

Mrs M.A.H. Fontein-Bijnsdorp, international officer at the Dutch Data Protection Authority (Dutch DPA) [College bescherming persoonsgegevens (CBP)]

“Article 4 WBP revisited”: Some comments regarding the applicability of the Wet bescherming persoonsgegevens (WBP) [Dutch Data Protection Act]

The Wet bescherming persoonsgegevens (WBP) [Dutch Data Protection Act] provides rules concerning the scope of the Act. These rules are contained in Article 4(1) of this Act, which reads:

"This Act applies to the processing of personal data carried out in the context of the activities of an establishment of a responsible party in the Netherlands."

E.M.L. Moerel asserts in *Computerrecht* 2008, 81¹ [*Computer Law*] that - in view of the wording of the Act - a fundamental discussion of the question when the WBP applies is possible. Moerel formulates the main line of the Dutch DPA's interpretation of the rules concerning the applicable law as follows: *"The Dutch DPA applies the WBP if the controller with respect to the processing of personal data is established in the Netherlands. If the controller is established in a different country, the Dutch DPA does not apply the WBP to the processing of personal data in the Netherlands by a Dutch branch of this foreign controller"*.² Moerel asserts that this application of the rules is not in line with the European Privacy Directive³ (hereinafter referred to as: the Directive), and that it leads to the possibility of gaps occurring in legal protection and does not prevent the problem of cumulation of legislation. Moerel provides an alternative interpretation: *"It is crystal clear that the Privacy Directive intends for national legislation to apply even if only a branch of a controller is established in the Netherlands. The controller itself need not be established in the Netherlands for this purpose"*.⁴

Moerel's call for a fundamental discussion of the applicability of the WBP must be seen in the light of the wording of the relevant provisions in both the Directive and the Act. The wording of the Act leaves room for different interpretations. In such cases, the interpretation that is most in line with the legislator's intention as evidenced by the legislative history and the methodology of the Act must serve as the basis. Notwithstanding the fact that the final word in that respect is ultimately up to the courts, the Dutch DPA considers it of great importance to learn the insights and experiences from the (legal) practice and to be able to include them in

¹ Ms E.M.L. Moerel, 'Back to basics: wanneer is de Wet bescherming persoonsgegevens van toepassing?', *Computerrecht* 2008, 81.

² Op cit. 1 p. 81.

³ Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 regarding the protection of natural persons in connection with the processing of personal data and regarding the freedom of movement of those data, *OJ L* 281/31.

⁴ Op cit. 1 p. 81 (and almost identically p. 82). In Moerel's application, the mere presence of an establishment (of the controller) in the context of whose activities personal data are processed is sufficient for the application of the WBP. These activities may also be performed elsewhere and/or by other parties, as long as they are performed "within the context" of a Dutch establishment. "In the context of" is interpreted broadly here, in any case as "for the benefit of" (p.85) the own establishment, but can apparently also be interpreted as "pertaining to". What party in which capacity processes data, on whose behalf or in whose name, who has the authority to make decisions on the processing etc. is, according to Moerel, not relevant.

the determination of the interpretation that is most in line with the legislator's intention, and to exercise maximum transparency in doing so.

It is against this background that the Dutch DPA took note with interest of Moerel's article. It must be stated first and foremost that the developments in the implementation or in legal practice, as the case may be, could give cause to adjust the supervisory authority's policy. The response below provides a substantiated explanation of the opinion that there are currently insufficient grounds for doing so. The implementation practice of the Dutch DPA will be placed in the context of the legislator's intention and the methodology of the Directive and national legislation. The legislator has attached great value to the determination of the role that the parties play in a specific processing of personal data. This has, as will be explained below, consequences for the interpretation of the provisions concerning the scope of the Act. Finally, a short reflection will be provided on the consequences of this interpretation and the interpretation propagated by Moerel for the legal protection of citizens, the internal markets and the burden on the controllers. The main focus of this article will be on the applicability rules within the European Union (EU). The processing of personal data by controllers in third countries and the disclosure of personal data to third countries outside the EU will only be dealt with peripherally.

Objective of the Directive

The objective of the Directive is two-fold. On the one hand, the Directive is intended to make the internal market possible by removing obstructions to the free movement of personal data within the EU. On the other hand, the Directive is intended to create a high and equal level of protection for citizens.⁵ In other words, the free movement of personal data within the EU and legal protection are central. These two objectives are interrelated and neither one is more important than the other: the free movement of personal data is made possible by the fact that the Directive creates an equal level of protection within the EU. The provisions concerning the applicable law need to be interpreted against this background.

Objective and main rule concerning the applicable law

In the determination of the applicable law of the Directive, the classic starting point, namely the place where data are held, has been abandoned. The object of the rules of the Directive is "data processing" that can no longer be attributed to a specific place. To the extent processing is still related to a file, the applicability of the legislation is no longer dependent on the place where this file is held. Instead, the starting point of the Directive and legislation is "the place where the controller is established".⁶ These regulations are more in line with the IT development whereby data are increasingly immaterial and therefore come to lack a determination of place. In that case, the classic rules for the determination of the applicable law no longer apply. So, the place where the data, or the file, are held is no longer the starting point for jurisdiction, but rather the place where the controller is established.⁷ In the words of the European Commission: "*the Directive requires Member States [...] to determine the controller's establishment as grounds for an application of the respective Member State's law*".⁸

⁵ See Article 1 of the Directive in conjunction with Recital 3 of the Directive.

⁶ *Parliamentary Papers II*, 1997-98, 25 892, no. 3. p. 75 (Explanatory Memorandum, EM).

⁷ *Idem*.

⁸ 'Analysis and impact study on the implementation of Directive EC 95/46 in Member States, technical analysis of the transposition in the Member States', belonging to the First Report on the Application of the Data Protection Directive (95/46/EC), COM(2003)265, 15 May 2003, p. 6.

In its first evaluation report on the Directive, the European Commission referred to the article on the applicable law as "one of the most important provisions of the Directive from the perspective of the internal market".⁹ In order to have the internal market operate properly, the regime of the applicable law is intended to prevent the cumulation of national legislation and the occurrence of gaps within the EU.¹⁰ After all, there is equality of personal data protection within the EU. Nor should there be unnecessary obstructions to the free movement of personal data within the EU, to the extent this does not harm the applicability of legal protection. The Directive contains its own 'rule of conflict' for this purpose.¹¹ This follows from Recital 18 and Article 4 of the Directive, which contain the main rule concerning the applicable law:

Recital 18 reads as follows¹²:

"Whereas, in order to ensure that individuals are not deprived of the protection to which they are entitled under this Directive, any processing of personal data in the Community must be carried out in accordance with the law of one of the Member States; whereas, in this connection, processing carried out under the responsibility of a controller who is established in a Member State should be governed by the law of that State".

The English text of the second part of Recital 18 is more clearly formulated: *"whereas, in this connection, processing carried out under the responsibility of a controller who is established in a Member State should be governed by the law of that State"*.

The first sentence of Article 4(1), at a of the Directive reads:

*"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"*¹³

Recital 18 and Article 4(1), at a of the Directive state, in other words, that the law of one of the Member States must apply to each processing of personal data within the EU. This is the law of the country where the controller is established. This prevents cumulation of legislation.¹⁴

Pursuant to Article (2) at d) of the Directive "'controller' shall mean the natural or legal person (...) which (...) determines the purposes and means of the processing of personal data". The answer to the question of who the controller is, should – on the one hand – be based on the formal-legal authority to determine the purposes and means of the processing of personal data, and on the other hand – and supplementary to it – on a functional meaning of the term. This also applies to group relationships. The controller is the legal person under whose

⁹ Eerste verslag over de toepassing van de Richtlijn gegevensbescherming (95/46/EG), COM(2003)265, 15 May 2003, p. 20.

¹⁰ See footnote 8, p. 6.

¹¹ See in this context also 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, WP56, 5035/01/EN/Final, 30 May 2002, p.6.

¹² This Recital is not quoted in Moerel's article.

¹³ The English text reads: 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.

¹⁴ Moerel does not deny this intention for that matter. In footnote 14 (p. 83) she asserts: "It is remarkable that the legislative history of establishment of the Privacy Directive shows that the European legislator intended Article 4 of the Privacy Directive to prevent a situation whereby the same processing of personal data would be governed by the law of various countries [...] This is, strictly speaking, correct". But Moerel does not interpret the Directive in this spirit.

authority the operational processing of personal data takes place. The line of reasoning is that the data subject in society can know against whom he may exercise his rights if so desired.¹⁵

As stated in the EM to the WBP as well, the text of Article 4 of the Directive shows that the term "establishment" is taken to mean in the Directive: one or more centres of economic activities, which may be located in several Member States of the European Union. Recital 19 of the Directive also shows that it is not relevant whether it concerns a branch office or a subsidiary with legal personality. The establishment in the territory of a Member State assumes the effective and actual performance of activities for an indefinite period. The legal form of such an establishment, irrespective of whether it concerns a branch office or a subsidiary with legal personality, is not decisive. In specific cases, it will have to be determined on the basis of the facts whether it concerns an establishment within the meaning of the Directive and therefore whether national law applies. Case law for the European Court of Justice in this respect can be found, inter alia, in case C/205/84, German insurances.¹⁶

The role of the establishments: who is responsible?

In the determination of the applicable law, it must consequently be first established who is responsible for the specific processing of personal data, and, subsequently, where the party responsible for the relevant processing of personal data is established.¹⁷ This main rule also applies if multiple parties are involved in the processing of personal data. In such cases, the role that parties play during the processing of personal data, and their mutual division of duties in respect thereof, must be assessed. In accordance with Recital 18 of the Directive, "responsibility" can in this context also be interpreted in the usual sense of "responsibility". The following questions are relevant in this context: Which establishment determines the purposes and means of the processing of personal data? Under whose responsibility does the operational processing of personal data take place? And to whom can the processing of personal data be attributed and who has power of disposal? Does an establishment, in this connection, to use the words of the working party of the European privacy supervisors, the Article 29 Working Party, play a "relevant role"?¹⁸ Or, who makes the "critical decisions on the processing of personal data"?¹⁹

This main rule also applies within group relationships. The further elaboration of the main rule of the applicable law, as formulated in Recital 19 and the second part of Article 4(1), at a of the Directive, must be interpreted in this light.²⁰

Recital 19 reads:

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

¹⁵ *Parliamentary Papers II*, 1997-98, 25 892, no. 3. p. 56 (EM).

¹⁶ *Idem*, p. 75.

¹⁷ The interpretation of the term "establishment" is not dealt with in this Article. When speaking of an "establishment", it is assumed that the criteria set in this respect by European law have been complied with.

¹⁸ Article 29 Working Party, Opinion on data protection issues related to search engines, WP148,00737/EN, 4 April 2008, p.10.

¹⁹ Article 29 Working Party, Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunications (SWIFT), WP128, 01935/06/EN, 22 November 2006, p. 9.

²⁰ An argument in favour of the view that the second sentence of Article 4(1), at a of the Directive, must be interpreted in light of the main rule contained in the first sentence of this provision, can also be found in the fact that the second sentence is not implemented separately in the Netherlands. Both elements of Article 4(1), at a of the Directive, are contained in Article 4(1) of the WBP.

rules, that each of the establishments fulfils the obligations imposed by the national law applicable to its activities.

The second sentence of Article 4(1), at a of the Directive reads:

When the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable.

It follows from Recital 19 and Article 4 of the Directive that the law of the place of establishment does not a priori apply to the processing of personal data performed by the subsidiaries. Reversely, it cannot be concluded from Recital 19 either, as reasoned by Moerel, that the law of the country where and establishment (of the controller) is established, applies to the processing of personal data within the context of that establishment. Each establishment of a company, including the subsidiary, will have to determine in respect of each processing of personal data in which it is involved which law applies²¹ to that processing of personal data by answering the questions who is responsible for the processing of personal data, and where this party is established. Recital 19 is, after all, a further specification of Recital 18. It follows from Recital 18 that it is not relevant for the determination of the applicable law at which party or establishment the processing of personal data – under the responsibility of the controller – takes place. The fact that activities are performed by an establishment other than the establishment of the controller is therefore not of influence on the determination of the applicable law. This means, in concrete terms, that it is possible that processing of personal data takes place within the context of an establishment of a company in the Netherlands to which the WBP does not apply. This line of reasoning is confirmed by the European Commission, which concludes that it is possible that the national laws of Member States "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 the processing takes place in the context of an establishment of that controller in another Member State".²²

And finally, the legal form of the relevant establishment is not decisive either for the determination of the applicable law. A Dutch branch office without legal personality of an American parent company will, in all likelihood, comply with the "establishment" requirements, and will also fall within the organisation of the American company. This means that this branch office constitutes an establishment of that company in the Netherlands. In order to determine whether Dutch law applies to a specific processing of personal data within the context of the activities of the relevant establishment, the role played by this branch office in the processing of personal data, as set out above, must be determined. This must be assessed on the basis of the facts and circumstances of the relevant case. This constitutes a functional substantiation of the applicable law.²³

Consequences: legal protection and free movement of personal data

²¹ See also: Eerste verslag over de toepassing van de Richtlijn gegevensbescherming (95/46/EG), COM(2003)265, 15 May 2003, p. 20, and 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, WP56, 5035/01/EN/Final, 30 May 2002, p.6.

²² See footnote 8, p. 6.

²³ Moerel also uses this example in her article (op cit. 2, p. 86) and applies different assessment criteria in that respect.

The above approach, which, as regards the applicable law, is in line with the place of establishment of those organisation(s) that have decision-making powers in respect of the processing of personal data, serves both objectives of the Directive: legal protection of citizens and free movement of personal data.

Legal protection is not promoted by making as many European national privacy laws as possible applicable to the processing of personal data within and outside the EU. Legal protection is promoted by ensuring that the party responsible, as regards the processing of personal data concerning an individual, can be effectively challenged concerning its duties by this individual or by the supervisory authority. This interpretation also limits the cumulation of legislation to the fullest extent possible. This contributes to the proper operation of the internal market and prevents the unnecessary increase of the burden imposed on parties that wish to work or cooperate internationally. This interpretation limits the cumulation of legislation to those situations in which establishments from multiple countries are responsible for the processing of personal data. In those cases it is also, from the perspective of legal protection, justifiable that multiple national laws are applicable. After all, the legal protection of citizens is served if the law of the country of that establishment, in respect of which they can enforce their rights, applies. This can be illustrated on the basis of a few examples.

A Dutch establishment of a Luxembourg bank has, as its only duty, the production of overviews of bank transactions on the instruction of that Luxembourg bank. In Moerel's vision, Dutch law would apply to the production of the overviews, in addition to Luxembourg law, as well. Only Luxembourg law would apply in the line of reasoning followed by the Dutch DPA. On holiday, a Dutch citizen opens an account with a Luxembourg bank. The Dutch citizen subsequently wishes to dispute a bank transfer on the basis of an overview of his bank transactions. Aware of the bank's Dutch branch office, he reports there. What does Moerel's interpretation – that Dutch law applies to the processing of personal data of the Dutch branch office – mean, specifically, for the legal protection of this client? Nothing, because the Dutch branch office has no decision-making powers as regards the processing of personal data, irrespective of which law applies. The client will have to submit his complaint to the company in Luxembourg. Moreover, the client should expect that he has to do so because he, after all, opened the account in Luxembourg. The situation would be different if a Dutch branch office of the Luxembourg bank were to be opened in the Netherlands and the Dutch citizen were to open an account with this branch office. It is highly likely, in that case, that the WBP applies to the processing of personal data in relation to the bank transactions. From the perspective of legal protection, this would also be the most desirable option for a client who has an account in the Netherlands.

Another example is provided by Moerel's article.²⁴ The example is applied here in an EU context: An Italian parent company awards a select group of worldwide employees share options (a 'Share Option Plan'). For this purpose, the Dutch subsidiary is required to disclose personal data of its employees to the Italian parent, which subsequently uses these to assess whether shares will be awarded. According to the interpretation provided by the Dutch DPA, Italian law would apply exclusively to the processing of personal data by the Italian parent. How would this work in practice for an employee? According to the WBP, the Dutch employer is responsible for the processing of personal data of its employee. The employer is therefore obliged to provide the personal data to the Italian parent in accordance with Dutch law. If the employee is of the opinion that his personal data were provided in a manner that is

²⁴ See footnote 1, p. 86-87.

not in accordance with the law, he may challenge the Dutch employer under Dutch law. The Italian parent is subsequently obliged to process the personnel information in accordance with the law. It will not be allowed to process the personal data further in a manner that is incompatible with the objective for which they were received. If the employee has a complaint in this respect, he will have to enforce his rights with the Italian parent. In such cases, Italian law will be applied in the Dutch DPA's policy line. In Moerel's vision, both Italian and Dutch law could be applied. Dutch and Italian law provide an equal level of protection. Application of both privacy laws to the Italian controller will not lead to a significantly different outcome. Application of both laws therefore has no added value for the legal protection of the data subject. This approach does increase the burden on the company, and an unnecessary increase of the burden could constitute an obstruction to the free movement of personal data in the EU.

Even if the Dutch subsidiary were obliged to provide personal data to a parent company in a third country outside the EU, Moerel's interpretation would lead to an unsatisfactory outcome: In that case Dutch law would apply to the processing of personal data by the parent in the third country.²⁵ This interpretation leads, as regards the current application, to an expansion of the extra-territorial scope of European legislation outside of the European Union.²⁶ This constitutes an increase in the burden on the parties involved in this case as well. Moerel is of the opinion that there is a gap in the legal protection (outside of the EU) in the current application, which would be undesirable on the basis of the principle of protection contained in the WBP. She does not deal with the fact that the both the Directive and the WBP contain a system of rules for the disclosure of personal data outside the EU. This system is actually intended to provide for legal protection in those cases in which, as a result of disclosure of personal data outside of Europe, national legislation no longer applies and/or the personal data fall outside the jurisdiction of the European national supervisory authorities. Moreover, increasing the applicability of the WBP in third countries (by means of a broader interpretation) does not guarantee compliance, enforceability and effective legal protection. The desirability of such an expansion is questionable as well.²⁷

Could the option of the land of origin principle, i.e. applying the law of the European principal place of business of the company, propagated by Moerel, provide a solution? This could perhaps ease the burden for the controllers and facilitate the free movement of personal data, but has adverse consequences for the data subject from the perspective of legal protection. Someone who does business in the Netherlands with a Dutch branch office of a Luxembourg bank expects to do so subject to Dutch law. Applying the law of the country where the company has its principal place of business increases the lack of clarity and the complexity for the client and makes it more complicated for clients to enforce their rights. A

²⁵ This is in line with the example provided by Moerel herself, see op cit. footnote 1, p. 86-87.

²⁶ This is the case in all examples provided by Moerel.

²⁷ Another important aspect relating to third countries is the interpretation of Article 4(1), at c of the Directive, which has been incorporated in Article 4(2) of the WBP. This Article regulates jurisdiction if the controller is not established in the EU. Article 4, second paragraph of the WBP reads: *This Act applies to the processing of personal data by or for responsible parties who are not established in the European Union, whereby use is made of automated or non-automated means situated in the Netherlands [...]* Moerel argues that this "Article only applies if a controller does not have an establishment, apart from the EU, in one of the Member States" (op cit. footnote 1, p. 90). Partly on the basis of the interpretation of this provision, Moerel concludes that there are gaps in legal protection (outside the EU). The Dutch DPA applies a different interpretation of this Article, which, in its opinion, is in line with the methodology of the Act. This provision must be interpreted in light of Article 4(1), at a of the Directive and the Article 4, first paragraph of the WBP. This leads to the fact that the Dutch DPA – succinctly stated – already deems this provision applicable if, with regard to the specific processing of personal data, there is no establishment within the EU which is the controller..

Dutch employee of a Dutch subsidiary of a Finnish company will also invoke the Dutch rules on inspection, in connection with the inspection of his medical file at the occupational health and safety service, the more so as this is closely connected with Dutch legislation concerning sickness absence.

Summary and conclusion

The wording chosen by the legislator in the legislative texts on the applicable law leaves room for different interpretations. In such cases, the interpretation that is most in line with the legislator's intention, as evidenced by the legislative history and the methodology of the Act, must serve as the basis. The Dutch DPA attaches great value to the meaning of the principles that underlie the EU Privacy Directive; i.e. guaranteeing the legal protection of citizens and the free movement of goods. This leads the Dutch DPA to the interpretation in which a decisive meaning is attributed to the role that parties play in a specific processing of personal data. Which establishment is responsible for a specific processing of personal data is decisive. This constitutes a functional substantiation of the applicable law. The mere fact that an "establishment" of the controller exists in the Netherlands is not considered decisive in this context.

I have tried to illustrate in the above examples that this interpretation should be preferred from the perspective of the legal protection of citizens, the prevention of an unnecessary increase of the burden and, finally, the operation of the internal market. There is no reason for adjusting this line of reasoning as long as an alternative interpretation for the realisation of objectives described above does not provide demonstrable benefits.

This does not mean that the last word has been said about the most desirable regulation of the applicable law concerning privacy legislation. After all, the above comments only dealt with the interpretation within the methodology of current legislation. Both the WBP and the EU Directive will be evaluated in the coming years. That will provide an opportunity to also think outside the parameters currently provided by legislation, and to engage in a discussion of the most desirable legislation in the area of the regulation of the applicable law. Such an evaluation will also offer the opportunity to gain inspiration in other areas of law, such as European consumer law, European competition law or the law that applies to (the supervision of) financial institutions. The Dutch DPA looks forward to this discussion with great interest.