Evaluation of the EU Data Protection Regulation

Final report version 1.0

Nieuwegein, 31 May 2013

P.M.H.H. Bex
M.A. Bloemheuvel
S.A. Prij, LL.M.

Version	Date	Status report (nature of the change)
1.0	31 May 2013	Final version of the report

Contents

Summary and conclusions

Introduction

A review of the European Data Protection Directive from 1995 was due in 2012 to bring it into line with advances in technology. After a broad consultation, it was decided to replace the Directive with the European Data Protection Regulation [1]. This report quantifies the impact (in terms of administrative burden and compliance costs[2]) of the Data Protection Regulation on Dutch businesses.

Findings

The total cost to Dutch businesses resulting from the proposed Data Protection Regulation is set out in Table 1. The total cost resulting from the current Dutch Data Protection Act (Wet bescherming persoonsgegevens, "DDPA") is set out in Table 2. It was impossible to quantify the costs associated with several obligations, so it is therefore possible that the actual costs may be higher.

Table 1. Total costs burden resulting from the European Data Protection Regulation.

Type of cost		Low estimate		High estimate
Administrative burden (AB)	€	1,490,532	€	1,490,532
Compliance costs (CC)	€	1,123,998,948	€	1,467,573,948
Total	**€**	**1,125,489,480**	**€**	**1,469,064,480**

The bandwidth used is due to the inherent uncertainty surrounding the documentation obligation in Article 28 of the proposed Data Protection Regulation. There are currently still some unanswered questions about practical implementation of this Article, which introduces the obligation on businesses to maintain records of processing operations on personal data under their responsibility, instead of a general notification to the supervisory authority required by Articles 18 and 19 of Directive 95/46/EC.

Table 2. Total costs resulting from the Dutch Data Protection Act

Type of cost		Costs
Administrative burden (AB)	€	1,726,363
Compliance costs (CC)	€	70,804,716
Total	**€**	**72,531,079**

1 European regulations are the most direct form of legislation by the EU. Regulations are binding on all member states as soon as they are ratified. Regulations are passed either by the Council and the European Parliament acting in concert or by the European Commission. Directives commit member states to achieve a certain outcome, but without stipulating how this should be achieved. Member states must transpose directives into national law by means of Acts of Parliament and delegated legislation.

2 Administrative burden refers to the costs that businesses incur in order to meet the information obligations imposed by legislation and regulations. Compliance costs refer to the costs that businesses incur in order to meet other obligations imposed by legislation and regulations,

Conclusions

- It is clear that the administrative burden resulting from the current law and the proposed Regulation only constitute only a small part of the overall regulatory burden; the compliance costs are significantly higher.
- The administrative burden will reduce slightly when the Data Protection Regulation comes into force, but the compliance costs will increase significantly.
- The total quantifiable impact of the proposed European Data Protection Regulation on the burden felt by Dutch businesses will therefore increase to between €1,052,958,401 (low estimate) and €1,396,533,401 (high estimate).

Evaluation

This study is solely focused on quantifying the impact of the proposed Data Protection Regulation on the administrative burden and compliance costs for Dutch businesses. Other financial effects have not been taken into account in the study.

As described above in relation to Article 28, the proposed Data Protection Regulation leaves some scope for how certain obligations are to be interpreted. It is therefore difficult to estimate in advance which businesses will have to comply and how they will have to comply. Consequently, the resulting cost to businesses cannot be precisely determined, and the study therefore often makes assumptions and suppositions. All assumptions and suppositions used in this report are accounted for and are also set out in the appended Standard Cost Model (SCM)[3].

3 "SCM is a mode that has been developed to quantify the cost of administrative burden.

1 Introduction

With the emergence of social media and the rise of the digital age, people have come to accept the sharing of their personal data on the internet as part of modern life. However, the EU's Eurobarometer of June 2011 shows that around 80% of European citizens who are active internet users feel as though they have lost control of their own personal data.

This is an important indicator that the current national and European rules are no longer fit to guarantee an acceptable level of protection of our personal data. The European Data Protection Directive (95/46/EC)[4] that dates from 1995 has not been brought into line with the fast evolving, increasingly international digital world.

Although the Directive did achieve the introduction of a minimum level of protection across the EU, it also led to large-scale fragmentation as it was transposed into law and interpreted in accordance with the legal regimes of 27 member states. This led to additional costs for businesses active across the entire EU. The Directive was transposed into law in the Netherlands in the Dutch Data Protection Act (Wet bescherming persoonsgegevens, "DDPA").

A review of the European Data Protection Directive from 1995 was due in 2012 to bring it into line with advances in technology. After a broad consultation, it was decided to replace the Directive with the European Data Protection Regulation[5].

The Ministry of Economic Affairs asked SIRA Consulting to make an assessment of the quantitative impact, in terms of administrative burden and compliance costs, that the European Data Protection Regulation will have on Dutch businesses. The findings of the study are set out in this report.

---

4 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, Official Journal L 281. EU Directives commit member states to achieve a certain outcome, but without stipulating how this should be achieved. Member states must transpose directives into national law by means of Acts of Parliament and delegated legislation.

5 (Proposal for a) Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM (2012) 11. European regulations are the most direct form of legislation by the EU. Regulations are binding on all member states as soon as they are ratified. Regulations are passed either by the Council and the European Parliament acting in concert or by the European Commission.

2 Objectives

The objectives of the study, entitled “Evaluation of the EU Data Protection Regulation”, were formulated as follows:

1. Describe the information obligations contained in the European Data Protection Regulation and make a comparison with the current regime.
2. [6]Quantify the identified impact of the proposed legislation and regulation on the administrative burden (AB) and compliance costs (CC) [7] to businesses using the Standard Cost Model (SCM), and compare this with the current situation.
3. Compare the assumptions and the outcomes of the impact assessments made by the Confederation of Netherlands Industry and Employers (VNO-NCW), the United Kingdom and Germany with the outcomes based on the SCM.

6 To calculate the costs of administrative burden for businesses, a method was developed by the former Regulatory Reform Group, and this was described in a manual for defining and measuring the cost of administrative burden (‘Meten is Weten II’, 2008). To calculate the cost of administrative burden, this study used the Standard Cost Model for the Administrative Burden of Businesses'. The original method was developed by SIRA Consulting and others on behalf of the Ministry of Finance.

7 Administrative burden refers to the costs that businesses incur in order to meet the information obligations imposed by legislation and regulations. Compliance costs refer to the costs that businesses incur in order to meet other obligations imposed by legislation and regulations,

3 Method and assumptions

3.1 Method

The project was conducted in four stages, which are explained in the following paragraphs.

Stage 1. Establish the assumptions and conduct a desktop study

In preparation of the study, a considerable part of the data needed for the study was made available by the Ministry of Economic Affairs and the Ministry of Security and Justice. SIRA Consulting analysed this data and adjusted its approach accordingly. These adjustments were primarily related to the processual aspects of the study and establishing the assumptions, rules and documents which form the basis of the study.

Based on the most recent version of the proposed Data Protection Regulation and the consolidated version of the Dutch Data Protection Act, a qualitative description was drafted of the current and proposed regulatory regime. The description includes a summary of the differences between the current obligations and those under the proposed Regulation.

Stage 2. Conduct interviews with policy experts and produce an initial quantification of the costs

The qualitative description of the current and proposed regulatory regime from Stage 1 was then adjusted based on an interview with the Ministry of Security and Justice. In order to make most efficient use of the cost and the available time for the study, the cost impact was initially quantified based on data that was already available. Particularly useful were the cost calculations already performed by VNO-NCW as these offer the best match for the situation in the Netherlands. In conducting the provisional cost calculations, SIRA Consulting processed the data in such a way that the source can be traced and that it is potentially usable in any future studies.

Furthermore, an interview was held with VNO-NCW for further clarification of their own estimate of the cost to Dutch businesses. In the interview, the cost calculations of the VNO-NCW were critically evaluated, and the consequences that these obligations of the Data Protection Regulation would have were checked for correct interpretation. Furthermore, the discussion also covered the sources used by VNO-NCW and what their assumptions and suppositions were. Based on the outcomes of the interview with VNO-NCW, the cost aspects resulting from the proposed Data Protection Regulation and the current regime were adjusted in the provisional cost calculation.

Stage 3. Conduct interviews with implementing experts

In Stage 3, the data taken and the assumptions used were verified with practising professionals. Any missing data was also gathered. The number of interviews in Stage 3 was limited given that as much use as possible was made of specialist expertise in Step 2. Furthermore, during the interviews it was found that many implementing experts could not make an estimate of the costs under either the current regime or the proposed Regulation. Data was therefore only collected from implementing experts who were able to make quantitative estimates of the costs.

Based on the outcomes of the interviews with the implementing experts, the costs included in the cost calculations were adjusted. This completes the calculation of the costs for Dutch businesses. For the sake of comparability of the various results within the project, but also for comparison with other cost calculations, national measurement methods were used to calculate the costs. This study used the Standard Cost Model (SCM). The SCM also offers the advantage that all data in the model can be traced back to the source data and that all calculations made are therefore transparent.

Apart from the quantitative data that is included in the SCM, qualitative data was also discussed during the interviews. All relevant qualitative data has been included in the description of the obligations in Chapter 4 of this report.

Stage 4. Consolidation and final report

In the final stage of the report, the outcomes of the study were presented in this report, which sets out the quantitative and the qualitative impact of the current and the proposed regimes. It also makes a comparison with previously conducted impact assessments.

This report has been discussed with the client. An executive summary of the report and the outcomes of the study are available in Dutch and English.

3.2 Assumptions

A number of assumptions were made for the purposes of the study, and these are accounted for below.

1. AB and CC are calculated in accordance with the SCM

AB refers to the costs that businesses incur in order to meet the information obligations imposed by legislation and regulations. CC refers to the costs that businesses incur in order to meet other obligations imposed by legislation and regulations, including information obligations vis-à-vis third parties outside government circles.

AB and CC were calculated using the SCM method for businesses.

2. Cost calculation only relates to AB and CC

In accordance with the scope of the assignment, the study only focused on quantifying the impact of the proposed Data Protection Regulation on AB and CC for businesses in the Netherlands. Other financial effects have not been taken into account in the study.

3. The study was conducted on the basis of the proposed Regulation as available on 25 January 2012

The study was conducted on the basis of the Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) as it stood on 25 January 2012.[8].

8 COM (2012) 11.

4 Comparison of the obligations

This chapter compares the obligations under the current Dutch Data Protection Act with the obligations that would arise under the proposed European Data Protection Regulation. In doing so, we followed the structure set out in the figure below.

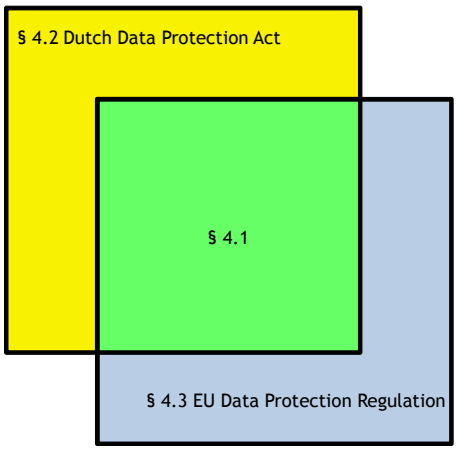

Figure 1. Relationship between the obligations in the current and in the proposed situation.

There are three relevant categories that can be identified:

1. Obligations that apply under the Dutch Data Protection Act and under the Data Protection Regulation (green).
2. Obligations that only apply under the Dutch Data Protection Act (yellow).
3. Obligations that only apply under the Data Protection Regulation.

In each category, the obligations are subdivided into information obligations and other obligations. Information obligations give rise to AB, while other obligations give rise to CC.

4.1 Obligations that apply in the current and in the proposed situation

This section describes the obligations that apply under the current Dutch Data Protection Act (Wet bescherming persoonsgegevens, "DDPA") and under the proposed European Data Protection Regulation ("EDPR"). Businesses already have to comply with obligations in the current regime that more or less correspond with obligations in the proposed Regulation. Some obligations are completely unchanged in the proposed Regulation, while others are slightly changed. Where necessary, an explanation is provided for each obligation. The explanation includes:

- A description of the change to the obligation, where it appears in the Regulation in a modified form.
- Where relevant, the fact that the obligation could not be quantified.
- The assumptions that had to be made to quantify the obligation.

Information obligations that give rise to AB

Art.	Obligation under DDPA	Art.	Obligation under EDPR
23	Request for exception from the prohibition on processing personal data under Article 16	9	Request for exception from the prohibition on processing personal data under Article 9.
Article 9 of the EDPR includes implicit scope for an exception. *The assumption for the calculation is that the number of exceptions will not change because of the EDPR.*			

Art.	Obligation under DDPA	Art.	Obligation under EDPR
25	Applications for recognition of code of conduct	38	Applications for recognition of code of conduct
Applications for recognition of a code of conduct are not compulsory in either the DPA or the EDPR. However, this action has been taken into account in the study because the costs were included in the AB baseline measurement. This ensures that comparability with the AB baseline is retained.			

Art.	Obligation under DDPA	Art.	Obligation under EDPR
32	Notification of data processing to the Dutch Data Processing Authority (CBP) covered by Art. 31 (i)	34	Consultation with supervisory authority prior to personal data processing
The assumption for the calculation is that the list of processing operations which the obligation covers will not change compared to the DDPA.			

Art.	Obligation under DDPA	Art.	Obligation under EDPR
63	Register the data protection officer with the Dutch Data Protection Authority.	35	Communicate name and contact information of the data protection officer
*In the DDPA, **the designation** of a data protection officer is not obligatory. In the EDPR, it is obligatory for certain businesses. The action has been taken into account for both situations as the costs have been included in the AB baseline measurement. This ensures that comparability with the AB baseline is retained.* *The number of times that this action is performed increases in the EDPR. This is because the number of appointments of data protection officers increases, as it will be compulsory for certain businesses.*			

Art.	Obligation under DDPA	Art.	Obligation under EDPR
77	Applications for permission to transfer personal data or to transfer categories of personal data to a third country that does not offer suitable assurances of the level of protection.	34	Apply to the supervisory authority for permission prior to personal data processing
		44	Inform the supervisory authority of transfer in the case of legitimate interests of the data controller or the data processor, including documentation
The costs are comparable, but the EDPR offers businesses more options. For instance, large businesses can draft a binding corporate protocol and submit it for approval so that there is no need to apply for permission. Drafting and submitting such a protocol for approval is not an obligation, however. In the course of time, it is possible that this may lead to a reduction in the number of requests for permission.			

Other obligations that give rise to CC

Art.	Obligation under DDPA	Art.	Obligation under EDPR
13	Assurances of suitable technical and organisational measures to protect personal data from loss or from any other form of unlawful processing.	30	Assurances of an appropriate level of data security
The costs relating to this obligation could not be quantified and furthermore form part of a business's overhead costs. *The obligation in the EDPR is extended to the data processor regardless of their contract with the data controller. For the data processor, this could be a reason to take further security measures, and it is therefore assumed that complying with the obligations of the EDPR could lead to increased costs compared to the DDPA regime.* *The compulsory risk evaluation on which this obligation is based is explicitly mentioned in the EDPR. However, the obligation to carry out a risk evaluation already appears in the DDPA, albeit implicitly. Furthermore, a risk evaluation forms part of a business's overhead costs and these are not taken into account in the study. However, we do note here that the evaluation of a risk (i.e. probability x impact) is traditionally carried out from the perspective of risk to the organisation itself. The EDPR, on the other hand, looks at the issue from the perspective of risk to the personal data and the data subject.*			

Art.	Obligation under DDPA	Art.	Obligation under EDPR
14	Make a contract/legal transaction with the data processor	26	Make contractual arrangements concerning processing operations by the data processor

Art.	Obligation under DDPA	Art.	Obligation under EDPR
31	Cooperate in prior study by the Dutch Data Protection Authority	34	Cooperate with supervision by the supervisory authority

Art.	Obligation under DDPA	Art.	Obligation under EDPR
33-34	Notify the data subject of the identity, purpose of the processing and additional informative (active)	14	Provide the data subject with all information and notices on the processing of personal data (active)
The costs of this obligation could not be quantified. During the study, it was found that businesses are unable to indicate what costs they will incur to comply with this obligation. Similarly, in previous studies it was also impossible to quantify the costs for complying with this obligation. However, the information provision required by the DDPA is less extensive than that required by the EDPR; it is therefore assumed that the costs of complying with the obligation in the EDPR will be higher than under the DDPA.			

Art.	Obligation under DDPA	Art.	Obligation under EDPR
35	Inform the data subject whether personal data is processed and provide data (passive)	12	Inform the data subject of actions following a request to provide information
		15	Provide the data subject with confirmation of whether personal data is processed and provide data (passive)
The costs are comparable. The information provision required by the DDPA is less extensive than that required by the EDPR; it is therefore assumed that the costs of complying with the obligation in the EDPR will be higher than under the DDPA. This increase in cost, however, cannot be quantified. *The assumption for the calculation is that small businesses (less than 200 employees) will have to comply with this requirement once a year, while large businesses (more than 200 employees) will have to comply 10 times a year. This is a conservative estimate.*			

Art.	Obligation under DDPA	Art.	Obligation under EDPR
36	Respond to requests from data subject to change personal data and execute change	12	Inform the data subject of actions following a request to provide information
		16	Rectification or completion of personal data
		17	Erasure and abstention from further dissemination of personal data or restricted processing of data
The costs arising from this obligation could not be separately quantified. In the EDPR, the data controller must, however, conduct further research in order to prevent further dissemination of data (by third parties) (in connection with the right to be forgotten); the assumption is that the costs of complying with this obligation will be higher for the EDPR than under the DDPA regime. *The number of requests to amend or delete personal data depends on the branch of industry. In the financial sector in particular, relatively many requests are submitted, because data subjects are inconvenienced by the processing of their data (e.g. in the context of credit registration).* *In the calculation, the costs for complying with this obligation are deemed to fall within the costs for complying with Article 35 of the DDPA or Articles 12/15 of the EDPR. In practice, businesses combine compliance with both obligations, where relevant. The associated costs are regarded as a single cost item and not two separate cost items.*			

Art.	Obligation under DDPA	Art.	Obligation under EDPR
38	Notifying third parties of personal data changes and informing the data subject	12	Inform the data subject of actions following a request to provide information
		13	Informing the recipients of rectification or erasure of data
The costs arising from this obligation could not be separately quantified. Under the DDPA, the data subject only has to be informed of the notification to third parties if the data subject so requests. Under the EDPR, the data subject must always be informed, and so it is assumed that complying with this obligation from the EDPR will entail greater cost than under the DDPA. *In the calculation, the costs for complying with this obligation are deemed to fall within the costs for complying with Article 35 of the DDPA or Articles 12/15 of the EDPR. In practice, businesses combine compliance with both obligations, where appropriate. The associated costs are regarded as a single cost item and not two separate cost items.*			

Art.	Obligation under DDPA	Art.	Obligation under EDPR
40	Assessing the legitimacy of a data subject's objection	12	Inform the data subject of actions following a request to provide information
		19	Assessing the legitimacy of a data subject's objection
The costs arising from this obligation could not be separately quantified. *In the calculation, the costs for complying with this obligation are deemed to fall within the costs for complying with Article 35 of the DDPA or Articles 12/15 of the EDPR. In practice, businesses combine compliance with both obligations, where relevant. The associated costs are regarded as a single cost item and not two separate cost items.* *There is also a difference between the DDPA and the EDPR in the way a business assesses the legitimacy of an objection. Under the DDPA, a business must first make a generic balance of interests consideration, which is then individualised under Article 40. Under the EDPR, a business must first make a generic balance of interests consideration in accordance with Article 6, which may only be maintained in an objection procedure under Article 19 if the business can demonstrate that it has compelling and legitimate grounds. This means that in the generic consideration of the balance of interests under Article 6, the business must already cite compelling and legitimate grounds for the processing operation because an objection based on Article 19 would otherwise always be upheld.*			

Art.	Obligation under DDPA	Art.	Obligation under EDPR
41	Taking appropriate measures to end data processing and to inform the data subject of the measures taken	12	Inform the data subject of actions following a request to provide information
The costs arising from this obligation could not be separately quantified. *In the calculation, the costs for complying with this obligation are deemed to fall within the costs for complying with Article 35 of the DDPA or Articles 12/15 of the EDPR. In practice, businesses combine compliance with both obligations, where relevant. The associated costs are regarded as a single cost item and not two separate cost items.*			

Art.	Obligation under DDPA	Art.	Obligation under EDPR
41	Take adequate measures to inform data subjects of the option to object to data processing for commercial or charitable purposes	19	Informing the data subject of the option to object when personal data is processed for direct marketing purposes.
The costs arising from this obligation could not be separately quantified. *In the calculation, the costs for complying with this obligation are deemed to fall within the costs for complying with Article 35 of the DDPA or Articles 12/15 of the EDPR.*			

4.2 Obligations that only apply in the current situation

This section describes the obligations that only apply under the Dutch Data Protection Act (DDPA). This relates to obligations that will no longer apply when the proposed Data Protection Regulation (EDPR) comes into force. Where necessary, an explanation is provided for each obligation

Information obligations that give rise to AB

Art.	Obligation under DDPA
27	Report full or partial processing of personal data required for the realisation of a purpose or of various related purposes
By contrast, under Article 28 of the EDPR documents relating to processing operations must be kept.	

Art.	Obligation under DDPA
27	Report full or partial processing of personal data required for the realisation of a purpose or of various related purposes, where this is subject to a prior study.
By contrast, under Article 28 of the EDPR documents relating to processing operations must be kept.	

Art.	Obligation under DDPA
28	Reporting changes to initial report
By contrast, under Article 28 of the EDPR documents relating to processing operations must be kept.	

Other obligations that give rise to CC

Art.	Obligation under DDPA
28	Record non-standard processing operation and keep for three years
By contrast, under Article 28 of the EDPR documents relating to processing operations must be kept.	

Art.	Obligation under DDPA
30	Keep a register of notified data processing operations (including other activities of the data protection officer)
*In the DDPA, **the designation** of a data protection officer is not obligatory. However, this action has been taken into account in the study because the costs were included in the AB baseline measurement. This ensures that comparability with the AB baseline is retained.* *By contrast, under Article 37 of the EDPR, the data protection officer must ensure that documentation on data processing operations is retained. All duties of the data protection officer under the EDPR have of course been included in the calculation of the EDPR effects (under Article 35 of the EDPR).*	

Art.	Obligation under DDPA
30	Provision of information as referred to in Article 28 (1a-e) concerning the notification of exempt data processing operations to anyone who submits a request.

4.3 Obligations that only apply in the proposed situation

This section describes the obligations that would only apply under the proposed European Data Protection Regulation (EDPR). This refers to new obligations compared to the current regime with the Dutch Data Protection Act (DDPA). An explanation is given for each obligation. The explanation includes:

- Where relevant, the fact that the obligation could not be quantified.
- The assumptions that had to be made to quantify the obligation.
- Any remarks from the interviews that are relevant, but not quantifiable.

Information obligations that give rise to AB

Art.	Obligation under EDPR
31	Reporting data protection breaches to the supervisory authority.
The assumption for the calculation is that the number of reports will double compared to the calculation of the costs relating to the proposed Dutch legislation on the duty to report data leaks (wetsvoorstel meldplicht datalekken)[9]. The proposed legislation includes a softer regime for 'minor' breaches, while under the EDPR all breaches must be reported. *Furthermore, only the costs of submitting the report have been taken into account. This ensures that comparability with the calculation of costs for the proposed Dutch legislation on the duty to report data leaks is retained. The study that a business conducts into the cause of a data leak and its solution is not taken into account.*	

Art.	Obligation under EDPR
32	Demonstrate that compromised personal data has been rendered unintelligible.
It is not necessary to report a breach to the data subject if the data controller can demonstrate that protective measures have been taken to the satisfaction of the supervisory authority, and that these measures were applied to the compromised data. These protective measures must ensure that the data is rendered unintelligible for anyone not entitled to access it. A business can demonstrate this to the supervisory authority by registering the data as encrypted or unintelligible. The costs arising from this obligation could not be separately quantified. During the study it was found that businesses are not yet able to estimate the quantitative impact of this future obligation.	

Art.	Obligation under EDPR
34	Provision of a data protection impact assessment to the supervisory authority
The costs arising from this obligation are included with Article 33 of the EDPR.	

Other obligations that give rise to CC

Art.	Obligation under EDPR
12	Establish procedures for provision of information and provision of means to submit requests electronically.
The costs arising from this obligation could not be separately quantified. During the study it was found that businesses are not yet able to estimate the quantitative impact of this future obligation.	

9 As Published by the Ministry of Security and Justice on 20 December 2011 on http://www.internetconsultatie.nl/ and consulted on 29 May 2013.

Art.	Obligation under EDPR
17	Informing the data subject of the ending of restricted data processing
The costs arising from this obligation could not be separately quantified. During the study it was found that businesses are not yet able to estimate the quantitative impact of this future obligation.	

Art.	Obligation under EDPR
17	Establish mechanisms to ensure that the periods established for erasure of personal data or for periodic review of the need to store are observed.
The costs arising from this obligation could not be separately quantified. During the study it was found that businesses are not yet able to estimate the quantitative impact of this future obligation.	

Art.	Obligation under EDPR
18	Provision of copy of data processed and in an electronic and structured format
This obligation assumes that businesses will invest in developing systems so that data subjects can transfer their data in a commonly used electronic format to another automated processing system. The key part of the obligation is contained in paragraph 2. The obligation embodies an implicit right of acceptance for a business responsible for the automated processing system to which the data is transferred. *The assumption for the calculation is that this obligation will in practical application not apply to all businesses. Although the text of the proposed Regulation seems to assume that the obligation will apply to all businesses, the calculation makes an estimate of the businesses that are expected to be faced with the obligation. It is assumed that only businesses of a certain size in the sectors of energy, telecoms, information services, financial services and major retailers will be affected.* *It is also assumed that the number of businesses per sector will be similar to the situation in the United Kingdom, and the calculation therefore makes the assumption that the number of businesses within the stated sectors will be the same as the total number of businesses assumed in the study conducted in the United Kingdom.* *Furthermore, the calculation assumes that the cost for complying with this obligation will be at least €125,000 per business.[10] Respondents indicated that they thought this was a conservative estimate.*	

Art.	Obligation under EDPR
22	Establish policies to ensure and to demonstrate that personal data is processed in compliance with the Regulation.
Establishing policies goes hand in hand with organisational changes, internal coordination and in some cases transition costs. Policies are drafted per system. Complying with this obligation may therefore require a major time investment. However, the costs arising from this obligation could not be quantified. During the study it was found that businesses are not yet able to estimate the quantitative impact of this future obligation. *Furthermore, in the current situation this time is already spent by businesses to ensure compliance with Articles 33 and 34 of the DDPA, which obliges businesses to make a similar effort.*	

Art.	Obligation under EDPR
22	Establish mechanisms to test the effectiveness of the measures referred to in Article 22 (1-2).
Businesses will incur costs from appointing an independent internal or external auditor. This is also the case for drafting an audit plan and conducting monitoring. However, the costs arising from this obligation could not be quantified. During the study it was found that businesses are not yet able to estimate the quantitative impact of this future obligation.	

10 Source: Impact on business of the proposed Data Protection Regulation, www.parliament.uk/documents/commons-vote-office/November_2012/22-11-12/7/-Justice-DataProtection.pdf, Written Ministerial Statement of 22 November 2012, consulted on 29 May 2013.

Art.	Obligation under EDPR
23	Implementing technical and organisational measures, procedures and mechanisms to ensure compliance with the Regulation and to guarantee protection of the data subject's rights

The costs arising from this obligation could not be separately quantified. In the calculation for the EDPR, it is assumed that these costs will overlap with the costs for ensuring compliance with Article 18 of the EDPR, as both obligations require investments in the development of new systems. The investments needed will be treated as a single cost item rather than two separate cost items.

Art.	Obligation under EDPR
28	Keeping documentation on data processing operations

This obligations serves to replace the reporting obligations under sections 27 and 28 of the DDPA. The obligation does not apply to organisations with fewer than 250 employees which process data as an ancillary activity. The term 'ancillary activity' is not clearly defined, which means there is scope for interpretation of the scope of the obligation.

The obligation therefore applies to large businesses and small business that do not process data as an ancillary activity. For the calculation, two scenarios were produced in which an assumption was made for the number of small business that do not process data as an ancillary activity.

The first scenario results in a low estimate: the assumption here is that businesses in the following sectors will not process data as an ancillary activity:

- *Web shops*
- *IT service providers*
- *Information service providers*

The second scenario results in a high estimate: the assumption here is that businesses in the following sectors will not process data as an ancillary activity:

- *Web shops*
- *IT service providers*
- *Information service providers*
- *Telecom businesses*
- *Legal services*
- *Selection and recruitment*
- *Healthcare*

Many other scenarios are, of course, possible. For instance, the term 'ancillary activity' could be interpreted in such a way that it only covers incidental data processing. If data processing is not incidental, but is done to facilitate (and is necessarily integrated with) the core business, then it can no longer be regarded as an ancillary activity. Presumably, the number of businesses processing personal data other than as an ancillary activity would then be even greater than in the second scenario.

Furthermore, it is assumed that small businesses would perform five processing operations and large businesses would perform 50 processing operations per year. This is a conservative estimate.

Art.	Obligation under EDPR
31	Documentation of personal data breach

The assumption for the calculation is that the number of documented cases will double compared to the calculation of the costs relating to the proposed Dutch legislation on the duty to report data leaks (wetsvoorstel meldplicht datalekken). The proposed legislation includes a softer regime for 'minor' transgressions, while under the EDPR all breaches must be documented.

Art.	Obligation under EDPR
32	Communication of a personal data breach to the data subject

In general, it can be said that the chance of data protection breaches is greater in the case of a minor processing operation than for a major processing operation, because the focus within the organisation is likely to be on appropriate security measures in the case of major processing operations compared to minor processing operations.

A single data breach could affect multiple data subjects, meaning that the number of communications to data subjects could be higher than the number of data protection breaches. In theory, the number of data subjects could be many times greater. It is impossible to make a reliable estimate of this in advance.

The assumption for the calculation is therefore that one data subject will be affected for each data protection breach. This ensures that comparability with the calculation of costs for the proposed Dutch legislation on the duty to report data leaks is retained.

Art.	Obligation under EDPR
33	Data protection impact assessment

A data protection impact assessment is compulsory where processing operations present specific risks to the rights and freedoms of the data subject by virtue of their nature, their scope or their purposes. The term 'specific risk' is not clearly defined, which means there is scope for interpretation of the scope of the obligation.

The assumption for the calculation is that small businesses will carry out one data protection impact assessment per year, while large businesses will carry out five; this only relates to businesses that are registered with the Dutch Data Protection Authority. This is a conservative estimate. In some sectors, the number of data protection impact assessments per business may be many times higher.

Furthermore, the text of the Regulation implies that a data protection impact assessment will be preceded by a quick scan, given that it must first be established whether a specific risk is present.

Art.	Obligation under EDPR
35	Designation of a data protection officer

In the DDPA, the designation of a data protection officer is not obligatory. Under the EDPR, the obligation applies where:

a) the processing is carried out by a public authority or body; or
b) the processing is carried out by an enterprise employing 250 persons or more; or
c) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects.

The calculation of the costs arising from this obligation include the costs of the duties carried out by the data protection offers in relation to data protection.

The assumption for the calculation is that in 4% of small businesses, the core activities consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects. These businesses will not designate a permanent data protection officer, but will hire an external party to fulfil the role of a data protection officer. It is assumed that small businesses will hire an external data protection officer for 24 hours per year. This is a conservative estimate.

For large businesses, it is assumed that they will employ one data protection officer. This is a conservative estimate. To avoid duplication, it is assumed that 75% of the work of the data protection officer is already included in the costs of complying with other obligations (such as Article 33). This means that the cost of complying with this obligation is based on 25% of the salary costs of a data protection officer. We note that there are differing views as to the duties of a data protection officer.

Training costs for the data protection officer are then added.

Note that this only refers to the costs of an actual data protection officer. A business will also have to spend time on inducting a data protection officer in the organisation and also on following their instructions.

5 Comparison of administrative burden and compliance costs

This chapter sets out the costs arising under the proposed European Data Protection Regulation as well as under the Dutch Data Protection Act. The costs are calculated using the SCM and originate from the obligations as described in Chapter 4 and the described assumptions. The appended information on the SCM provides further details on how the costs were calculated. It also indicates exactly what the calculated costs are based on for each operation.

5.1 Administrative burden

Table 3 shows the AB originating from the proposed European Data Protection Regulation. Table 4 shows the AB originating from the Dutch Data Protection Act.

Table 3. AB resulting from the European Data Protection Regulation.

Art.	Obligation		Costs
9.	Request for exception from the prohibition on processing personal data under Article 9.	€	87
31.	Reporting data protection breaches to the supervisory authority.	€	982,500
34.	Consultation with supervisory authority prior to personal data processing	€	818
34/44.	Apply to the supervisory authority for permission prior to personal data processing and inform the supervisory authority of transfer in the case of legitimate interests of the data controller or the data processor, including documentation	€	202,500
35.	Communicate name and contact information of the data protection officer	€	254,627
38.	Applications for recognition of code of conduct	€	50,000
Total		**€**	**1,490,532**

Table 4. AB resulting from the Dutch Data Protection Act

Art.	Obligation		Costs
23.	Request for exception from the prohibition on processing personal data under Article 16	€	87
25.	Applications for recognition of code of conduct	€	50,000
32.	Notification of data processing to the Dutch Data Processing Authority covered by Art. 31 (i)	€	818
63.	Register the data protection officer with the Dutch Data Protection Authority.	€	108
77.	Applications for permission to transfer personal data or to transfer categories of personal data to a third country that does not offer suitable assurances of the level of protection.	€	202,500
27.	Report full or partial processing of personal data required for the realisation of a purpose or of various related purposes	€	351,000
28.	Reporting changes to initial report	€	1,121,850
Total		**€**	**1,726,363**

When the European Data Protection Regulation comes into force, the cost of AB for businesses in the Netherlands will reduce from €1,726,363 to €1,490,532 per year.

However, as already described in the preceding chapter, a number of information obligations under the existing Dutch Data Protection Act are covered by the documentation obligation under Article 28 of the European Data Protection Regulation. The costs ensuing from this article actually qualify as CC rather than AL. These costs are therefore included in the next section.

5.2 Compliance costs

Table 5 shows the CC originating from the proposed European Data Protection Regulation. Table 6 shows the CC originating from the Dutch Data Protection Act. It was impossible to quantify the costs associated with several obligations, so it is therefore possible that the actual costs may be higher.

Table 5. CC resulting from the European Data Protection Regulation.

Art.	Obligation		Low estimate		High estimate
15.	Provide the data subject with confirmation of whether personal data is processed and provide data (passive)	€	68,137,500	€	68,137,500
18/23.	Provision of copy of data processed in an electronic and structured format, and implementing technical and organisational measures, procedures and mechanisms to ensure compliance with the Regulation and to guarantee protection of the data subject's rights	€	87,041,235	€	87,041,235
26.	Make contractual arrangements concerning processing operations by the data processor	€	2,543,400	€	2,543,400
28.	Keeping documentation on data processing operations	€	156,337,500	€	499,912,500
31.	Documentation of personal data breach	€	982,500	€	982,500
32.	Communication of a personal data breach to the data subject	€	388,875	€	388,875
33.	Data protection impact assessment	€	471,612,500	€	471,612,500
34.	Cooperate with supervision by the supervisory authority	€	20,438	€	20,438
35.	Designation of a data protection officer	€	336,935,000	€	336,935,000
Total		**€**	**1,123,998,948**	**€**	**1,467,573,948**

Table 6. CC resulting from the Dutch Data Protection Act

Art.	Obligation		Costs
14.	Make a contract/legal transaction with the data processor	€	2,543,400
28.	Record non-standard processing operation and keep for three years	€	13,650
30.	Keep a register of notified data processing operations (including other activities of data protection officer)	€	89,728
31.	Cooperate in prior study by the Dutch Data Protection Authority	€	20,438
35.	Inform the data subject whether personal data is processed and provide data (passive)	€	68,137,500
Total		**€**	**70,804,716**

When the European Data Protection Regulation enters into force, the CC for Dutch business will increase from €70,804,716 to at least €1,123,998,948.

When assuming the second scenario (high estimate) [11] in relation to the documentation obligation under Article 28 of the proposed EDPR, CC increases to €1,467,573,948.

11 See Chapter 4 for a description of the scenarios.

5.3 Summary of results

Table 7 shows the total costs originating from the proposed European Data Protection Regulation. Table 8 shows the total costs originating from the Dutch Data Protection Act. It was impossible to quantify the costs associated with several obligations, so it is therefore possible that the actual costs may be higher.

Table 7. Summary of costs resulting from the European Data Protection Regulation.

Type of cost		Low estimate		High estimate
Administrative burden (AB)	€	1,490,532	€	1,490,532
Compliance costs (CC)	€	1,123,998,948	€	1,467,573,948
Total	**€**	**1,125,489,480**	**€**	**1,469,064,480**

Table 8. Summary of costs resulting from the Dutch Data Protection Act

Type of cost		Costs
Administrative burden (AB)	€	1,726,363
Compliance costs (CC)	€	70,804,716
Total	**€**	**72,531,079**

When the proposed European Data Protection Regulation enters into force, the total cost to Dutch businesses will increase from €72,531,079 to at least €1,125,489,480. The total quantifiable impact of the proposed European Data Protection Regulation on the cost to Dutch businesses is therefore an increase of at least €1,469,064,480.

When assuming the second scenario (high estimate) in relation to the documentation obligation under Article 28 of the proposed EDPR, the total cost increases to €1,469,064,480. The total quantifiable impact of the proposed European Data Protection Regulation on the cost to Dutch businesses is therefore an increase of at least €1,396,533,401.

6 Comparison with other studies

6.1 The impact of the Data Protection Regulation in the EU

The report on the Impact of the Data Protection Regulation in the EU [12] presents the findings of a study into the impact of the proposed European Data Protection Regulation on small and medium-sized businesses (SMEs).

Assumptions

The study that led to the report on the Impact of the Data Protection Regulation in the EU and the Evaluation of the EU Data Protection Regulation both carry out a legal analysis of the obligations (and categories of obligations) contained in the proposed European Data Protection Regulation. In both studies, this analysis formed the basis for the calculation of the costs.

However, there are also some key differences in the assumptions made in the two reports. For instance, in the Impact of the Data Protection Regulation in the EU:

- The study was specifically focused on SMEs and therefore disregarded large businesses.
- A number of specific branches of industry were highlighted. A separate calculation was made for each of these industries.
- The study was concerned with businesses across the entire EU.
- The study was an impact assessment of the European Data Protection Regulation and provides no information on the costs in the current situation.
- The study by the European Commission into the impact of the proposed Data Protection Regulation[13] was taken as the starting point for the calculations. The results of the study were then amended based on a third-party study.

Results

According to the report on the Impact of the Data Protection Regulation in the EU, the cost to an average SME increases by between €3,000 and €7,200 per year, depending on the branch of industry. It was also calculated that these costs represent between 16% and 40% of the annual IT budget of these SMEs. The costs referred to are those directly arising from the Regulation.

Based on these calculations, an estimate is also made of the indirect impact of the proposed European Data Protection Regulation, i.e. its impact on employment growth. It is estimated that the Regulation would have a substantial negative impact on employment growth. This negative impact would be greater in sectors where the direct costs arising from the Regulation are higher, such as sectors where businesses are obliged to designate a data protection officer.

---

12 L. Christensen (Analysis Group, Denver), A. Colciago (University of Milan, Bicocca), F. Etro (Ca' Foscari University, Venice) and G. Rafert (Analysis Group, Denver), 13 February 2013.

13 Impact Assessment, SEC(2012) 72, Commission Staff Working Paper, 25 January 2012.

Difference

The costs calculated in the study that led to the report on the Impact of the Data Protection Regulation in the EU are higher than the costs calculated in the Evaluation of the EU Data Protection Regulation. If the results from the report on the Impact of the Data Protection Regulation in the EU were applied to the Dutch situation, the increase in the cost to the Dutch SME sector would be between €2,607,000,000 and €6,256,800,000 per year. However, the costs for all Dutch businesses increase according to the Evaluation of the EU Data Protection Regulation to between €1,052,958,401 and €1,396,533,401, as set out in Chapter 5.

The aforementioned differences in the assumptions are not the only explanation of the difference in the results. The difference in the results can also be explained by the fact that the study that led to the report on the Impact of the Data Protection Regulation in the EU quantified the impact of more obligations than the Evaluation of the EU Data Protection Regulation did. For instance, it quantified obligations for which the costs were not separately included in the calculations in the Evaluation of the EU Data Protection Regulation. Specifically, this concerns:

- Articles 5, 19 and 20 relating to minimising the processing of personal data and measures based on profiling.
- Article 7 relating to the conditions for consent.
- Article 8 relating to the processing of personal data of a child.
- Article 11 relating to the principle of transparent information and communication.
- Articles 24 and 25 relating to joint data processing controllers and representatives of controllers not established in the EU.

6.2 Impact on business of the proposed Data Protection Regulation

In the report on the Impact on Business of the Proposed Data Protection Regulation [14] the UK's Ministry of Justice sets out the findings of a study into the impact of the proposed Regulation.

Assumptions

Some of the assumptions made by the United Kingdom were also adopted by VNO-NCW, which calculated the costs for businesses in the Netherlands (see § 6.3). Given that the Evaluation of the European Data Protection Regulation also makes some use of the cost calculations of VNO-NCW, some of the assumptions made by the United Kingdom also apply in the Evaluation of the European Data Protection Regulation.

However, there are also some differences in the assumptions made in the UK study and those made in the Evaluation of the EU Data Protection Regulation. For instance, the UK study:

- Only looks at businesses in the United Kingdom.
- The study was an impact assessment of the European Data Protection Regulation and provides no information on the costs in the current situation.
- The study by the European Commission into the impact of the proposed Data Protection Regulation[15] was taken as the starting point for the calculations. The results of the study were then amended based on further research.

Results

According to the UK study, the costs for businesses will increase. The costs were calculated individually for a number of obligations:

- The notification of a personal data breach will cost businesses between €138,000,000 and €375,000,000 per year.
- Designation of a data protection officer will costs the SME sector at least €42,000,000 per year.
- Providing confirmation that personal data is processed and providing data to the data subject will cost businesses between €15,000,000 and €47,000,000 a year more than in the current situation.
- Carrying out data protection impact assessments will cost businesses between €84,000,000 and €170,000,000 per year.
- Provision of a copy of data processed in an electronic and structured format and the data portability that this requires will cost businesses at least €125,000 each. This assumes that the obligation in its practical implementation will only apply to businesses of a certain size in the sectors of energy, telecoms, information services, financial services and major retailers.

---

14 Impact on business of the proposed Data Protection Regulation, www.parliament.uk/documents/commons-vote-office/November_2012/22-11-12/7/-Justice-DataProtection.pdf, Written Ministerial Statement of 22 November 2012, consulted on 29 May 2013.

15 Impact Assessment, SEC(2012) 72, Commission Staff Working Paper, 25 January 2012.

Difference

As already stated above, the assumptions made in the UK study do not entirely match the assumptions made in the Evaluation of the EU Data Protection Regulation. This leads to a discrepancy in the calculated results. Furthermore, the calculations of the individual obligations make a number of assumptions that do not match the assumptions made in the Evaluation of the European Data Protection Regulation. Specifically, these are:

- The costs incurred for reporting a personal data breach also include the costs for the study that a business conducts into the cause of a data breach. In the Evaluation of the EU Data Protection Regulation, these costs are disregarded and only the costs of submitting the report have been taken into account.
- The work activities of a data protection officer will cost every SME four hours a year. In the Evaluation of the EU Data Protection Regulation, an assumption of 24 hours a year is made.
- The change meaning it is no longer possible for a data controller to charge a fee for providing confirmation that personal data is processed will lead to an increase in the number of requests of between 25% and 40%. The Evaluation of the EU Data Protection Regulation assumes that the loss of the option to charge a fee will not lead to an increase in the number of requests.
- Data protection impact assessments are already carried out by 89% of large businesses and 74% of small businesses. The impact of this obligation is therefore only calculated for 11% of large businesses and 26% of small business that do not yet carry out data protection impact assessments. The Evaluation of the EU Data Protection Regulation assumes that almost all large businesses and all small businesses do not yet carry out data protection impact assessments.

The UK included the cost of fines in the study. These were estimated at between €78,000,000 and €466,000,000. In the Evaluation of the EU Data Protection Regulation, these costs were not included because it was assumed that the rules would be complied with by all businesses.

The UK study does not include the costs relating to a number of obligations that were calculated in the Evaluation of the EU Data Protection Regulation. For instance, the costs arising from the data processing documentation obligation are not taken into account. In the Evaluation of the EU Data Protection Regulation these costs were estimated at between €156,337,500 and €499,912,500. The cost to large businesses for designating a data protection officer were not included in the UK calculations.

6.3 Rough estimate of DPR cost to Dutch business

In the report entitled 'Rough estimate of DPR cost to Dutch business', [16]VNO-NCW presents its findings on the impact on the proposed Data Protection Regulation.

Assumptions

As the Evaluation of the EU Data Protection Regulation makes use of some aspects of the cost calculations by VNO-NCW, the assumptions made in the two studies have a degree of overlap.

However, there are also some differences in the assumptions made in the VNO-NCW study and the Evaluation of the EU Data Protection Regulation. For instance, the VNO-NCW study:

- The study was a cost assessment of the European Data Protection Regulation and provides no information on the costs in the current situation.
- The UK study into the impact of the proposed Data Protection Regulation was taken as the starting point for the calculations. The results of the study were then amended based on further research.

Results

According to the report by VNO-NCW, the cost to Dutch industry would be between €1,294,789,300 and €3,733,697,500. The costs were calculated for a number of obligations:

- The notification of a personal data breach will cost businesses between €270,812,000 and €829,895,000 per year when all breaches have to be reported, and between €14,911,800 and €45,696,750 per year when only breaches that present a high risk to the data subject must be reported.
- Designation of a data protection officer will cost businesses between €331,010,000 and €801,060,000 per year.
- Provision of a copy of data processed in an electronic and structured format, and the data portability that this requires will cost businesses at least €130,942,500. This assumes that the obligation in its practical implementation will only apply to businesses of a certain size in the sectors of energy, telecoms, information services, financial services and major retailers. It is also assumed that the number of businesses per sector will be similar to the situation in the United Kingdom. and the calculation therefore makes the assumption that the number of businesses within the stated sectors will be the same as the total number of businesses assumed in the study conducted in the United Kingdom.
- Confirming whether personal data is processed and providing data to the data subject will cost businesses €68,137,500 per year.
- Carrying out data protection impact assessments will cost businesses €471,612,500 per year.
- Keeping documentation on data processing operations will cost businesses €1,362,750,000 per year if all operations have to be documented, and €266,625,000 per year if all operations that present a high risk to the data subject have to be documented.

Furthermore, businesses will have to pay fines of €11,550,000 per year or €69,300,000 per year, depending on the question of whether the turnover of micro businesses is included in the turnover of all businesses.

---

16 Informal document prepared by VNO-NCW.

Difference

The costs calculated in the VNO-NCW study are higher than those calculated in the Evaluation of the EU Data Protection Regulation. According to the report by VNO-NCW, the cost to Dutch industry of the proposed Data Protection Regulation would be between €1,294,789,300 and €3,733,697,500. As indicated in Chapter 5, however, the costs according to the Evaluation of the EU Data Protection Regulation would be between €1,125,489,480 and €1,469,064,480.

The difference in the results can be explained by the fact that VNO-NCW's calculations of the individual obligations made assumptions that do not correspond with the assumptions made in the Evaluation of the EU Data Protection Regulation. Specifically, these are:

- The costs incurred for reporting a personal data breach also include the costs for the study that a business conducts into the cause of a data breach. In the Evaluation of the EU Data Protection Regulation, these costs are disregarded and only the costs of submitting the report have been taken into account.
- The work activities of a data protection officer will cost every SME between 4 and 24 hours a year. A large business will have to hire a data protection officer (0.75 to 1.5 FTE) on a salary of €100,000 per year. The Evaluation of the EU Data Protection Regulation assumes that the work activities of a data protection officer will cost every SME 24 hours a year. It also assumes that a large business will have to hire one data protection officer on a salary of €100,000 per year. However, 75% of this salary has already been discounted in the obligations already quantified. The calculations are therefore based on 25% of €100,000 per year. However, the annual training expenditure has been added to this figure.
- The obligation to provide a copy of data processed in an electronic and structured format and the data portability that this require will apply to 0.1% of all businesses, given that the obligation in the UK also applies to 0.1% of all businesses. This means that the obligation will apply to 873 businesses in the Netherlands. The cost will be €150,000 per business. The Evaluation of the EU Data Protection Regulation assumes that the obligation will apply to 0.07976% of all businesses, given that the obligation in the UK also applies to 0.07976% of all businesses. This means that the obligation will apply to 696 businesses in the Netherlands. The cost will be at least €125,000 per business, although it must be borne in mind that the actual cost could be greater than this.
- The obligation to keep documentation on data processing operations applies to all businesses. Small businesses will carry out five data processing operations per year, while large businesses will carry out 50. If only processing operations that present a high risk to the data subject have to be documented, the obligation will apply to one processing operation per small business and five processing operations per large business. The Evaluation of the EU Data Protection Regulation assumes that the obligation to keep documentation on data processing operations will not apply to businesses with less than 250 employees as long as data processing is an ancillary activity. Two scenarios have been produced for the number of small businesses that process personal data other than as an ancillary activity. It is also assumed that all processing operations must be documented and not just processing operations that expose the data subject to a high risk.

VNO-NCW has included the cost of fines in the study. These are estimated at either €11,500,000 per year or €69,300,000 per year, depending on whether the turnover of micro business is included or not. In the Evaluation of the EU Data Protection Regulation, these costs were not included because it was assumed that the rules would be complied with by all businesses.

The study by VNO-NCW does not include costs arising from a number of obligations that were taken into account in the Evaluation of the EU Data Protection Regulation. For instance, the costs arising from the obligation to record the performance of data processing operations by a data processor in a contract/legal transaction. Furthermore, the costs arising from a number of information obligations have not been taken into account.