The scope of the Dutch Personal Data Protection Act: some remarks on the interpretation of Article 4(1) Dutch Personal Data Protection Act

Gerrit-Jan Zwenne and Chris Erents[1]

It is not always clear to which and when the Dutch Personal Data Protection Act applies. For example, there is still a lot of discussion about the territorial effect of the act. Or how Article 4(1) thereof must be interpreted and applied. Recently, it has turned out that the Dutch Data Protection Authority departs from a restricted interpretation – this in derogation of what seems to be assumed in general. In this contribution, we will explore this discussion in depth and place it in a wider context.

§1 Introduction: discussion on the territorial effect of the PDPA

In an article in the Dutch Law Review *Computerrecht* the discussion on the territorial effect of the Dutch Personal Data Protection Act (PDPA) was started in the middle of last year.[2] In an extensive argument, Moerel set out how article 4(1) of this act is interpreted by the Dutch Data Protection Authority (DPA), and how according to her it should be interpreted. The core of her argument is that the text of this provision leaves room for both a restricted and a broader interpretation. Subsequently, the author pointed out that the watchdog has opted for a restricted interpretation for reasons of its own, i.e.: an interpretation in which the act only applies if a controller is established in the Netherlands and therefore not if there is only an establishment of the controller in the Netherlands. This interpretation is incompatible with, as the author set out, the intention of the community legislator with the privacy directive.[3] And, as a result hereof, this interpretation gives

What did this contribution precede?

In the magazine Computerrecht, Moerel brings up for discussion the standpoint of the DPA on the applicability of the PDPA in international situations. The DPA would interpret article 4 PDPA in that way that the privacy act only applies if the controller is established in the Netherlands. If data are processed by an establishment in the Netherlands of a foreign controller, the PDPA would not apply according to the watchdog. According to Moerel, this restricted interpretation leads to confusion in the international business sector and to gaps in legal protection. (Computerrecht 2008/3, p. 81-91).

In a reaction, the DPA confirms that it indeed interprets article 4 PDPA in this restricted way. It indicates where its standpoint has been based upon and what its ground for this is. The watchdog thinks that with this interpretation the functioning of the internal market is guaranteed in the best possible way as a cumulation of national laws is prevented. The DPA derives some support for its standpoint from recital 18 from the preamble of the directive and the evaluation of the privacy directive 95/46. (Computerrecht 2008/6, p. 285-289).

Moerel reacts to this in a postscript. She sets out that the DPA chooses its sources for the substantiation of its standpoint in a selective way. In an extensive analysis she discusses the formation history of the article in question in the directive, and the sources cited by the DPA. She also discusses a recent opinion of the Article 29 data protection working party and some literature on the directive. Her unamended conclusion is that for the applicability of the PDPA it is not required that the controller itself is established in the Netherlands (Computerrecht 2008/6, p. 290-298).

rise to confusion in (mainly) the international business sector. She also asserts that the interpretation creates gaps in the personal data protection.

Subsequently, something surprising happened. In an extensive reaction to the argument of Moerel, DPA-employee Fontein-Bijnsdorp stated that the watchdog indeed departs from the abovementioned restricted interpretation of article 4(1) PDPA.[4] She also set out why the watchdog does this. This is remarkable for various reasons. First, as this interpretation seems to deviate from how it is seen by many other authors. Furthermore, as Fontein-Bijnsdorp does not avail herself, as is common, of the reservation that the text has been written 'in a personal capacity'. Pursuant to this, we might assume that it concerns an unorthodox communication of a policy view of the DPA – something that usually takes place through decisions and policy rules, either or not published in the Netherlands Government Gazette (*Staatscourant*).

In a postscript to this reaction of the DPA, Moerel gave an extensive further substantiation of her argument.[5] In it, she particularly refers to the formation history of the privacy directive and some documents of the so-called Article 29 data protection working party.

This discussion is apt for further analysis, and not only because it affects the foundations (or as Moerel says: the basics) of the act and the protection it offers. This discussion is also important because it deals with how far a watchdog can go in the interpretation of the act and which meaning should be attached to this. In our contribution, we place this discussion, for which we refer to the contributions in question in the abovementioned magazine, in a wider context and we will check how various stakeholders think about it. We will start with a brief explanation of article 4(1) PDPA and how this article is interpreted (§2). It is important for this that a distinction is made between the more factual question on the one hand: which interpretation did the community legislator actually intend, and on the other hand the more normative question: which interpretation promotes legal protection and the proper functioning of the internal market in the best way? Subsequently, we will discuss the question to what extent, in view of the interpretation that is given to the article, there is a problem with regard to the territorial effect of the act (§3). In some conclusive remarks (§4) we will finally give our view on this discussion so far.

§2 Article 4(1) PDPA

Multiple authors have said something about the interpretation and application of article 4(1) of the act. The majority of these authors seem (either or not implicit) to depart from an interpretation in which the act applies if there is an establishment in the Netherlands, and not necessarily if the controller himself is established in the Netherlands. Furthermore, also the DPA and the con-

sultative body of European privacy watchdogs, the Article 29 data protection working party, have expressed themselves on the territorial effect of the act, be it not always in a clear way.

We will go through all this and start with what the act and privacy directive themselves state.

2.1 What does the act state?

What does the act itself state on the territorial effect of the act? The text of the article in the act is not particularly clear:

> *"This act applies to the processing of personal data in the context of activities of an establishment of a controller in the Netherlands."*

The question that immediately arises is who or what must reside in the Netherlands in order to be able to determine that the act applies. Does the act apply if the activities take place in the Netherlands? Or if the controller is residing in the Netherlands? Or also if there is only an establishment in the Netherlands, without the controller himself being established here? If we confine ourselves to the text of the provision alone, all the abovementioned options seem possible.

This is not clarified in the parliamentary history of the act. On the contrary: in the explanatory memorandum, the following somewhat confusing (because ambiguous) remark is made:

> *"the application point of the PDPA is the place where the controller is established"*

The phrase 'the place where the controller is established' can be interpreted in two ways, i.e. in the sense that the act only applies if the responsible himself is established in the Netherlands (restricted interpretation), but also in the sense that the act applies if the controller has an establishment in the Netherlands (broader interpretation). In the last case, the phrase quoted must be interpreted as 'the place or places where the controller is established'. Pursuant to the text of the act there is, in our opinion, in any case no reason to necessarily opt for the first, restricted interpretation.

2.2 What do the comments per article state?

The books that explain the act per article obviously discuss article 4(1) PDPA. In the much-used book *Tekst en Toelichting Wbp* (edited by Hooghiemstra & Nouwt)[6] the passage in question from the explanatory memorandum is paraphrased, however, without clarifying whether it concerns the establishment of the controller himself or the places where establishments are located. This means that this question remains unanswered in this book.

In the less-known *Compendium Wbp* an attempt is made to clarify the text of the article somewhat. This attempt does not fully succeed. The author asserts that:

> *"Dutch law does not apply to forms of data processing in the Netherlands by controllers that do not have such fixed establishment in the Netherlands."[7]*

It is therefore decisive for the compendium whether the controller has a 'fixed establishment in the Netherlands' or not: if this is the case, the act applies; if this is not the case, not. It is not entirely clear though whether the term 'a fixed establishment in the Netherlands' means that the controller himself is established in the Netherlands (restricted interpretation) or that a controller that is established elsewhere also has an establishment in the Netherlands (broader interpretation). We suppose that the author supports the last, i.e. broader interpretation, but are not entirely sure about this.

In the *Handboek Privacy*[8] the following comments are given that are not unambiguous either:

> *"The applicability of the act is assessed on the basis of the establishment of the controller in the first place. Is he established in the Netherlands, the PDPA is applicable to the data processing operations [underlining added by us] of the controller. If the establishment of the controller is located in the European Union, the laws of the country where the controller is established apply."*

The obscurity in this explanation can be found in the use of the plural 'data processing operations' in the second sentence. With this, the authors seem to leave room for a restricted interpretation. This as their interpretation does not seem to exclude that the PDPA applies if a Dutch controller lets a processing perform in the context of (one of) his establishment(s) in another member state. However, by further speaking of 'establishment of the controller' and 'the country where the controller has his establishment' it does not become clear whether the authors mean the member state where the controller himself has his establishment (restricted interpretation) or also the member states where he has establishments (broader interpretation).

Berkvens and De Vries are the most clear and explicit. In the known *Leidraad voor de praktijk* (the 'blue loose-leaf book') Berkens gives the following explanation of article 4(1) of the act:[9]

> *"The starting point of the regime for foreign countries is that the right of establishment [word underlined by the author] of the controller applies. In this case, it does not matter in which country the controller has his headquarters. If the controller has his headquarters in another EU member state but has an establishment in the Netherlands, Dutch law applies to processing operations that can be attributed to the Dutch establishment. If the controller has his headquarters in a country beyond the EU, Dutch law also applies to the Dutch establishment and the processing operations to be attributed to it. Conversely, (pursuant to the Directive) it applies in the EU that the processing operations that can be attributed to a Belgian establishment of a Dutch company fall under Belgian law."*

These comments depart from the broader interpretation, be it that the author does not exclude a more balanced approach by the concept 'attribution of processing operations': the Dutch privacy act applies to the extent that the processing operations can be attributed to an establishment in the Netherlands, also if the controller himself has another establishment.[10]

In her notes to the PDPA in *Tekst & Commentaar Telecommunicatierecht* De Vries does not leave any doubt about the fact that according to her article 4(1) PDPA must not be interpreted in a strict way:

> *"The PDPA also applies if the controller himself is not established in the Netherlands, but has an establishment in the Netherlands, on the condition that there is a processing of personal data in the context of the activities of that establishment."[11]*

This means that on balance all this does not provide much support for a restricted interpretation of article 4(1) PDPA. To the extent that this issue is discussed, support can mainly be found for a broader interpretation, in which the act also applies if the controller himself is not established in the Netherlands but only has an establishment here.

2.3 What does the privacy directive state?

The PDPA does not stand at itself, as it forms the implementation of the privacy directive. This is why it is important how the community legislator has formulated the rule implemented in article 4(1) of the act. At first sight, the directive does not seem very clear either on this point. The first sentence of article 4(1)(a) of the directive states that the act must apply to the data processing operations that are carried out:

> *"…in the context of the activities of an establishment of the controller on the territory of the Member State"*

In this, we read that the act applies if there is an establishment of the controller in the member state, also when the controller himself is not established in the member state. It must be admitted though that this sentence at itself may not exclude an interpretation in which the act only applies if the controller himself is established in the member state (restricted interpretation). As far as there is any doubt about this, this is dispelled though by the consecutive sentence in the provision:

> *"…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 intention of the community legislator can be traced from the formation history of the privacy directive with not too much trouble. Moerel's analysis in her postscript does not leave much to be desired in respect of clarity on this point.[12] The community legislator can only have meant that the act applies if data processing operations are carried out in the context of activities of an establishment in the Netherlands. What is therefore at stake is whether there is an establishment in the Netherlands and whether data are processed in the context of activities of that establishment. Whether the controller himself is established in the Netherlands is not directly important for this.

This means that also the directive does not provide much ground for another interpretation than the PDPA applies if there is an establishment in the Netherlands, also if the controller himself is established elsewhere in the European Union.

2.4 What is (further) stated in literature?

As far as we could check, most authors [13] who have directly or indirectly written about this subject assume that the PDPA applies if there is an establishment in the Netherlands, also if the controller himself might be established elsewhere in the EU. Many authors do this implicitly. Particularly Blok[14] makes an issue of the interpretation of article 4 PDPA in such way by explicitly asserting that the privacy directive gives little to go on for the answer to the question when data processing is carried out in the context of the activities of an establishment. The author analyses the provision and comes to the so-called given, broader interpretation of the article on that basis. Other authors, like Terstegge,[15] Cuipers,[16] Thijssen[17], De Vries[18] and Berkvens[19] seem to depart from a broader interpretation.[20]

All this does not mean though that all authors agree with the implications of this broader interpretation. Almost every one of them sees this interpretation as problematic. This mainly because as a result hereof controllers may have to deal with plural application of national privacy acts: [21] a multinational with establishments in multiple member states must adhere to just as many national privacy acts. For this problem, various practical (partial) solutions are advanced, but none of them is a restricted interpretation of article 4(1) PDPA. We will discuss this further below (par. 3).

2.5 What does the Article 29 data protection working party say?

The consultation body of national privacy watchdogs in the European Union, the Article 29 data protection working party has expressed itself multiple times on the territorial effect of national privacy acts. Its opinions do not seem to depart from the same interpretation though. The working party sometimes seems to support a restricted interpretation of article 4 of the directive, but

sometimes also a broader interpretation. In its opinion on the processing of personal data by SWIFT, the working party seems to have chosen to depart from the applicability of the law in the country where the controller of the data processing is established (restricted interpretation). Or, in this complex case[22], the working party comes to the conclusion that Belgian law applies to the processing of personal data by SWIFT, because the headquarters in Belgium take all crucial decisions on the processing.[23] The working party does not discuss the question whether the data are processed in the scope of the establishments. It is irrelevant for the working party that also in other EU member states personal data are processed by SWIFT. If these data are processed in the context of establishments in the other EU member states, the law of these member states would apply, departing from a broader interpretation.

However, in a less recent opinion on the applicability of the privacy directive on non-EU web sites[24], the working party tries to bend in various, not quite plausible ways to read a so-called country-of-origin principle in article 4(1)(a) of the directive. In its recent opinion on internet search engines [25] the working party comes to the conclusion that for applicability of the article 4(1)(a) it is not required that the controller is established on the territory of the EU but an establishment suffices in the context of which data processing is carried out.

This means that from the opinion of the working party both arguments for a broader or for a more restricted interpretation of article 4(1) PDPA or article 4(1)(a) of the directive respectively can be deduced. Departing from the most recent opinion, it is obvious to assume that the Article 29 data protection working party is currently of the opinion that a broader interpretation must be employed.

2.6 And what does the DPA think?

Until recently, the standpoint of the DPA on the interpretation of article 4(1) PDPA has been unclear. From the statements made by the DPA in public we deduced at first that it has not wanted to make the fundamental choice for a restricted interpretation of article 4(1) PDPA as yet. In her argument, Moerel refers to some publications to be found at the website of the DPA[26] from which it could be deduced according to this author that the watchdog departs from a restricted interpretation of article 4(1) PDPA. These publications do not convince us though. To the extent that it concerns documents of the DPA [27], only paraphrases can be found of the parliamentary history of the act.[28] And with regard to this, we had already determined that this does not excel in clarity and (thus) does not necessarily provide support for the view that the legislator opted for a restricted interpretation.

On the basis of all this, it seemed able to maintain that the DPA has not adopted any standpoint. And that there is therefore only a somewhat academic, almost semantic, discussion about the meaning of the phrase 'the place where the controller is established' in the article of the act. In our opinion, this is not altered by the fact that the watchdog – apparently – would depart from a restricted interpretation in some unpublished correspondence mentioned by Moerel. It is unclear (to us) what the DPA has exactly stated in this correspondence, and how or why it has done this. In addition, it does not seem logical to us that the DPA would not make such policy assumptions with great practical relevance generally public, for example by publishing this correspondence (if necessary anonymised) at its website. As far as it concerns us, no, or in any case no paramount, meaning can be attributed to this then.

All in all this could be a reason for assuming, for the time being, that the DPA, also in view of the statements published by it, has not opted for the abovementioned restricted interpretation. However, this turned out to be no longer defensible pretty fast after the publication the magazine Computerrecht. In an extensive reaction to Moerel's argument, the watchdog indicates frankly for the first time how it finds that article 4(1) PDPA should be interpreted.[29] It appears that the DPA (indeed) adopts the standpoint that it interprets article 4(1) PDPA in a restricted way. This because in its opinion this interpretation "justifies the intention of the legislator to the best". And also because according to it this interpretation:

> *"is to be preferred from the viewpoint of the legal protection of citizens, the prevention of unnecessary additional burden and finally the functioning of the internal market."[30]*

In order to substantiate this standpoint, the watchdog refers to recital 18 and 19 in the privacy directive, and to the First Evaluation Report of the European Commission on the directive,[31] one quotation from the preparatory documents to this Evaluation Report, [32] the explanatory memorandum to the PDPA [33] and some publications of the Article 29 data protection working party.

This reaction by the DPA (quite surprising for us) on Moerel's argument therefore shows that the watchdog indeed interprets article 4(1) PDPA in that sense that the act applies only then if the controller himself is established in the Netherlands.[34]

2.7 What should we think hereof?

In the Netherlands and as far as we can see the rest of the European Union[35], the DPA seems isolated in its option to depart from a restricted interpretation of article 4(1) PDPA. In any case, it does not mention any convincing and authoritative sources (authors, other watchdogs, etc.) that provide clear and direct support for its standpoint. The substantiation given by the watchdog

is extensive, but does not rest on much more than a goal argument for the support of which it could point to some arguments in some policy documents, particularly the First Evaluation Report of the Commission and some texts of the Article 29 data protection working party.

Our conclusion, and as we presume, that of the other authors mentioned above,[36] is that the community legislator has made a clear choice. Different from for example in the E-Commerce Directive (2001/31/EG)[37], it has explicitly not opted for the country-of-origin principle, in which only the law would apply of the country where the controller is established. Instead of this, it departs from plural application if there are establishments in various member states. If a controller has establishments in various member states, the national privacy acts of the distinctive countries apply.

We therefore determine, with Moerel[38] and maybe the other authors mentioned above, that the restricted interpretation of article 4(1) PDPA as supported by the DPA is untenable. We appreciate the creativity of the reasoning built up by the DPA. We also sympathise the intention of the DPA to block cumulation of laws as much as possible and to decrease administrative burdens.[39] However, all this is insufficient to run counter to the intention of the (community) legislator.

In addition, the restricted interpretation as employed by the DPA may solve concrete implementation problems, but simultaneously opens up gaps in the legal protection that the act intends to offer. In her argument, Moerel gives an example of an international whistleblower regulation, pursuant to which personal data are provided to a controller established in the US by a Dutch establishment. This case is important because this makes clear what the implications may be of the restricted or the broad interpretation. Moerel argues that in the restricted interpretation this provision does not seem to fall under the PDPA:

> *"the controller is established beyond the Netherlands [and] because the controller does have an establishment in the Netherlands, article 4(2) PDPA does not apply either".[40]*

From the transfer advice practice of the DPA, an example[41] is known that is comparable to this case. It concerns a permit application (pursuant to article 77(2) PDPA) for the transfer of personal data to the United States in the context of a so-called squeak line, which the controller had to implement in his complete enterprise pursuant to the American law (Sarbanes-Oxley). The DPA has to advise the Minister of Justice about such permit application. In the present case, the DPA does not discuss the question in its advice whether the PDPA is applicable, so that the question remains which assessments the DPA had on the applicability of the PDPA in this advice on the transfer of personal data in the context of squeak lines and whistleblower regulations. Was

the watchdog of the opinion that the Dutch establishment, on the basis of the facts and circumstances of the case, had to be regarded as controller for the transfer in question? Or has the option that the PDPA could not be applicable not occurred to the DPA at all? These are intriguing questions, the answer to which we cannot find back in the advice in question.

Fontein-Bijnsdorp does not discuss these questions but does remark that Moerel passes over the fact that the PDPA contains a whole system of rules for the transfer of personal data beyond the EU.[42] However, for the question whether the act applies anyhow, the transfer rules as such are irrelevant. In her postscript, Moerel is therefore right to assert that the transfer rules do not offer any relief as these only come up after it has been determined that the PDPA applies.[43]

Furthermore, we deem the restricted interpretation of the DPA problematic because this, as far as we can see, is not followed by privacy watchdogs in other member states and therefore affects the harmonisation envisaged by the directive. The consequence is that the DPA may have found a solution for the problem of plural application of privacy acts this way, but this simultaneously gives rise to new problems, i.e. lack of clarity about the territorial effect of the act and the deviation from the assumptions employed in other member states. All this can hardly be regarded as a contribution to the realisation of the internal market – and that is one of the two main goals of the privacy directive and privacy act.[44]

3. Plural application: problem and solutions

The above[45] shows that the DPA has mainly chosen for a restricted interpretation of article 4(1) PDPA in order to prevent that a multinational controller with establishments in various member states would have to adhere to the privacy acts in all these member states. The question is then whether this plural application leads to problems, and subsequently whether the DPA is right to address this by its choice for a restricted interpretation of article 4(1) PDPA. In this last but one paragraph of this contribution we will discuss this.

In her argument, Moerel herself does not extensively discuss the drawbacks of the broader interpretation advocated by it, in which the PDPA is already applicable if there is an establishment in the Netherlands without the controller himself being established here. She does indicate that this interpretation leads to what can also be qualified as problematic according to it:

> *"expansion of the obligations of the controller in the form of cumulation of applicable laws"[46]*

She then also indicates to be an advocate of the implementation of the country-of-origin principle.[47] She is not alone herein. According to other authors like Blok, Terstegge and Cuijpers, the plural application of national privacy acts that is the consequence of a broader interpretation of

article 4(1) PDPA leads to practical problems. Blok points out that controllers must take the privacy laws of various member states into account, which is problematic as these, despite the envisaged harmonisation, differ a lot. He also point out that there is

"unnecessary cumulation of bureaucratic obligations such as the notification requirement".[48]

As practical solution he therefore proposes a centralised (European) notification register.

Terstegge points out that plural application leads to high costs. He does not even exclude that the compliance with various national privacy acts is impossible. In any case, it will lead to compliance problems and what he graphically calls a 'massive administrative burden'.[49] He therefore pleads for the implementation of a country-of-origin principle (so-called *home country control*), be it that this should be applied in a balanced way.[50]

Also Cuijpers points to the aspect of the costs. She speaks of an 'unnecessary burden; by the lack of clarity that exists on the applicable law and the fact that various national privacy acts apply.[51] Just like Terstegge, she advocates the implementation of a country-of-origin principle. In addition thereto, she pleads for a system of mutual recognition in which only one watchdog, i.e. that of the home country, supervises the processing of personal data by a particular organisation, on the territory of the complete European Union.

We concur with these authors. Practice points out that controllers have trouble with and have to incur extra costs if it is necessary to go deeply into the fulfilment of various national privacy acts. As stated above, we certainly support the attempt by the DPA to block cumulation of laws (as much as possible).

In essence, the problems that the DPA wants to address with its restricted interpretation of article 4 should actually be qualified as harmonisation problems. For, if the harmonisation had succeeded better, it would not make much difference which national privacy act (or acts) applies (or apply). In that case, the same rights and obligations would apply everywhere. And where problems arise after all, these could be solved for the time being by streamlining procedures and by an improved collaboration of watchdogs. As far as it concerns us, partial solutions must be sought along these lines for the time being - i.e. as long as the directive has not been amended.

One example concerns the simplification and harmonisation of the way in which the notification requirement of article 18 directive and article 27(1) PDPA is complied with. For this, the DPA has already proposed to come to a uniform standard notification form to be used in all member states.[52] It appears to us that this cannot be very hard, certainly as watchdogs are already consulting each other regularly in the context of the Article 29 data protection working party. And if

privacy watchdogs are developing such uniform notification form, it cannot be very complicated either to draw up a minimum list of the processing operations that (in principle) should be exceptions to the notification requirement. Let us say a harmonisation of the Exemption Decree.[53] It seems very well possible to us, and, in view of the lesser administrative burdens, certainly worth the effort to try it.

Even more practical solutions may be thought of for further streamlining the existing faulty harmonisation of privacy laws in the EU. In a particular term, there is much to say to come to a (uniform) country-of-origin principle, but that solution is obviously reserved to the community legislator. A privacy watchdog will have to confine itself to the abovementioned improved collaboration and streamlining of procedures, and maybe some other solutions of practical nature.

4. Conclusion

A lot more can and will be said about this discussion. In this contribution we come to an end though. The PDPA contains a lot of open and vague standards and abstract, general concepts. At itself, this is not wrong, if it is not inevitable.[54] Open standards are the means by which the legislator sets rules for the situations he cannot view yet or only in a restricted way. And precisely if it concerns something as dynamic as the use of automated processing means, the use of standards and concepts that can be filled in and applied in accordance with the concrete situation and factual circumstances would be appropriate. A consequence of the use of such standards is that the act is generally experienced as difficult, complicated and hard or even unfeasible.[55]

Where it concerns article 4(1) of the act, the legislator has not meant to give the standard an open and vague character though. It is therefore surprising (not to say: amazing) that precisely the interpretation of that standard, more than ten years after the formation of the directive and almost seven years after the entry into effect of the PDPA, still gives rise to a fundamental discussion through the actions of the watchdog. Obviously, this does not alter the importance of this discussion. In her reaction, Fontein-Bijnsdorp was right to remark with all due respect that the final say is up to the court. We hope though that, in view of the term and costs of legal proceedings, it will not be necessary that proceedings are initiated up to and including the Court of Justice.

Whatever may be, as stated, it is more than one step too far that the privacy watchdog, by an own and on balance interpretation of the act and directive shared by few, attempts to come to a solution of the problem of the cumulation of national privacy acts – whatever may be said about the effectiveness of that solution.

In addition, we have doubts about the procedure followed by the watchdog. It makes you think that policy views on something as fundamental as the territorial effect of the act at first only

seems to have been laid down in unpublished correspondence. With regard to us, the most important result of this discussion until now is therefore that the DPA has been open and has made it clear when the law applies according to it, and when not.

What a controller should do with this is the question though. He might appeal to a justified confidence or the principle of legitimate expectations. As the occasion arises, he could assert then that he could assume that the PDPA did not apply. But if this has any chance of success, this only seems helpful with regard to the controller himself, not to others, such as data subjects. What would help is if the watchdog would be prepared to give more comfort with regard to the standpoints it has adopted in this gripping discussion.[56]

A Creative Commons Licence (by-nc-nd 2.5 Netherlands) applies to this text. See for user's conditions:
http://creativecommons.org/licenses/by-nc-nd/2.5/nl

---

[1] Gerrit-Jan Zwenne and Chris Erents are both lawyers at Bird & Bird in The Hague. Gerrit-Jan is also associate professor at eLaw@Leiden, the centre for law and information technology in Europe, of the Leiden University, and fellow at the E.M. Meijers Instituut (Graduate School) of the same university. The authors want to thank Prof. *Mr.* J.M.A. Berkvens, *Mr.* J.H.J. Terstegge and Mr. L. Mommers for their comments on an earlier version of this contribution.

[2] E.M.L. Moerel, 'Back to basics; wanneer is de Wet bescherming persoonsgegevens van toepassing?, *Computerrecht* 2008/3, p. 81-91.

[3] Directive 95/46/EC of the European Parliament and of 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, *OJ* 1995, L 281/31–50.

[4] M.A.H. Fontein-Bijnsdorp, 'Art. 4 Wbp revisited: enkele opmerkingen inzake de toepasselijkheid van de Wet bescherming persoonsgegevens', *Computerrecht* 2008/6, p. 285-289.

[5] E.M.J. Moerel, 'Art 4 Wbp revisited; postscript De nieuwe WP Opinie inzake Search Engines', in: *Computerrecht* 2008/6, p. 290-298.

[6] T. Hooghiemstra & S. Nouwt, *Tekst en toelichting Wet bescherming persoonsgegevens*, 2007, p. 61.

[7] J.G. Brouwer, *Compendium Wet bescherming persoonsgegevens. Tekst en toelichting*, 2002, p. 102.

[8] A. Holleman, J. Nouwt & H.H. de Vries, Artikelgewijs commentaar, in: (Holvast e.a. red.), *Handboek Privacy: Bescherming persoonsgegevens*, update 27, 1300: article 4, Kluwer.

[9] J.M.A. Berkvens, in: *Wet bescherming persoonsgegevens; Leidraad voor de praktijk*, comments to article 4, supplement 3, April 2002.

[10] The postscript of Fontein-Bijnsdorp also contains a, somewhat concealed, clue for such balanced approach. In her reaction, this author indicates that "in order to determine whether Dutch law applies to a specific processing in the context of the activities of the establishment in question, [..] the role which the branch plays in the specific processing [must] be determined, as set out above. This must be assessed on the basis of the facts and circumstances of the case." As stated M.A.H. Fontein-Bijnsdorp, 'Art. 4 Wbp revisited: enkele opmerkingen inzake de toepasselijkheid van de Wet bescherming persoonsgegevens', *Computerrecht* 2008/6, p. 287.

[11] De Vries 2009 (*T&C Telecommunicatierecht e.a*), article 4 PDPA, note 1, p. 559-560.

[12] Especially see E.M.J. Moerel, 'Art 4 Wbp revisited; naschrift De nieuwe WP Opinie inzake Search Engines', *Computerrecht* 2008/6, p. 290-298.

[13] An exception may be: L.B. Sauerwein & J.J. Linnemann, *Handleiding voor verwerkers van persoonsgegevens*, 2002, p. 15. These authors paraphrase the explanatory memorandum, of which we have already determined that this does not excel in clarity but from which it must not be absolutely deduced that a restricted interpretation was chosen.

[14] P.H. Blok, 'Privacybescherming in alle staten', *Computerrecht* 2005/6, p. 297-304, with note p. 299.

[15] J.H.J. Terstegge, 'Home Country Control - Improving privacy compliance and supervision', *P&I* December 2002, p. 257-259.

[16] C. Cuijpers, 'Evaluatie van de Richtlijn', in: *Privacy Concerns*, 2003, p. 114.

[17] M.B.J. Thijssen, 'Grensoverschrijdend gegevensbeschermingsrecht', in: *P&I* June 2005, no. 3, p. 110-113.

[18] De Vries 2009 (*T&C Telecommunicatierecht e.a*), article 4 PDPA, note 1, p. 559-560, 2009.

[19] J.M.A. Berkvens, in: Wet bescherming persoonsgegevens; Leidraad voor de praktijk, comments to article 4, supplement 3, April 2002.

[20] In the companian "Privacyregulering in theorie en praktijk", Terstegge (p. 68-69) follows u pon the broader interpretation in the fourth edition (2007). Less clear are J.E.J. Prins & J.M.A. Berkvens in the third edition (2002): "the PDPA asserts that the Dutch provisions are applied, if the processing of personal data is made in the context of activities of an establishment of a controller in the Netherlands" and "The above shows that with regard to the question which law applies at first the place of establishment of the controller charged with the processing is followed. If this place is beyond the Community, the place where the processing takes place is followed." (p. 100).

[21] With 'the national privacy act' we mean, in accordance with the somewhat misleading but yet current language, the law with which the privacy directive has been converted into national law.

[22] SWIFT is a world-wide operating service provider for financial messages traffic for international money transfers. SWIFT stores all its messages in two processing centres established in the EU and in the US for 124 days. In addition, SWIFT has establishments in various EU member states. After the attacks in the US in September 2001, the American authorities claim access to the message data. SWIFT's headquarters, established in Belgium, negotiates with the American authorities and consents tot hem getting access to the message data.

[23] Article 29 Data Protection Working Party, WP 128, opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunications (SWIFT) approved on 22 November 2006, see: paragraph 2.2.

[24] Article 29 Data Protection Working Party, WP 56, working document on determining the international application of EU data protection laws to personal data processing on the Internet by non-EU based web, approved on 30 May 2002, see: paragraph 2.

[25] Article 29 Data Protection Working Party, WP 148, opinion 1/2008 on data protection issues related to search engines, approved on 4 April 2008, see: paragraph 4.1.2.

[26] E.M.L. Moerel, 'Back to basics; wanneer is de Wet bescherming persoonsgegevens van toepassing?', *Computerrecht* 2008/3, see: footnote 21 in that text.

[27] Sauerwein & Linnemann wrote their handbook on the instructions of the Dutch Ministry of Justice.

[28] This also applies to the publication of D. Alonso Blas not cited by Moerel, Nota derde Landen. *De doorgifte van persoonsgegevens naar derde landen in het kader van de WBP*, College bescherming persoonsgegevens 2003, p. 6.

[29] M.A.H. Fontein-Bijnsdorp, 'Art.4 Wbp revisited': enkele opmerkingen inzake de toepasselijkheid van de Wet bescherming persoonsgegevens, *Computerrecht* 2008/6, p. 285-289.

[30] M.A.H. Fontein-Bijnsdorp, 'Art.4 Wbp revisited': enkele opmerkingen inzake de toepasselijkheid van de Wet bescherming persoonsgegevens, *Computerrecht* 2008/6, p. 289.

[31] First report on the implementation of the Data Protection Directive (95/46/EC), COM/2003/265, 15 May 2003.

[32] Analysis and impact study on the implementation of Directive EC 95/46 in Member States, technical analysis of the transposition in the Member States.

[33] Parliamentary Documents II 1997/98, 25 892, no. 3.

[34] This is clearly shown by the remarks in footnote 5 of M.A.H. Fontein-Bijnsdorp, 'Art.4 Wbp revisited: enkele opmerkingen inzake de toepasselijkheid van de Wet bescherming persoonsgegevens', *Computerrecht* 2008/6, p. 285.

[35] See E.M.J. Moerel, 'Art 4 Wbp revisited; naschrift De nieuwe WP Opinie inzake Search Engines', *Computerrecht* 2008/3, p. 81.

[36]See par. 2.4 of this contribution.

[37] 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, OJ 2000 L178/1-16.

[38] E.M.J. Moerel, 'Art 4 Wbp revisited; naschrift De nieuwe WP Opinie inzake Search Engines', *Computerrecht* 2008/6, p. 295.

[39] M.A.H. Fontein-Bijnsdorp, 'Art.4 Wbp revisited: enkele opmerkingen inzake de toepasselijkheid van de Wet bescherming persoonsgegevens', *Computerrecht* 2008/6, p. 288.

[40] E.M.L. Moerel, 'Back to basics; wanneer is de Wet bescherming persoonsgegevens van toepassing?', *Computerrecht* 2008/3, paragraph 3.5.

[41] DPA, Opinion permit application pursuant to article 77(2) PDPA, z2004-1233, 16 January 2006.

[42] M.A.H. Fontein-Bijnsdorp, 'Art.4 Wbp revisited: enkele opmerkingen inzake de toepasselijkheid van de Wet bescherming persoonsgegevens', *Computerrecht* 2008/6, p. 288

[43] E.M.J. Moerel, 'Art 4 Wbp revisited; naschrift De nieuwe WP Opinie inzake Search Engines', *Computerrecht* 2008/6, p. 296.

[44] See recital 3 of the privacy directive and obviously article 1 thereof.

[45] Par. 2.6 of this contribution.

[46] E.M.L. Moerel, 'Back to basics; wanneer is de Wet bescherming persoonsgegevens van toepassing?', *Computerrecht* 2008/3, p. 81.

[47] E.M.L. Moerel, 'Back to basics; wanneer is de Wet bescherming persoonsgegevens van toepassing?', *Computerrecht* 2008/3, p. 85.

[48] P.H. Blok, 'Privacybescherming in alle staten', in: *Computerrecht* 2005/6, p. 300.

[49] J.H.J. Terstegge, 'Home Country Control - Improving privacy compliance and supervision', *P&I* December 2002, p. 257; also see: G-J. Zwenne et al, *Eerste fase evaluatie Wet bescherming persoonsgegevens*, Ministry of Justice, December 2007. p. 68.

[50] This is the explanation we received from the author by e-mail. He may work out a discussion on this interesting thought in a contribution for this magazine.

[51] C. Cuijpers, 'Evaluatie van de Richtlijn', in: *Privacy Concerns*, NVvIR 2003, p. 114.

[52] DPA Letter to Minister of Justice, 7 December 2004, z2004-1086; on this, see G-J. Zwenne et al, *Eerste fase evaluatie Wet bescherming persoonsgegevens*, Ministry of Justice, December 2007, p. 70.

[53] Dutch Bulletin of Acts and Decrees 2001, 250.

[54] *Inter alia* see Parliamentary Documents II 1997/98, 25 892, no. 3, p. 5-6, 9, 12-13, 33.

[55] See G-J. Zwenne et al, Eerste *fase evaluatie Wet bescherming persoonsgegevens*, Ministry of Justice, December 2007. p. 64-64.

[56] This may lend itself for an Opinion by the Authority. See DPA Rules for request for opinion, 11 March 2008, Dutch Bulletin of Acts and Decrees 2008; 71.