processing in the context of the activities of a controller in another Member State'. This cannot simply be considered equivalent to being a 'processor'. If the Commission had intended for processors to be always subject to the law of the controller, it would simply have provided that if a processing is carried out in the capacity as processor, the processing will be governed by the law of the state where the controller is established. The second sentence in the quote shows this unambiguously by allowing the explicit possibility that a controller in a Member State processes data in the context of an establishment of this controller in another Member State in which case the law of that establishment applies. It is, therefore, not invariably the law of the controller that is applicable. My conclusion is that the applicability of national data protection legislation does not follow the distinction controller/processor, but is subject to another test, namely whether data are (also) 'processed in the context of the activities of an establishment on the territory of a Member State' (in which case the data protection law of that Member State is applicable). As set out above, the WP 29 gave some guidelines when data processing should be considered to be 'processed

91 See SWIFT Opinion (n 5) para. 2.2. See further para. 6.3: 'Actions regarding SWIFT: For all its data processing activities, SWIFT as a controller must take the necessary measures to comply with its obligations under Belgium data protection law implementing the Directive'. In para 2.3 the WP 29 further qualifies the financial institutions to be controllers in their own right insofar as 'their' message data is concerned. This also entails application of the laws of the financial institutions to their respective message data. See para 2.3: 'This means that, in the case of financial institutions, different—though harmonized—laws are applicable. The WP 29 stresses that, since personal data are being processed in financial transactions regarding hundreds of thousands of citizens via institutions established in the EU (the cooperative SWIFT as well as financial institutions making use of the SWIFTNet FIN services), the national laws on data protection—adopted in implementation of the Directive—of the different Member States concerned are applicable.'

92 Technical Analysis (n 34) 6. See Fonteijn-Bijnsdorp (n 29) 289; Bygrave (n 71) 7, indicates that the language of Article 4(1)(a) seems by contrast to imply that the law of a Member State does not apply to a processor established on its territory if the controller were established in another Member State.

93 Note that the Technical Analysis is not drafted by the European Commission itself, see n 37.

in the context of the activities of an establishment'.[94] Specific guidance of the WP 29 on when processor activities should be considered to be performed in the context of the activities of the processor itself would obviously be welcomed.

The above distinction becomes obsolete if one were to assume (apparently like the WP 29 in the SWIFT Opinion) that if a processing is performed by a processor, then it is always to be considered as having been performed exclusively in the context of the activities of the controller (thus sidelining the data protection law of the Member State of the processor). However, this position seems erroneous, since it would lead to legal gaps being created in the protection of personal data, a result that the WP 29 would not have welcomed had it given this more consideration (see the sections below on three undesirable reults). How these legal gaps are dealt with by a proper application of the provision of Article 4(1)(a) is discussed in the final sub-section before the concluding section.

Undesirable result (1)

Application of the rule that a national data protection law is not applicable if the establishment processes data as a processor creates a lacuna in the protection of personal data if the controller is established outside the EU. This is illustrated by the SWIFT case itself. If SWIFT were to move its Belgian headquarters to a country outside the EU, the controller would no longer be established within the EU and it would no longer be the case that Belgian data protection law would also not apply to all other establishments of SWIFT in the EU (which apparently all qualify as data processors for the SWIFT headquarters). Also Article 4(1)(c) of the Directive would not help; we saw above that this provision only applies if the controller outside the EU has no establishment in one of the Member States. The Dutch processing centre of SWIFT, however, without doubt qualifies as an 'establishment' in the EU as a result of which Article 4(1)(c) of the Directive does not apply.

The above gap in legal protection arises because the WP 29 (lacking an official country of origin principle that applies to the EU only) attempts to achieve the same result by attributing the processing by a processor to the controller of such processing. The result of this is that this rule also applies if the controller is established outside the EU, which cannot have been the intention of the EU legislators. In all other cases where the country of origin principle has been implemented, this only has an effect within the EU. Providers established outside the EU cannot profit from this rule, and will need to comply with the laws of all Member States involved.

Undesirable result (2)

The position of the WP 29 in the SWIFT Opinion leads to another loophole in the protection of personal data: if a processor is never subject to its own law, the mandatory processor provisions of its own data protection law would also not apply.[95] For compliance purposes it will then be required to solely rely on the mandatory processor agreements made between the controller and the processor.[96] If a controller outside the EU has a processor in the EU there would not even be an obligation to enter into such mandatory processor agreement (ie if SWIFT were to move its headquarters outside the EU, its EU processing centre would therefore not be bound by any material processor obligations either). Although the DPA of the processor in theory would have formal enforcement powers,[97] there would be no material obligations to supervise. This gap does not arise if the advocated interpretation is followed.

94 The Dutch DPA bases the rule 'processor follows controller' on Recital 18 of the Directive, especially the second sentence. This was however not the purpose of Recital. As is the case with its predecessors (Recital 10 Original Proposal and Recital 12 Amended Proposal), Recital 18 expresses the first rationale for the Directive (avoiding potential circumvention of the protection) and not (as the Dutch DPA assumes) the second rationale (avoidance of cumulative application of laws). Also the second sentence of Recital 18 should be read in the context of avoiding circumvention of the protection (as evidenced by the introduction of this sentence 'whereas, in this connection'). The second sentence intends to express that the Directive cannot be circumvented by involving a processor outside the EU. The Recital makes clear that in that case the law of the Member State of the controller applies.

95 Various EU data protection implementation laws contain mandatory processor obligations. Examples are the Irish Data Protection Act (see for instance Articles 2, 7, and 21); the Dutch Data Protection Act, under which processors are directly liable for any damages resulting from their processing activities (see Article 49(3); and the Greek Data Protection Act which applies to controllers and processors alike (see Article 3(3)).

96 It is striking that for the processing provisions the European legislators have opted for the 'country of origin' principle. Pursuant to Article 17(3) Directive, the controller is to impose on the processor the security obligations of Article 17(1) of the Directive, as defined by the legislation of the Member State where the processor is established. This is to prevent a processor having to comply with the processor provisions of different Member States (which in practice differ substantially) especially as regards to the required security measures. This is justified if the starting point is that the processor is indeed subject to the data processor requirements of its own law as supervised by its national DPA.

97 Pursuant to Article 28(6) Directive, the DPA of the processor has jurisdiction over data processing occurring on its territory 'whatever the national law applicable to the processing in question'.

Undesirable result (3)

With its interpretation the WP 29 apparently intends to avoid the cumulative application of the national data protection laws applicable to any processing.[98] However, application of the rule that a national data protection law is only applicable if the controller is established in the relevant Member State does not solve the problem of cumulative application of applicable rules at all. Examples were provided above which deal with a central system operated by a parent on behalf of its subsidiaries (as a data processor for these subsidiaries). We saw that the data in these central systems will as a rule be processed also in the context of the activities of the parent's own establishment. If the parent company of such a multinational is established in the EU, the data protection law of the EU country where the parent is established should apply to the processing at large (in addition to the laws of the subsidiaries for their relevant parts of the processing). In this case nothing is therefore achieved in practice by ruling that 'processors' follow 'controllers'.

However, even if one were to assume that a parent who operates the central HR system does so solely on behalf of its EU subsidiaries (ie as a processor), such central system is subject to a great many EU data protection laws (as many as there are EU subsidiaries). As each of the subsidiaries is the controller in respect of the processing of its own employee data, the various parts of the central HR system are consequently subject to as many EU data protection laws. As a result, each EU subsidiary, for example, has to notify the database (for its own part) to the DPA in its own country.

Multinationals therefore do not benefit in any way from the above interpretation by the WP 29. This explanation will at best entail that the Dutch parent (if it is considered a mere processor for its subsidiaries) does not have to notify the central database in its entirety in its own country, but only for the part that concerns its own employees. Simplification only occurs if the parent is to be considered as the sole controller for such central database and only needs to notify the database (in respect of the whole of the EU) in its country of establishment. This will only be achieved if the country of origin principle is introduced. This is by far preferable from a supervisory perspective. Article 28(6) of the Directive provides that a DPA has supervisory jurisdiction over processing occurring on its respective territory, which applies irrespective of the national law applicable to the processing in question. The Directive therefore contemplated that DPAs would under certain circumstances be required to apply foreign laws. How is a DPA going to supervise a central system on its territory if such DPA will have to apply the data protection laws of a host of different Member States (which differ on numerous points) to the dispute in question?[99] In short: the WP 29 should not seek to effect the non-applicability of a national data protection law if a parent company processes data on behalf of its subsidiaries centrally. On the contrary, in these cases the DPAs benefit from the possibility of central supervision over this 'processor' while applying their own national law to the conflict.

Further thought has to be given to whether the introduction of a country of origin principle should also apply to the rights of data subjects, or that data subjects would keep their rights under their national law. However, under present legal rules, the rights of data subjects may in some cases be governed by the law of another Member State if the processing takes place in the context of activities of an establishment of a controller in another Member State. Full harmonization of the rights of data subjects and cooperation between the DPAs in the event of complaints may be a better solution than excluding the rights of data subjects from applicability of the country of origin principle altogether.

SWIFT revisited

We just saw that if we follow the rule of the WP 29 (processor follows controller), and SWIFT were to relocate its Belgian headquarters to a country outside the EU, the controller would no longer be established within the EU and Belgium data protection law would no longer apply. This legal gap does not exist if the test advocated in this article is applied. If SWIFT's headquarters were in the USA, the test would be: are the data (also) 'processed in the context of the activities of an establishment of SWIFT US on the territory of a Member State'. The Dutch processing centre as well as the sales offices each qualify as an establishment. Looking at the guidance provided by the WP 29 for criteria when processing activities by a non-EEA controller can be considered to be carried out in the context of activities of establishments in the EU, the following criteria seem relevant:[100]

- The sales offices of SWIFT are responsible for relations with the customers of SWIFT (the financial institutions) in the relevant Member States (with corresponding EU citizens as their end-customers).

98 Fonteijn-Bijnsdorp (n 29) 288–9.

99 See also Kuner (n 28) 112.

100 I do not know the exact details of the activities of the SWIFT branches, so this is an educated guess.

- In most cases this will involve some local activities in the Member States (local sales people, local relationship management, local brochures about the services, etc.).
- I assume that the Dutch processing centre actively complies with court orders and/or law enforcement requests by the competent authorities of a Member State with regard to financial transaction data of EU citizens.
- The processing of financial transaction data is not a by-product, but a primary business process of SWIFT (ie the services of SWIFT are facilitating these transactions). The Dutch processing centre therefore conducts a primary business process which involves many employees. The processing of the data therefore takes place in the context of the activities of the Dutch branch.

The conclusion is that insofar as data are processed in the context of the activities of a sales office (data of the customers in certain Member States), the data protection law of such a sales office is applicable. As the data are also processed in the context of the Dutch establishment, Dutch law also applies to the processing as a whole. This seems fully justified (even desirable), since the data processed concern sensitive data of millions of EU citizens.

Application of this test also leads to a good result in case, for instance, a US parent sets up an EU subsidiary just for data processing purposes, but has no (other) activities in the EU. In that case the data will not be processed in the context of the activities of the establishment of the parent in the EU and EU data protection law will not apply.[101]

To conclude

At the moment there are a number of Member States that have not properly implemented the applicability rule of the Directive. Also the WP 29 uses in the SWIFT opinion an interpretation of the applicability rule which seems contrary to the legislative history of the Directive. This interpretation does not solve the problem of cumulative application of national EU data protection laws but rather creates gaps in the protection of personal data. A proper implementation and interpretation of the applicability rule does not give rise to these problems. Although the attempt of some DPAs and the WP 29 to prevent the cumulative application of legislation is commendable, this result will only be achieved if the country of origin principle is introduced. This should be done by the European legislators and not via the short-cut of opinions of the WP 29. In view of the current confusion, it would be welcomed if the WP 29 explicitly lays down its position regarding Cases I–V in an opinion and in that context in particular clarifies how the concept of 'controller' and the concept 'carried out in the context of the activities of an establishment' should be applied to the cases at hand.[102] Further, given the present differences in the implementation of the Directive's rules in the Member States, it would be welcome if the Commission were to take as its first priority ensuring that Article 4 of the Directive is correctly implemented in all Member States.

doi:10.1093/idpl/ipq009
Advance Access Publication 24 January 2011

101 If my proposal for review of Article 4(1)(c) is followed, EU data protection law would also not apply if the US parent involves a third party processor. See Moerel (n 1), para. V.

102 The WP 29 announced such opinion in WP The Future of Privacy (n 8) para. 28.