UNOFFICIAL TRANSLATION

Written opinion on the application of the Wet bescherming persoonsgegevens [Dutch Data Protection Act] in the case of a contract for cloud computing services from an American provider

Introduction

On 20 February 2012, the Dutch Data Protection Authority (Dutch DPA) [College bescherming persoonsgegevens (CBP)] received a request (dated 25 January 2012) from SURFmarket (at that time still called SURFdiensten) for a written opinion.[1] Parallel to meeting this request, the Dutch DPA also worked together with the other European Data Protection Authorities, assembled in the Article 29 Data Protection Working Party (WP29), to formulate a joint position on cloud computing in relation to the protection of personal data. This latter activity resulted in an Opinion that was adopted on 1 July 2012 by the plenary session of WP29.[2] The Dutch DPA's wish to align its position in this written opinion with the European position was one of the reasons it has taken longer to meet this request than is customary. The Dutch DPA has meanwhile contacted SURFmarket about this.

In its request, SURFmarket states that it is in discussion with a European establishment of an American provider regarding the free provision of a number of cloud services,[3] and that during these discussions 'differences [have] arisen concerning the interpretation of the EU Data Protection Directive 95/46/EC' and its implementation in the Wet bescherming persoonsgegevens (Wbp) [Dutch Data Protection Act]. SURFmarket comments in this regard that due to the differences in interpretation 'there is a risk that the security and protection of personal data of a great many people will be found wanting, since SURFmarket, through its services, can potentially provide hundreds of thousands of employees and students with the [cloud services]'. SURFmarket points out that special categories of personal data are also processed.

Briefly summarised, SURFmarket has submitted the following questions to the Dutch DPA:

1. Does the self-certification by the American provider to the *Safe Harbor Framework* offer sufficient safeguards for the transfer of personal data to the United States (U.S.)?
2. Does the *Statement on Auditing Standards no. 70* (SAS 70) standard offer sufficient certainty regarding the security of the processed personal data, or are the *International Standard for Assurance Engagements* (ISAE) 3402 and *Statement on Standards for Attestation Engagements* (SSAE) 16 standards better equipped for this purpose?

---

[1] SURFmarket is part of SURF, the collaborative organisation for higher education and research within which Dutch research universities, universities of applied sciences and research institutions unite to undertake joint investments nationally and internationally in IT-driven innovation. SURF consists of several organisations, each responsible for its own field: SURF, SURFnet, SURFmarket, SURFshare and, shortly, SURFsara. Since 1991, SURFmarket has negotiated and concluded contracts with providers of software and scientific content and sources of information on behalf of employees and students in higher education and scientific research in the Netherlands.
See < http://www.surfmarket.nl/Over/Paginas/Samenwerking.aspx >.

[2] At the time of issue of this opinion, this Opinion was only available in English: *Opinion 05/2012 on Cloud Computing* of 1 July 2012.
< http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf >

[3] The cloud services offered concern e-mail, agenda management, group discussions and (customer) relationship management.

3. Is the self-certification of the American provider to the *Safe Harbor Framework* sufficient to safeguard that sub-processors engaged by the provider satisfy a comparable suitable level of protection?

The three questions submitted by SURFmarket to the Dutch DPA are answered in this written opinion below. The Dutch DPA intends that these responses should provide clarity to as large a group of providers and clients as possible regarding the matters raised in the questions submitted by SURFmarket. The responses to the questions are therefore formulated in rather general terms. The responses assume the existence of a controller established in the Netherlands who uses the cloud computing services of a provider established in the United States (U.S.) for the processing of personal data subject to the Wbp.

Legal framework

Article 13 (security measures), Article 14 (engagement of data processors), Article 15 (supervision by the controller) and Articles 76 and 77 (international transfer) of the Wbp are of relevance for responding to the questions that have been submitted. These Articles will be discussed in further detail in the response to the questions given in this written opinion below.

The *Safe Harbor Framework*, which is referred to in two of the three questions submitted, aims to facilitate the transfer of personal data from the European Union (EU)/the European Economic Area (EEA) to the U.S. without thereby compromising the protection of the personal data. It involves a type of self-certification whereby organisations undertake to comply with a number of principles in the area of data protection (the *Safe Harbor Principles*). The relevant substantive aspects of the *Safe Harbor Framework* are discussed in further detail in the response to each question.

On 1 July 2012, WP29, an assembly of European Data Protection Authorities, adopted an Opinion on cloud computing in relation to the protection of personal data.[4] This written opinion is partly based on this Opinion. Furthermore, the Dutch DPA took due note of the earlier decisions of the Norwegian[5] and Danish[6] data protection authorities on cloud computing when drafting this written opinion.

Transfer of personal data in the cloud

Does the self-certification by the American provider to the Safe Harbor Framework offer sufficient safeguards for the transfer of personal data to the United States (U.S.)?

Before proceeding to answer the above question, the requirements which the Wbp and the *Safe Harbor Principles* impose on transfer in general will first be set out below. The Opinion adopted by the WP29 will also be discussed in this context.

Articles 76 and 77 Wbp provide for the transfer of personal data to countries outside the EU/EEA. Transfer is a form of data processing. In principle, personal data may only be transferred to a country outside the EU/EEA if that country guarantees an 'adequate level of protection'.

---

[4] WP29, Opinion 05/2012 on Cloud Computing of 1 July 2012.

[5] Decision of the Norwegian data protection authority: *Will not let Norwegian enterprises use Google Apps*, < http://www.datatilsynet.no/English/Publications/Will-not-let-Norwegian-enterprises-of-Google-Apps/ >

[6] Decision of the Danish data protection authority: *Processing of sensitive personal data in a cloud solution*, < http://www.datatilsynet.dk/english/processing-of-sensitive-personal-data-in-a-cloud-solution/ >

Where an adequate level of protection is absent, there is in principle a prohibition on transfer and personal data may only be transferred to countries outside the EU/EEA on the basis of one of the (statutory) exemptions referred to in Article 77 Wbp, such as the express permission of a data subject, for the necessary execution of an agreement or pursuant to a permit issued by the minister of Security and Justice. The general requirements of the Wbp must also be complied with in all cases.
The U.S. is not designated as a country with an 'adequate level of protection' due to the absence of general legislation providing for the protection of personal data. In order to facilitate trade relations between the U.S. and the EU, and without wishing to compromise the level of protection of personal data, the U.S. - EU *Safe Harbor Framework* was consequently established in 2000 and has since been designated by the European Commission by a Decision as affording an 'adequate level of protection'.[7]
The *Safe Harbor Framework* is a form of self-regulation by companies. In order to self-certify, an organisation wishing to enter the Safe Harbor programme must register with the U.S. Department of Commerce and declare publicly that it will comply with the *Safe Harbor Principles*. The Commission Decision also imposes different requirements on the registration, such as the requirement on the organisation to develop and publish its own self-regulatory privacy policy. Only organisations that have undertaken to adhere to the *Safe Harbor Principles* will be deemed to afford an adequate level of protection.

The statement of compliance with the *Safe Harbor Principles* does not in itself guarantee that the organisations actually implement those Principles in practice. The Opinion adopted by WP29 notes as follows in this regard:

> *'The Working Party considers that companies exporting data should not merely rely on the statement of the data importer claiming that he has a Safe Harbor certification. On the contrary, the company exporting data should obtain evidence that the Safe Harbor selfcertifications exists and request evidence demonstrating that their principles are complied with. This is important especially with regard to the information provided to data subjects affected by the data processing.'*[8]

Hence, in a cloud computing context the controller responsible for the transfer is expected not only to verify whether the self-certification exists, but also that he requests evidence demonstrating that the *Safe Harbor Principles* are actually complied with by the importer of the personal data.

The *Safe Harbor Principles*, on the basis of which self-certification takes place, are formulated at a high abstraction level.[9] As a guide to their interpretation, the U.S. authorities have published a set of *Frequently Asked Questions* (FAQs).[10] Regarding the relationship between the *Safe Harbor Privacy Principles* and related FAQs on the one hand and Directive 95/46/EC on the other the European Commission provides as follows in Article 2 of the Decision referred to above:

---

[7] 2000/520/EC Commission Decision of 26 July 2000, L 215, 25/08/2000, p. 0007-0047. See also: < http://export.gov/safeharbor/ >.
[8] WP 29, *Opinion 05/2012 on Cloud Computing* of 1 July 2012, § 3.5.1, page 17.
[9] *Safe Harbor Privacy Principles, issued by the U.S. Department of Commerce on 21 July 2000*, < http://export.gov/safeharbor/eu/eg_main_018475.asp >
[10] *U.S.-EU Safe Harbor Framework Documents: C. Frequently Asked Questions*, < http://export.gov/safeharbor/eu/eg_main_018493.asp >

'This Decision concerns only the adequacy of protection provided in the United States under the Principles implemented in accordance with the FAQs [...] and does not affect the application of other provisions of that Directive that pertain to the processing of personal data within the Member States [...].'

Therefore, compliance with the *Safe Harbor Principles* means solely that personal data may be transferred to the U.S., and does not guarantee that the processing of the personal data in the U.S. meets all the requirements under Directive 95/46/EC. Nor is there any guarantee that the processing in the U.S. meets all the requirements under the applicable national law in which Directive 95/46/EC has been implemented. Even where processing is carried out by a data processor, as well as in the case of processing in the cloud, the controller remains responsible for compliance with this law. The controller will therefore have to ensure, on the conclusion of the contract, that all applicable statutory provisions are covered, and he will also have to ensure that any additional agreements are incorporated in the contract.

One matter requiring specific attention in this connection is the protection of the processed personal data. WP29 states as follows in this regard:

'Finally, the Working Party considers that the Safe Harbor principles by themselves may also not guarantee the data exporter the necessary means to ensure that appropriate security measures have been applied by the cloud provider in the US, as may be required by national legislations based on the Directive 95/46/EC. In terms of data security cloud computing raises several cloud-specific security risks, such as loss of governance, insecure or incomplete data deletion, insufficient audit trails or isolation failures, which are not sufficiently addressed by the existing Safe Harbor principles on data security. Additional safeguards for data security may thus be deployed; such as by incorporating the expertise and resources of third parties that are capable of assessing the adequacy of cloud providers through different auditing, standardization and certification schemes. For these reasons it might be advisable to complement the commitment of the data importer to the Safe Harbor with additional safeguards taking into account the specific nature of the cloud.'[11]

So, compliance with the *Safe Harbor Principles* does not by itself offer any certainty that the personal data processed in the cloud are adequately protected, and it will be necessary to make additional agreements in this regard in the data processor's contract.[12]

In summary, the following can be stated with regard to the safeguards afforded by the *Safe Harbor Framework* for the transfer of personal data to the U.S., and the following attention points can be offered:

1. The statement of compliance with the *Safe Harbor Principles* does not by itself guarantee that the organisation actually adheres to them in practice. The controller will have to ensure that the self-certification exists and that it is actually complied with in practice.

---

[11] WP 29, *Opinion 05/2012 on Cloud Computing* of 1 July 2012, § 3.5.1, page 18.

[12] ENISA, the European Network and Information Security Agency, has published a guide on this topic. ENISA, *Procure secure: A guide to monitoring of security service levels in cloud contracts*, < http://www.enisa.europa.eu/activities/application-security/cloud-computing/procure-secure-a-guide-to-monitoring-of-security-service-levels-in-cloud-contracts >

2. Even if the *Safe Harbor Principles* are demonstrably complied with, this merely means that the transfer of personal data to the U.S. can take place and not that the processing in the U.S. meets all the requirements under Directive 95/46 EC. Nor is there any guarantee that the processing in the U.S. meets all the requirements under the applicable national law in which Directive 95/46/EC has been implemented. Even where processing is carried out by a data processor, as well as in the case of processing in the cloud, the controller remains responsible for compliance with this law. The controller will therefore has to ensure, on the conclusion of the contract, that all applicable statutory provisions are covered, and he will also have to ensure that any additional agreements are incorporated in the contract.
3. One matter requiring specific attention in this connection is the protection of the processed personal data. Compliance with the *Safe Harbor Principles* does not by itself offer any certainty that adequate security measures are put in place to protect the personal data processed in the cloud, and it will be necessary to make additional agreements in this regard in the data processor's contract.

Security of personal data in the cloud

Does the standard Statement on Auditing Standards no. 70 (SAS 70) offer sufficient certainty regarding the security of the processed personal data, or are the standards International Standard for Assurance Engagements (ISAE) 3402 and Statement on Standards for Attestation Engagements (SSAE) 16 better equipped for this purpose?

The standards referred to in the question contain guidelines for the issuing of a statement by an independent external expert regarding the measures implemented by a data processor. The statement is drawn up at the request of the data processor and is provided to the controllers making use of its services. The purpose of providing such a statement is to offer the controllers insight into the measures that have been implemented without every controller himself having to conduct his own investigation (or have one conducted) in that regard.
There are several broadly accepted standards for drawing up such statements. The main ones are the three standards mentioned in the question: SAS70, ISAE 3402 and SSAE 16. In the Netherlands, ISAE 3402 is the most commonly applied standard. SSAE 16 is heavily based on ISAE 3402, although in certain respects its effects are scaled for applicability within the American regulatory scope. Both standards replace the now defunct SAS 70.
Within ISAE 3402 as well as SSAE 16, the basis for the statement is constituted by a description by the data processor of the measures that are relevant to the target group of the statement. The external expert tests this description for example on completeness and then determines whether the data processor has actually implemented the measures described. Depending on the type of statement, the external expert delivers a judgement on the presence of the measures described on a particular date (type 1) or during a particular period (type 2).

Before proceeding to answer the question that has been submitted, the requirements that the Wbp imposes on the security of personal data in case of processing by a data processor will first be briefly set out below. These requirements are applicable to every form of processing by a data processor, even where the processing takes place in the cloud. The core of these requirements is set out in Article 14 Wbp. In addition, Article 12 and Article 13 Wbp are also applicable to processing by a data processor.
Article 14 Wbp prescribes that the controller, where he allows personal data to be processed by a data processor, must ensure that the data processor takes adequate technical and

organisational measures. The controller must supervise compliance with these measures.[13] The agreements that the controller makes with the data processor regarding the protection and security of personal data must be laid down in writing or in another equivalent form.[14] Article 13 Wbp prescribes that the controller must take suitable technical and organisational measures to protect the personal data processed by him against loss and unlawful or wrongful processing. In case of processing by a data processor, the controller must ensure that the data processor complies with the obligations to which the controller is subject under Article 13.[15] Article 12 Wbp prescribes that the data processor, its personnel and others coming under its authority may only process personal data on the instructions of the controller. The controller must supervise compliance with this obligation.[16] Article 12 furthermore imposes an obligation of confidentiality on the data processor, its personnel and others coming under its authority with regard to the personal data processed by them.

Such a statement can be a means for the controller to ascertain whether the data processor has actually taken the necessary organisational and technical protection measures. Important points in this regard are:

1. Standard SAS 70 is no longer used. Standards ISAE 3402 and SSAE 16, which have replaced SAS 70, are more or less comparable with one another. Both standards are concerned with the manner in which an independent external expert performs his examination and reports on it, and not with the measures that are audited.
2. Of particular significance to the controller is which measures are included in the statement and whether an opinion is given regarding the presence of the measures described on a particular date (type 1) or during a particular period (type 2). Gaps in the statement in relation to technical security measures that are specific to processing in the cloud, for example,[17] must be addressed via supplementary reports.

Processing by sub-processors in the cloud

Is the self-certification of the American provider to the Safe Harbor Framework sufficient to safeguard that sub-processors engaged by the provider satisfy a comparable suitable level of protection?

Processors of personal data can engage the services of sub-processors in the context of processing personal data. A cloud service provider that makes applications available to its clients can, for example, use the services of a sub-processor for the physical storage of the processed personal data.

Before proceeding to answer the question that has been submitted, the requirements under the Wbp and the *Safe Harbor Principles* relating to the engagement of sub-processors for the processing of personal data will first be briefly set out below.

---

[13] Article 14, subsection 1, Wbp.
[14] Article 14, subsection 2 Wbp: 'The performance of processing by a data processor is provided for in a contract or pursuant to another legal act resulting in an engagement between the data processor and the controller'. Article 14, subsection 5 Wbp: 'With a view to the storage of the evidence, the parts of the contract or the legal act relating to the protection of personal data as well as the security and protection measures referred to in Article 13 will be laid down in writing or in another equivalent form'.
[15] Article 14, subsection 3(b) Wbp.
[16] Article 14, subsection 3 (a) Wbp.
[17] For more information see ENISA, Procure secure: A guide to monitoring of security service levels in cloud contracts, URL: http://www.enisa.europa.eu/activities/application-security/cloud-computing/procure-secure-a-guide-to-monitoring-of-security-service-levels-in-cloud-contracts

The requirements imposed by Articles 12, 13 and 14 Wbp on the security and protection of personal data when processed by a data processor have been discussed under the response to the previous question. These requirements are applicable in their entirety where the data processor has the personal data processed by one or more sub-processors.
The starting point remains that the controller is responsible for everything that happens to the personal data, and it follows from this responsibility that personal data can only be processed by a sub-processor with the express consent of the data processor. If the controller has expressly provided scope for this in the data processor's contract, the data processor may - without loss or diminishment of its full liability for compliance with the contract with the controller - outsource parts of the processing to sub-processors. Where it does so, the data processor must nonetheless take steps to secure contractual assurance that the sub-processor will similarly be guided by and adhere to the instructions of the controller, will be obliged to maintain confidentiality and will take the necessary security and protection measures in respect of the data processing.[18]

In the principle relating to 'onward transfer', the *Safe Harbor Principles* impose the following requirements on the engagement of (sub-)processors:

> *'Where [an organization] wishes to transfer information to a third party that is acting as an agent,[19] it may do so if it first either ascertains that the third party subscribes to the Safe Harbor Principles or is subject to the directive or another adequacy finding or enters into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant Safe Harbor Principles. If the organization complies with these requirements, it shall not be held responsible (unless the organization agrees otherwise) when a third party to which it transfers such information processes it in a way contrary to any restrictions or representations, unless the organization knew or should have known the third party would process it in such a contrary way and the organization has not taken reasonable steps to prevent or stop such processing.'*

WP29 states as follows regarding the engagement of sub-processors in the processing of personal data in the cloud:

> *'If processors subcontract services out to sub-processors, they are obliged to make this information available to the client, detailing the type of service subcontracted, the characteristics of current or potential subcontractors and guarantees that these entities offer to the provider of cloud computing services to comply with Directive 95/46/EC. All the relevant obligations must therefore apply also to the sub-processors through contracts between the cloud provider and subcontractor reflecting the stipulations of the contract between cloud client and cloud provider.* […] *In the view of the WP29, the processor can subcontract its activities only on the basis of the consent of the controller, which may be generally given at the beginning of the service with a clear duty for the processor to inform the controller of any intended changes concerning the addition or replacement of subcontractors with the controller retaining at all times the possibility to object to such changes or to terminate the contract. There should be a clear obligation of the cloud provider to name all the subcontractors commissioned. In*

[18] Explanatory Memorandum to Wbp, with regard to Section 1 (e)
[19] In the Safe Harbor Principles, the role of data processor or sub-processor is described as 'a third party acting as an agent of an organization to perform task(s) on behalf of and under the instructions of that organization'.

addition, a contract should be signed between cloud provider and subcontractor reflecting the stipulations of the contract between cloud client and cloud provider.'[20]

WP29 stresses that, even in situations where there are several (sub-)processors, the responsibilities in relation to compliance with statutory provisions and legal regulations must be set out clearly and that the controller retains ultimate responsibility:

> *'In such scenarios, the obligations and responsibilities deriving from data protection legislation should be set out clearly and not dispersed throughout the chain of outsourcing or subcontracting, in order to ensure effective control over and allocate clear responsibility for processing activities'*[21]

In summary, it can be stated that self-certification to the *Safe Harbor Framework* is not sufficient to safeguard that (sub-)processors satisfy a comparable suitable level of protection for the following reasons, and the following attention points can be highlighted:

1. The 'Onward Transfer' principle from the *Safe Harbor Principles* permits processing by a (sub-)processor under certain conditions: the (sub-)processor must itself also subscribe to the *Safe Harbor Principles*, for example.
2. The limitations of the safeguards afforded by self-certification for processing by a (sub-)processor are analogous to what has been stated previously in this written opinion. An organisation that subscribes to the *Safe Harbor Principles* is not obliged to ascertain whether a (sub-)processor actually adheres in practice to the conditions that have been specified. Furthermore, even if the (sub-)processor does actually comply with the conditions that have been specified then still there is no guarantee that the processing by the (sub-)processor thereby also meets all the requirements under Directive 95/46/EC or under the national law in which this Directive is implemented.
3. The requirements set by the Wbp on processing by sub-processors go farther than the requirements under the *Safe Harbor Principles*. The Wbp only permits the engagement of sub-processors if the controller expressly provides scope for this in the data processor's contract, and the data processor must have secured contractual assurance that the sub-processor will similarly be guided by and adhere to the instructions of the controller, will be obliged to maintain confidentiality and will take the necessary security and protection measures in respect of the data processing.
4. Even where several (sub-)processors are engaged, the controller remains fully responsible for compliance with the Wbp.
5. In relation to the previous question, it can be noted furthermore that statements can be issued either under inclusion (*'inclusive'*) or exclusion (*'carve-out'*) of the steps taken by sub-processors. If use is made of statements, the controller must set out in the processor's contract whether the steps taken by sub-processors are or are not included.

Concluding observations

In this written opinion, the Dutch DPA has provided a general answer to the questions that were submitted to it. It has based its responses on the assumption of personal data processing subject to the Wbp, with a controller established in the Netherlands that sources cloud computing services from a data processor established in the U.S. subscribing to the *Safe Harbor Principles*.

---

[20] WP 29, *Opinion 05/2012 on Cloud Computing* of 1 July 2012, § 3.3.2, page 9.
[21] WP 29, *Opinion 05/2012 on Cloud Computing* of 1 July 2012, § 3.3.2, page 9.

However, a feature of cloud computing is that the processing of data can potentially take place on servers that may be located anywhere around the globe. The Opinion adopted by WP29 comments as follows in this regard:

> *'However, cloud computing is most frequently based on a complete lack of any stable location of data within the cloud provider's network. Data can be in one data centre at 2pm and on the other side of the world at 4pm. The cloud client is therefore rarely in a position to be able to know in real time where the data are located or stored or transferred. In this context, the traditional legal instruments providing a framework to regulate data transfers to non-EU third countries not providing adequate protection, have limitations.'*[22]

WP29 adds:

> *'Adequacy findings, including Safe Harbor, are limited in respect of the geographical scope, and therefore do not cover all transfers within the cloud.'*[23]

Furthermore, within a cloud context there will often be several (sub-)processors, and even several controllers. The starting point remains, as previously stated, that the controller retains ultimate responsibility for ensuring compliance with the Wbp, even in case of personal data processing in the cloud.

In order to meet his responsibility to ensure compliance with the Wbp, the controller will first have to conduct a risk analysis in order to ascertain whether, and under which conditions, use can be made of cloud computing in his specific situation. This was also a key conclusion in the Opinion adopted by WP29:

> *'A key conclusion of this Opinion is that businesses and administrations wishing to use cloud computing should conduct, as a first step, a comprehensive and thorough risk analysis. All cloud providers offering services in the EEA should provide the cloud client with all the information necessary to rightly assess the pros and cons of adopting such a service. Security, transparency and legal certainty for the clients should be key drivers behind the offer of cloud computing services.'*[24]

The risk analysis not only provides insight into the risks, but also into the additional steps that must be taken in order to safeguard that the relevant processing of personal data in the cloud satisfies the Wbp.

Secondly, the controller will have to select a cloud service provider that offers adequate safeguards, and he will have to set out the necessary agreements and arrangements made in the contract with the processor. WP29 makes the following general recommendations in this regard:

> *'In terms of the recommendations contained in this Opinion, a cloud client's responsibilities as a controller is highlighted and it is thus recommended that the client should select a cloud provider that guarantees compliance with EU data protection*

---

[22] WP 29, *Opinion 05/2012 on Cloud Computing* of 1 July 2012, § 3.5, page 17.
[23] WP 29, *Opinion 05/2012 on Cloud Computing* of 1 July 2012, § 3.5.1, page 17.
[24] WP 29, *Opinion 05/2012 on Cloud Computing* of 1 July 2012,Executive summary, page 2.

legislation. […] any contract between the cloud client and cloud provider should afford sufficient guarantees in terms of technical and organizational measures. Also of significance is the recommendation that the cloud client should verify whether the cloud provider can guarantee the lawfulness of any cross-border international data transfers.'[25]

An attention point is liability for possible breaches of the protection of personal privacy. Article 49 Wbp makes the controller liable for any loss or damage arising from non-compliance with the Wbp, and makes the data processor liable for any loss or damage that may be caused due to its activity. It is necessary to specify this liability in the processor's contract and to ascertain clearly in advance which natural or legal person is liable in which cases and to what degree.

Finally, the Dutch DPA wishes to draw attention to the Dutch government's intention to create the so-called 'brede meldplicht' [broad notification requirement] for data breaches. Providers of publicly available electronic communications services are already subject to such a notification requirement, which is included in Article 11.3.a of the Telecommunicatiewet [Dutch Telecommunications Act] (the so-called 'smalle meldplicht' [narrow notification requirement]). The broad notification requirement is directed towards the controller. Where personal data are processed by a data processor, the controller must ensure that the data processor 'complies with the obligations resting with the controller in terms of the requirement to notify [data breaches]'. The agreements made by the controller with the data processor regarding compliance with the notification requirement must be set out in writing or in another equivalent form.[26] The requirements under the Bill are applicable in their entirety to the processing of personal data in the cloud and to processing by sub-processors. It is recommended that this already be taken into account when entering into contracts and other agreements with providers of cloud services.

[25] WP 29, *Opinion 05/2012 on Cloud Computing* of 1 July 2012, Executive summary, page 2.

[26] Amendment of the Wet bescherming persoonsgegevens [Dutch Data Protection Act] to provide for extension of the use of camera images and the introduction of a notification requirement in case of data breaches

< http://www.rijksoverheid.nl/documenten-en-publicaties/kamerstukken/2011/12/20/wijziging-van-de-wet-bescherming-persoonsgegevens-voor-verruiming-gebruik-camerabeelden-en-invoering-van-meldplicht-bij-datalekken.html >;
Explanatory Memorandum to the Amendment of the Wet bescherming persoonsgegevens [Dutch Data Protection Act]< http://www.rijksoverheid.nl/documenten-en-publicaties/kamerstukken/2011/12/20/memorie-van-toelichting-wijziging-van-de-wet-bescherming-persoonsgegevens.html >.