Dutch Data Protection Authority

The data breach notification obligation as laid down in the Dutch Data Protection Act

Policy rules for the application of article 34a under the Dutch Data Protection Act

DATE 8 December 2015

INDEX

SUMMARY

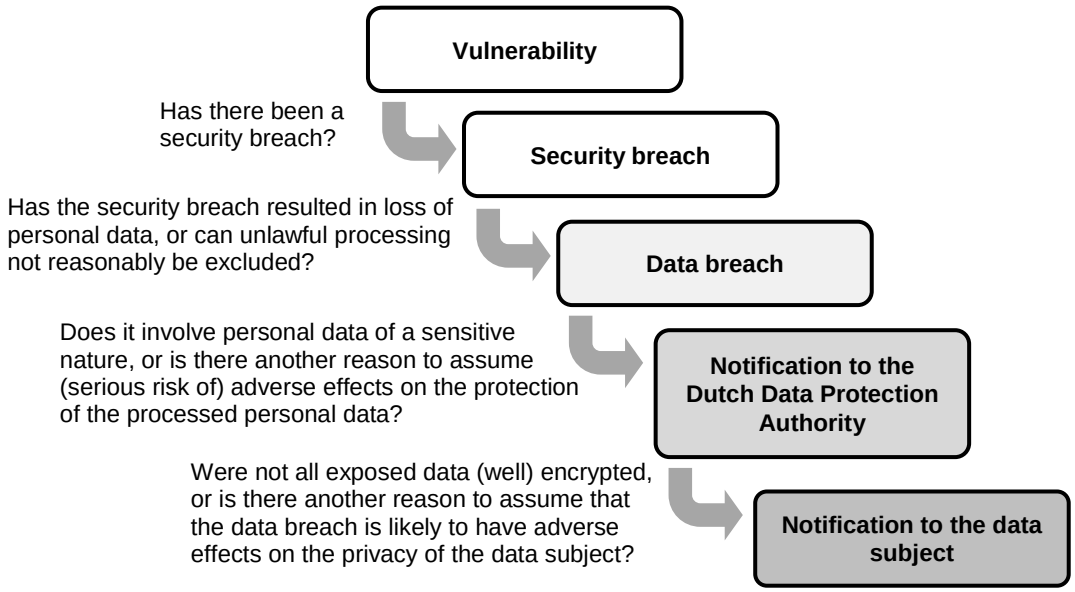
On 1 January 2016, the data breach notification obligation will enter into force. This obligation means that organisations (companies as well as governments) must immediately notify the Dutch Data Protection Authority as soon as they experience a serious data breach. And in some cases, they must also report the data breach to the data subjects (the persons whose personal data have been affected).

Framework

Everyone is entitled to respect for and protection of his privacy and careful handling of his or her personal data. The corresponding rules are set out in the Personal Data Protection Act (Dutch Data Protection Act). It states that you must protect the personal data you process against loss and unlawful processing (article 13 Dutch Data Protection Act). A data breach must be reported to the Dutch Data Protection Authority if it leads to a considerable likelihood of serious adverse effects on the protection of personal data, or if it has serious adverse effects on the protection of personal data (article 34a, paragraph 1, Dutch Data Protection Act). The data breach must also be reported to the data subjects if it is likely to adversely affect their privacy (article 34a, paragraph 2, Dutch Data Protection Act).

Considerations

When deciding whether the Dutch Data Protection Authority must be notified of a certain incident, and possibly the data subjects as well, a number of comparative assessments must be made.



Data breach

One can only speak of a data breach when an actual security breach has occurred. A security breach may be, for example, the loss of a USB-key, the theft of a laptop or the intrusion by a hacker.

However, not every security breach is also a data breach. A security breach is considered to be a data breach if it involves the loss of personal data, or if unlawful processing of personal data cannot reasonably be excluded.

If there is only a weak spot in security, we speak of a vulnerability and not of a data breach and there is no need for you to notify the Dutch Data Protection Authority.

Notification to the Dutch Data Protection Authority

There is no need to notify the Dutch Data Protection Authority of every single data breach. By law, you are required to notify the Dutch Data Protection Authority if the data breach leads to a considerable likelihood of serious adverse effects on the protection of personal data, or if it has serious adverse effects on the protection of personal data.

One of the factors that play a role here is the nature of the exposed personal data. If these concern personal data of a sensitive nature, then in general a notification is required. With regard to personal data of a sensitive nature you should think of:

- *Special personal data as provided in article 16 Dutch Data Protection Act*
  This includes personal data about a person's religion or belief, race, political opinions, health, sexual life, membership of a trade union, as well as criminal personal data and personal data relating to unlawful or objectionable behaviour in connection with a restraining order imposed in connection with such behaviour.
- *Data about the financial or economic situation of the data subject*
  This includes for example data on (problematic) debts, salary or payments details.
- *(Other) data which may lead to stigmatisation or exclusion of the person concerned*
  This includes for example data on gambling addiction, performances at school or at work or relational problems.
- *User names, passwords and other login details*
  The possible impact on the data subjects will depend on the data processing and the nature of the personal data that these login details give access to. When assessing the impact one should consider that many people reuse passwords for different applications.
- *Data which can be misused for (identity) fraud*
  This includes biometric data, copies of identity documents and the Citizens Service Number (CSN).

Other factors, such as the amount of exposed personal data per person or the number of data subjects whose personal data have been affected, may be a reason to report the data breach. But beware: if the nature of the exposed data give cause to do so, it is

possible that you are required to report a data breach where the personal data of only one person are involved.
You need to report the data breach without undue delay and if possible not later than 72 hours after the discovery of the data breach. For this purpose, a web form is available on the website of the Dutch Data Protection Authority. With this web form you can supplement or withdraw your notification as appropriate.

Notification to the data subject

If you come to the conclusion that you need to report a data breach to the Dutch Data Protection Authority, this does not necessarily mean that you must also notify the data subject of the data breach. You will need to make a separate assessment.

The law states that you must notify the data subject if the data breach is likely to affect the privacy of the person concerned. The interests of those involved may be harmed by the loss, unlawful use or misuse of the data. In this respect you should think of unauthorised publication, defamation of character, (identity) fraud or discrimination. If personal data of a sensitive nature have been exposed, you can basically assume that you should not only report the data breach to the Dutch Data Protection Authority, but also to the data subject.

Your notification allows the data subjects to be alert to the possible consequences of the data breach and to guard themselves against it by, for example, replacing their passwords. The law requires that you must report the data breach *without delay*. You have to take into account the fact that as a result of your notification, the data subject will possibly have to take measures to protect himself against the consequences of the data breach. The sooner you inform the person, the sooner he can take action.

If you have taken appropriate technical protective measures making the personal data concerned incomprehensible or inaccessible to unauthorised persons, then you may omit the notification to the data subject. Protective measures could include for example cryptographic processing such as encryption and hashing. You need to decide case by case whether the measures you have taken offer sufficient protection to omit the notification of the data breach to the data subject.

Exception to the notification obligation

The notification obligation as laid down in the Dutch Data Protection Act does not apply if the Dutch Data Protection Act does not apply. This may be the case, for example, if you process data exclusively for personal or household purposes.

If you are a provider of a public electronic communication service, you have to deal with two notification obligations for data breaches: the obligation under the Telecommunication Act (TA) and the obligation under the Dutch Data Protection Act. In case a data breach (partially) falls under the notification obligation in the TA then you need to report the data breach to the Dutch Data Protection Authority and possibly to the data subject as well. The Dutch Data Protection Act includes provisions to avoid double notification.

If you are a financial institution as referred to in the Financial Supervision Act (FSA), then the obligation under the Dutch Data Protection Act to report data breaches to the data subject does not apply to you. If you inform the party concerned, you do so based on your obligation as a financial institution.

Penalty

In case of violation of the data breach notification obligation as referred to in the Dutch Data Protection Act, the Dutch Data Protection Authority may impose an administrative penalty. This administrative penalty shall not exceed the amount mentioned in category six of article 23, paragraph 4, of the Dutch Criminal Code. As from 1 January 2016, this is the maximum amount of € 820,000.[1] If the violation was not deliberate and there is no serious culpable negligence, the Dutch Data Protection Authority will only impose binding instructions prior to any imposition of an administrative penalty. When imposing an administrative penalty, the Dutch Data Protection Authority will take into account all circumstances surrounding the case. A circumstance can consist of the fact that third parties have not been offered the opportunity to view the data concerned.

[1] The amounts in article 23, paragraph 4, of the Dutch Criminal Code are adjusted every two years to the developments of the consumer price index. This means that as from 1 January 2018, a different amount may apply.

INTRODUCTION

As from 1 January 2016, an amendment of the Dutch Data Protection Act, which regulates the notification obligation for data breaches, will take effect. This notification obligation means that companies, governments and other organisations that process data must report data breaches to the Dutch Data Protection Authority, and in certain cases to the data subject as well. The data subject is the person or party whose data have been affected by the data breach.

The companies, governments and other organisations to whom the notification obligation applies must make a reasoned assessment of whether an actual data breach which is brought to their attention falls within the scope of the legal notification obligation. The aim of this policy is to support them in this respect.[2] These policies also serve as a basis for the Dutch Data Protection Authority in the application of enforcement measures.

These policy rules address the data breach notification obligation which is included in the Dutch Data Protection Act. Providers of public electronic communication services have to deal with two notification obligations for data breaches: the current obligation and the already longer existing data breach notification obligation which is included in the Telecommunication Act (TA). The data breach notification obligation in the TA emanates from European Regulations, and European Regulation 611/2013 elaborates on the rules related to this obligation. Among others this Regulation states the time limit for notification of a data breach to the competent national authority, which information must be provided and how the data subject must be informed about the data breach. Furthermore, the notification obligation to the data subject has been specified by the cooperating European data protection authorities which has resulted in a recommendation that includes extended annotated examples.[3] These policy rules do not substantively focus on the notification obligation referred to in the TA, although, where possible they relate to the existing interpretation of this notification obligation.

These policy rules will take effect on 1 January 2016, being the effective date of the data breach notification obligation.

In the course of 2017, or when the number of notifications gives cause to do so, the policy rules will be reviewed and adjusted where necessary. In addition, another consultation will take place around that time.

More information about the security of personal data and the data breach notification obligation is available on the website of the Dutch Data Protection Authority.[4]

---

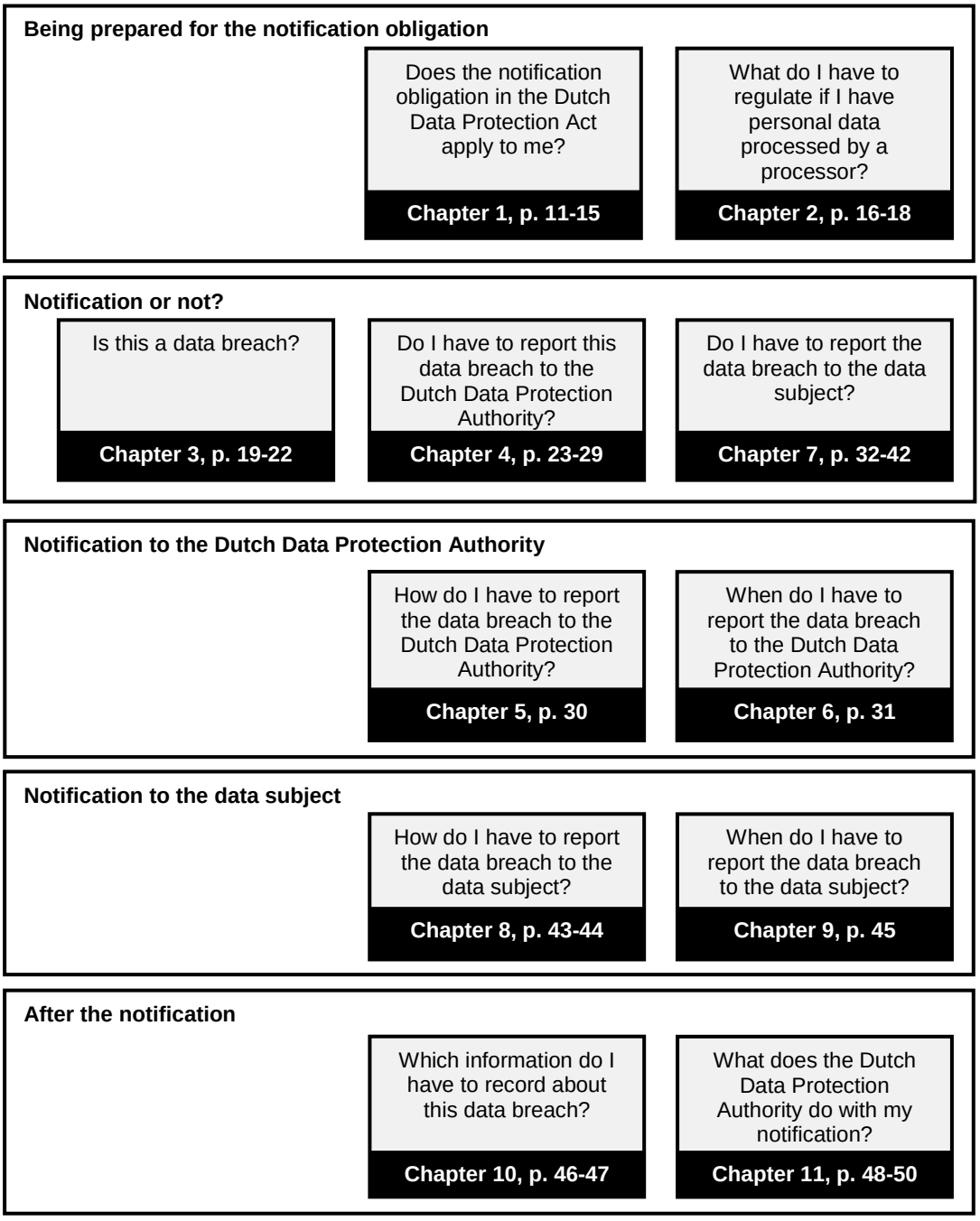
[2] Parliamentary Documents II 2014/15, 33 662, no. 11 , p. 2.

[3] Article 29-Working group, Advice 03/2014 about notification in case of intrusions connected with personal data, approved on 25 March 2014.

[4] Autoriteitpersoonsgegevens.nl.

READING GUIDE

The diagram below shows, for each subject, the relevant sections in these policy rules.

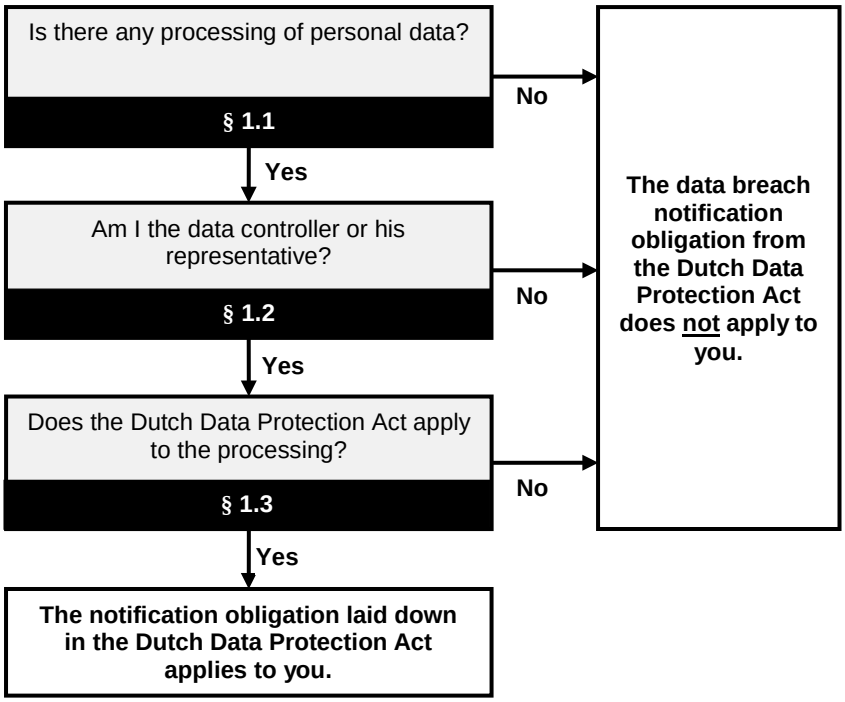


In addition to the elements shown in the diagram above, these policy rules contain a number of appendices. In appendix 1 to these policy rules, you will find a summary of the data you must provide in the notification. Appendix 2 shows the full text of the law articles that are referred to in this policy.

Where these policy rules mention the 'notification obligation under the Dutch Data Protection Act', reference is made to the data breach notification obligation which is included in article 34a Dutch Data Protection Act and to which reference is made in article 14 Dutch Data Protection Act, and not to the notification obligation for processing personal data as laid down in articles 27, 28, 29 and 30 Dutch Data Protection Act.

1. DOES THE DATA BREACH NOTIFICATION OBLIGATION FROM THE DUTCH DATA PROTECTION ACT APPLY TO ME?

The diagram below illustrates the questions you must answer in order to determine whether the data breach notification obligation from the Dutch Data Protection Act applies to you. Every question in the diagram corresponds to a paragraph in the remainder of this chapter.



This chapter discusses concepts such as 'personal data', 'processing' and 'responsible'. These terms from the Dutch Data Protection Act are briefly explained in the following paragraphs. More information about the Dutch Data Protection Act and about the meaning of these terms can be found on the website of the Dutch Data Protection Authority.[5]

1.1. Is there any processing of personal data?

In case there is no processing of personal data, the data breach notification obligation is not applicable.

'Personal data' means any information relating to an identified or identifiable individual (article 1, under a, Dutch Data Protection Act). A person is identifiable if his identity can reasonably be established, without disproportionate effort. A distinction can be made between directly and indirectly identifying data. Directly identifying data are data relating to a person whose identity can be established unambiguously and rather easily, such as the person's name, possibly in combination with the address and date of birth. We speak about indirectly identifiable data when these data may be linked to a particular person after having taken additional steps.

[5] Autoriteitpersoonsgegevens.nl.

Data are not personal data if effective, technical and organisational measures have been taken by which an actual identification of individual natural persons can reasonably be excluded (anonymisation).

The application of cryptographic processing such as encryption or hashing of identifying data leads to pseudonymisation (replacing an identifier with another identifier) but not to anonymisation. An example of such processing is the encryption or hashing of customer numbers. As the controller you are still capable of identifying the individual, even after the encryption or hashing. So we can still speak of personal data. However, pseudonymisation is a valuable security measure which can significantly decrease the risk of actual abuse of exposed data in case of a data breach.

Removing directly identifiable data does not, in itself, offer sufficient guarantee that these are no longer considered to be personal data. After all, by means of spontaneous recognition, comparison of data and/or linkage with data from another source, identification may nevertheless be accomplished, and even sometimes without extra effort. Furthermore, in case of anonymisation, the latest technical developments should be taken into account. Data which can be considered anonymous by certain technical standards – since the data cannot reasonably be traced back to a single person – can still become personal data as a result of increased possibilities created by technical developments.

Processing of personal data concerns any operation or set of operations with regard to personal data. This includes in any case the collection, recording, organisation, safeguarding, adaptation, alteration, retrieving, consulting, use, providing by means of transmission, distribution or otherwise making available, bringing together as well as shielding, deleting or destroying of data (article 1, paragraph b, Dutch Data Protection Act).

1.2. Am I the data controller or his representative?

The data breach notification obligation addresses itself to the party who is responsible for the processing of personal data.

The controller is the one who, alone or jointly with others, determines the purpose of and the means for the processing of personal data (article 1, paragraph d, Dutch Data Protection Act). This concerns the question of who ultimately decides what processing takes place of which personal data and for what purpose. Another important factor is who decides on the means used for this data processing: the question of how the data processing should take place. Sometimes, these competences may be in different hands, in which case we speak about shared responsibility.

If a controller from outside the European Union processes personal data and the Dutch Data Protection Act is applicable to this processing, the controller in the Netherlands must appoint a person or body who fulfils the obligations from the Dutch

Data Protection Act on his behalf. For the purposes of the Dutch Data Protection Act and the provisions based thereon, this person or body shall be considered to be the controller.

1.3. Does the Dutch Data Protection Act apply to the data processing?

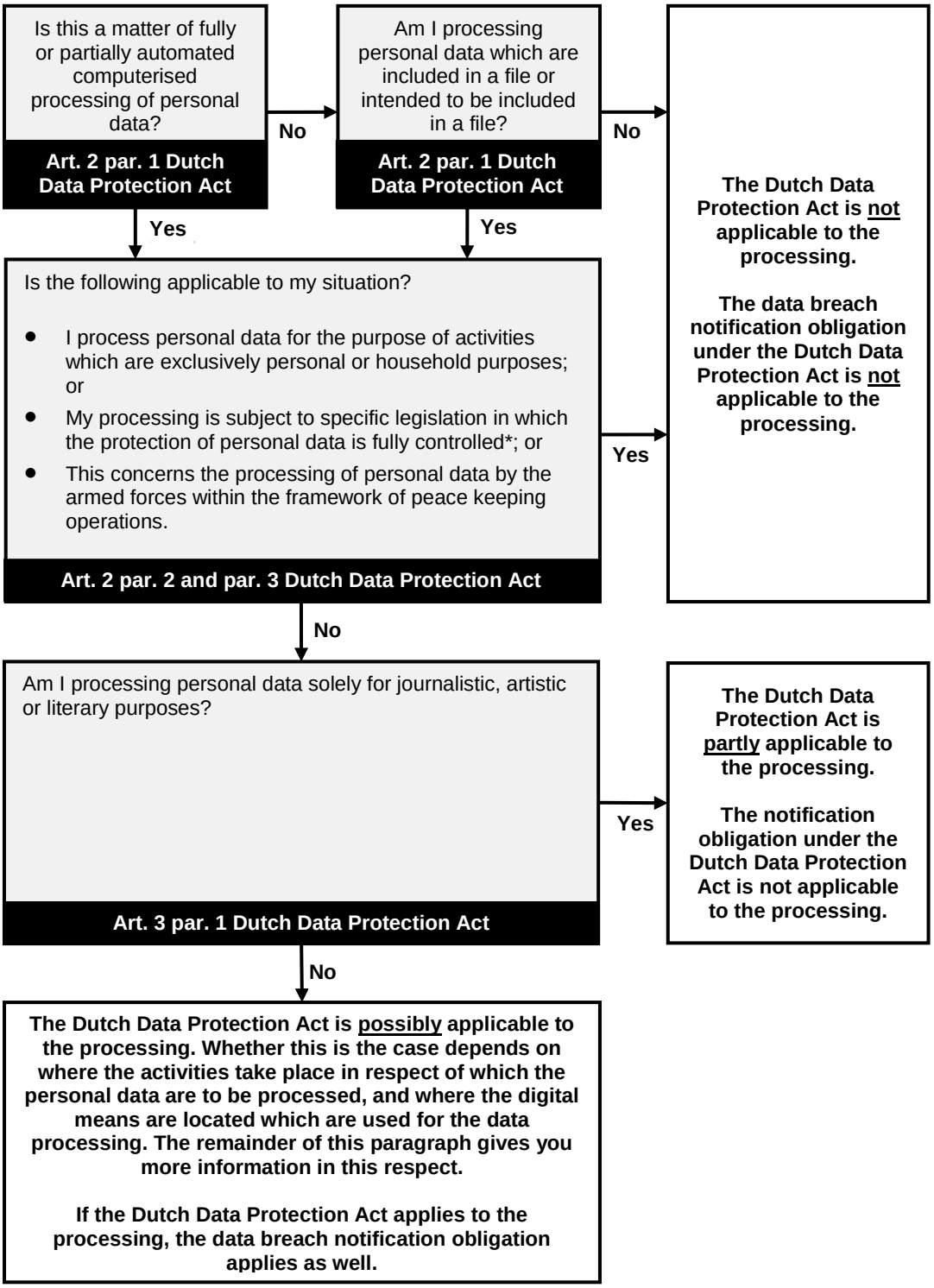
The data breach notification obligation as laid down in the Dutch Data Protection Act solely applies to the processing to which the Dutch Data Protection Act is applicable.

As to the question whether the Dutch Data Protection Act applies to the processing of personal data, two elements are essential. First, you will have to look at the nature and the purpose of the processing. By their nature or purpose, certain processing operations fall outside the scope of the Dutch Data Protection Act, and with regard to these operations the data breach notification obligation does not apply. Secondly, it is important where the activities related to the personal data that are to be processed actually take place, and where the digital means are located which are used for the data processing. Possibly the privacy laws of another European country are applicable to the processing or the processing is not governed by European privacy laws. In these situations, the data breach notification obligation under the Dutch Data Protection Act is not applicable either.

The two diagrams in the remainder of this paragraph explain the above in more detail. In both diagrams you will find, for each section, a reference to the relevant article from the Dutch Data Protection Act. More information about these articles can be found in the Dutch Data Protection Act-reference on the website of the Dutch Data Protection Authority.[6]

[6] Autoriteitpersoonsgegevens.nl.

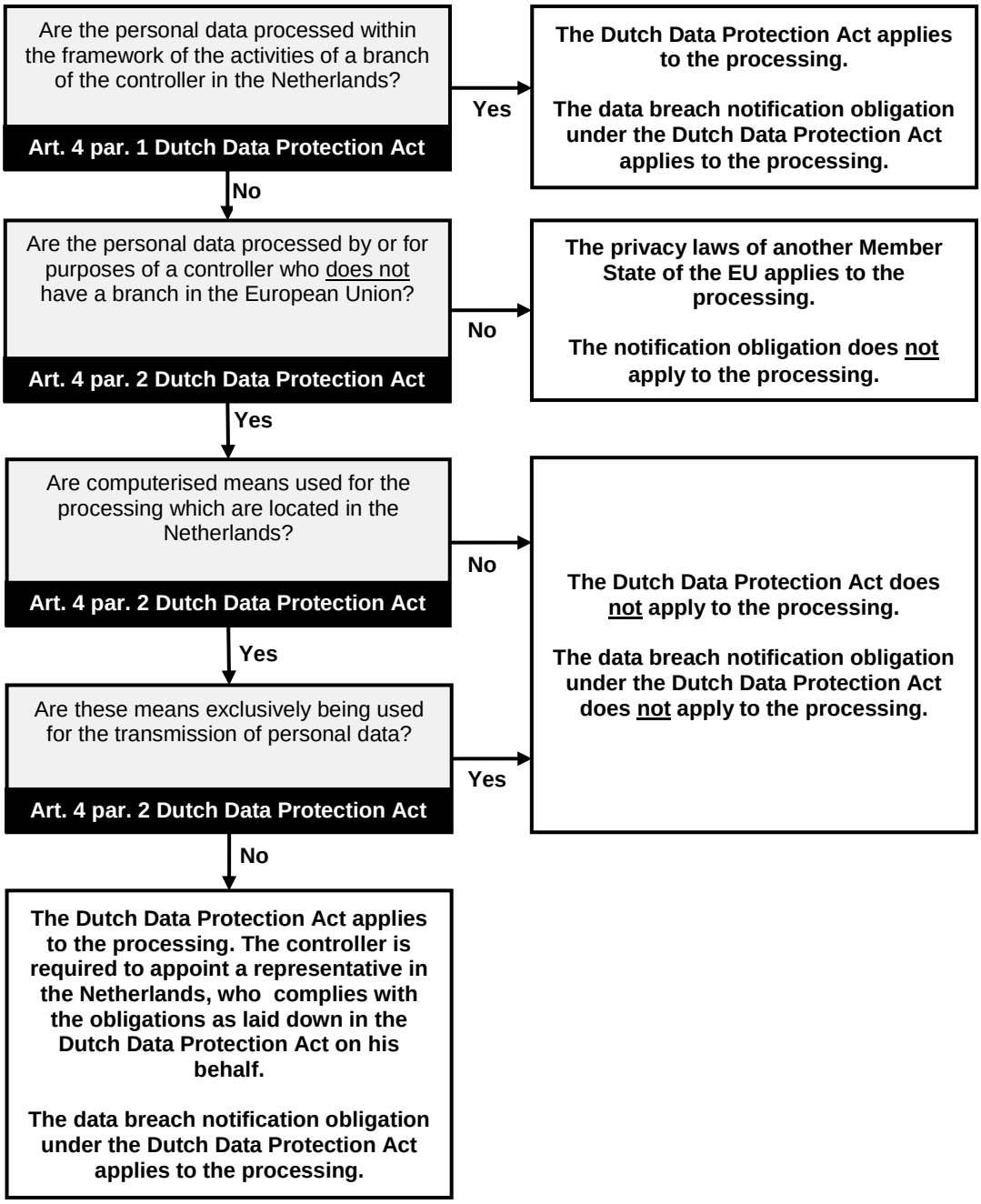
The diagram below provides a guide to the first element: the assessment based on the nature and purpose of the processing.



*) Paragraph 2 of article 2 Dutch Data Protection Act contains a full listing of these laws.

For processing not covered by the exceptions listed above it is also important where the activities related to the personal data that are to be processed actually take place

and where the digital means are located which are used for the processing. The diagram below explains this in more detail.



An example of a situation in which the data breach notification obligation does not apply to the processing of personal data in the Netherlands[7]

An organisation based in France which does not have a branch in the Netherlands has personal data processed by a company in the Netherlands. Since the controller of the processing is located in another European country, the Dutch Data Protection Act does not apply to the processing and a potential data breach does not need to be reported to the Dutch Data Protection Authority.

[7] Parliamentary Documents II, 2013/14, no. 6, p. 15.

2. WHAT AGREEMENTS DO I HAVE TO MAKE IF I HAVE PERSONAL DATA PROCESSED BY ANOTHER PROCESSOR?

Many controllers have the processing of their personal data wholly or partly executed by a so called processor. A processor processes personal data for the data controller without being subjected to the direct authority of the controller (article 1, par. e, Dutch Data Protection Act). For example, processing by a processor occurs when personal data are processed in the cloud, or external hosting of a website on which personal data are processed. This chapter answers the question as to what agreements you have to make if the data breach notification obligation as laid down in the Dutch Data Protection Act applies to you, and you hire a processor for the processing of personal data. If you still do not know whether the data breach notification obligation applies to you, go through the questions from chapter 1 first.

2.1. Why is it important to make the proper agreements?

If you have personal data processed by a processor, you have to make sure that this processor offers sufficient guarantees with regard to compliance with the data breach notification obligation. You must monitor compliance (article 14, paragraph 1, Dutch Data Protection Act).

You must see to it that the processor takes the steps that are necessary to enable you to comply with the data breach notification obligation (article 14, paragraph 3 under c, Dutch Data Protection Act).

In many cases the processor is the first one to become aware of a data breach. Your duty, as the controller for the processing, explicitly covers the data breach recognised by the processor. This means that you must ensure, even if you have personal data processed by a processor, that you are able to comply with your legal obligations. In any case, make sure that the processor informs you timely and adequately about the data breach of which he becomes aware.

If the actual situation occurs, you may agree with the data processor that in case of a data breach, he will notify the Dutch Data Protection Authority first. One condition, based on the agreements you made with the processor, is that he is able to recognise in which case a notification to the Dutch Data Protection Authority is necessary. Being the controller, you will still be ultimately responsible for the notification in this case. This means that you must make sure that the processor keeps you informed of his notification of a data breach to the Dutch Data Protection Authority.

2.2. Which agreements do I have to make with the processor?

Apart from ensuring compliance by the processor, as discussed in the preceding chapter, the law does not dictate what exactly you have to agree upon with the processor. You should at least consider the following:

- Will the processor actually inform you about all the relevant incidents?
- Will the processor himself notify the Dutch Data Protection Authority if relevant?

- Will you get all the necessary information about each incident?
- How will the processor inform you about the incidents?
- Will you be informed timely about the incidents?
- Will you be kept informed about possible new developments surrounding the incident, and the measures taken by the processor to limit the consequences of the incident on his side and to prevent any reoccurrence?
- Will you be able to establish whether you are actually kept informed about all relevant incidents, and whether the information provided is correct?

The Dutch Data Protection Act obliges you to ensure sufficient protection for the personal data that you process, even when you have hired a processor to do the job. Adequate security measures carried out by the processor are important in several respects for compliance with the data breach notification obligation. Firstly, adequate security provides an important contribution to the prevention of data breaches. Secondly, measures such as *intrusion detection* enable the processor to timely recognise (possible) unauthorised access to personal data and to inform you about them. More information about the security of personal data when processed by a processor can be found in the guidelines *Protection of personal data* of the Dutch Data Protection Authority.[8]

Although as the controller you are responsible and liable for the data processing by a processor (see article 12 Dutch Data Protection Act), the processor also bears rights and obligations. He does not only need to follow the instructions from the controller, but he is also independently liable for compliance with the principles relating to the processing of personal data referred to in chapter 1 and 2 of the Dutch Data Protection Act.[9]

2.3. How do I record the agreements I make with the processor?

The agreements you make with the processor may be recorded in writing or in another equivalent form (article 14, paragraph 5, Dutch Data Protection Act). An oral agreement between you as the controller and the processor is not sufficient.

2.4. What if I hire a processor abroad?

For the data breach notification obligation the location of the processor is not relevant. In addition, data breaches which occur at the location of a foreign processor (in another EU Member State or in a country outside of the EU) must be reported to the Dutch Data Protection Authority. In this respect, all that has been referred to in the preceding paragraphs is applicable.

[8] Autoriteitpersoonsgegevens.nl.

[9] Parliamentary Documents II, 1997/98, 25 892, no. 3, p. 61. Also see: CBP, Investigation into the security of Humannet Starter and Humannet Omission by VCD Humannet B.V., z2012-00288, Report of final findings of December 2014.

Example of a data breach notification obligation that applies to data processing in a foreign country[10]

An organisation located in the Netherlands has data processed by a company in France. The personal data are stored in a server in France. If unauthorised persons gain access to these data, this falls under the data breach notification obligation as laid down in the Dutch Data Protection Act and it must be reported by the Dutch controller to the Dutch Data Protection Authority.

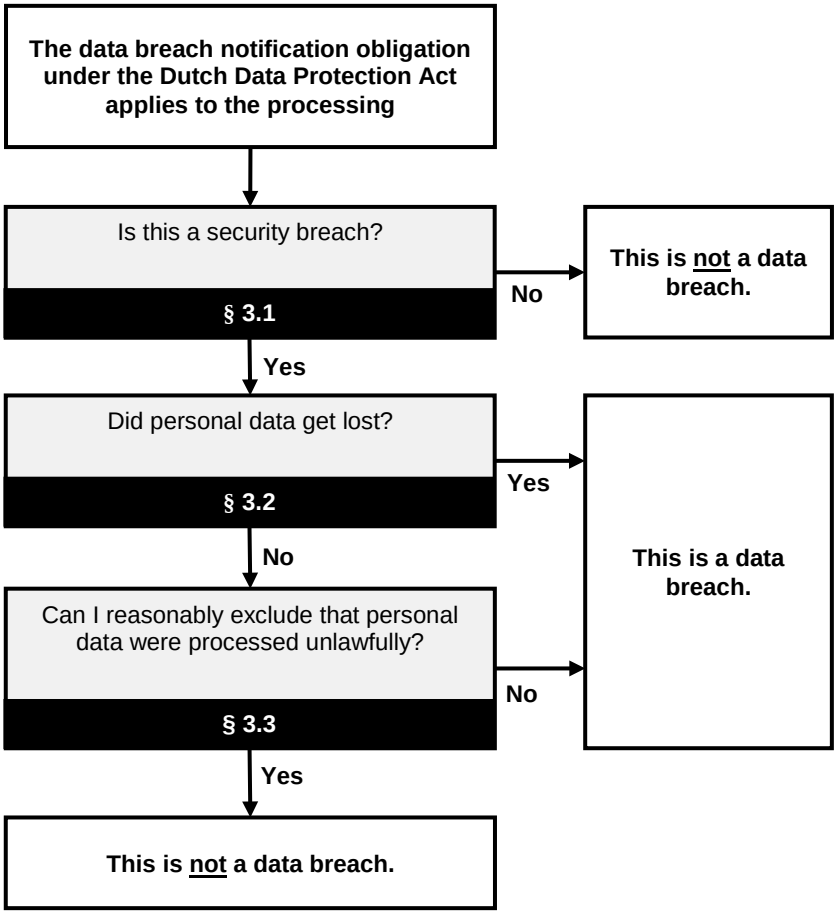
Incidentally, paragraph 4 of article 14 of the Dutch Data Protection Act stipulates that when the processor is located in another EU Member State, you are required to ensure that the processor complies with the laws of that Member State. The 'laws of that State' refers to the local obligations in the field of data security. This means that in the Processor Agreement you must guarantee compliance with the security measures as they are defined in the laws of the Member State in which the processor is established.[11]

[10] Parliamentary Documents II, 2013/14, no. 6, p. 16.

[11] Also see: Article 29-Working group, Recommendation 8/2018 on applicable law, paragraph III.5.

3. IS THIS A DATA BREACH?

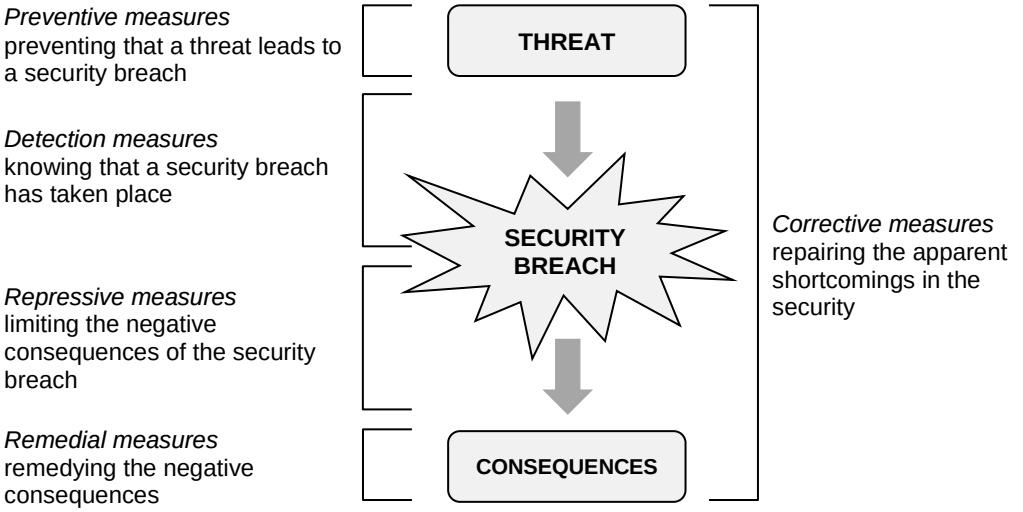
Paragraph 1 of article 34a, Dutch Data Protection Act refers to a "breach of security as referred to in article 13". In brief, in the policy rules such breach of security is referred to as a data breach. This chapter will help you to establish whether an incident that has occurred must be considered by you as a data breach. The principle is that the data breach notification obligation as laid down in the Dutch Data Protection Act applies to the processing at issue. If you do not yet know whether that is the case, please start by going through the questions in chapter 1.



3.1 Is this a security breach?

Article 13 Dutch Data Protection Act obliges you as the controller to undertake appropriate technical and organisational measures to protect personal data against loss or any form of unlawful processing.

The measures as meant in article 13 Dutch Data Protection Act can be divided into several types. This is reflected in the diagram below. By means of this diagram, the remainder of this paragraph explains when there is a case of infringement of security or not.



A security breach means that there has actually been an incident. It is not just a threat or a shortcoming in the security (also referred to as a vulnerability) which could lead to a security breach. An actual security breach has occurred and the preventive measures taken by have proven not to be sufficient to prevent the incident from happening.

With respect to security breaches that involve an infringement of the security of personal data one can think of the following:

- a lost USB-key;
- a stolen laptop;
- computer hacking;
- a malware infection;
- a disaster such as fire in a data centre.

Furthermore, typical for a data breach is that the security breach actually has effects on the personal data that you process. Personal data have been lost and you cannot reasonably exclude that personal data have been processed unlawfully. The repressive measures and the remedial actions possibly taken by you were not sufficient to completely eliminate these consequences.

An infringement of the security of personal data should be interpreted broadly. It does not matter whether you have taken appropriate technical or organisational measures or not. A data breach can occur in both situations.[12]

[12] Parliamentary Documents II 2013/14, 33 662, no. 6, p. 4.

3.2 Did the breach involve loss of personal data?

Loss means that you do not have the personal data anymore. With the security breach, personal data were destroyed or lost in a different way, and you do not have a complete and current back-up of the data. In this situation, there has been a data breach.

Example: yes / no data breach (loss of personal data)
A database with personal data has been destroyed due to human error of a system administrator. A complete and current back-up of this database is available, based on which the database can be restored immediately. In this situation, one does not speak of a data breach.

The nature of the security breach is not relevant to the question of whether or not there is a data breach. Other than suggested by the explanatory memorandum to the amendment,[13] there is also a data breach if the personal data have been lost due to a disaster and there is no current back-up available.

3.3 Can I reasonably rule out that personal data have been processed unlawfully?

Types of unlawful processing include the impairment of personal data, unauthorised perusal, alteration or provision thereof. If you cannot reasonably rule out that a security breach has led to unauthorised processing, you must consider the incident as a data breach.[14]

Example: yes / no data breach (unlawful processing of personal data)[15]
An employee has provided a third party with the username and password which give access to all customer data of the employee's company.
After discovery of this incident, the company changes the password of the account, so the third party does not have access to the data anymore.
Subsequently, the company investigates whether the third party has actually tried to gain access to the customer data. For this purpose the company makes use of log files which contain, for each customer, records of all actions taken, at what time and with respect to which customer data.
If, on the basis of the log files, it can reasonably be ruled out that access to the customer data has been gained by means of the account in question, there has just been a security breach and not a data breach.

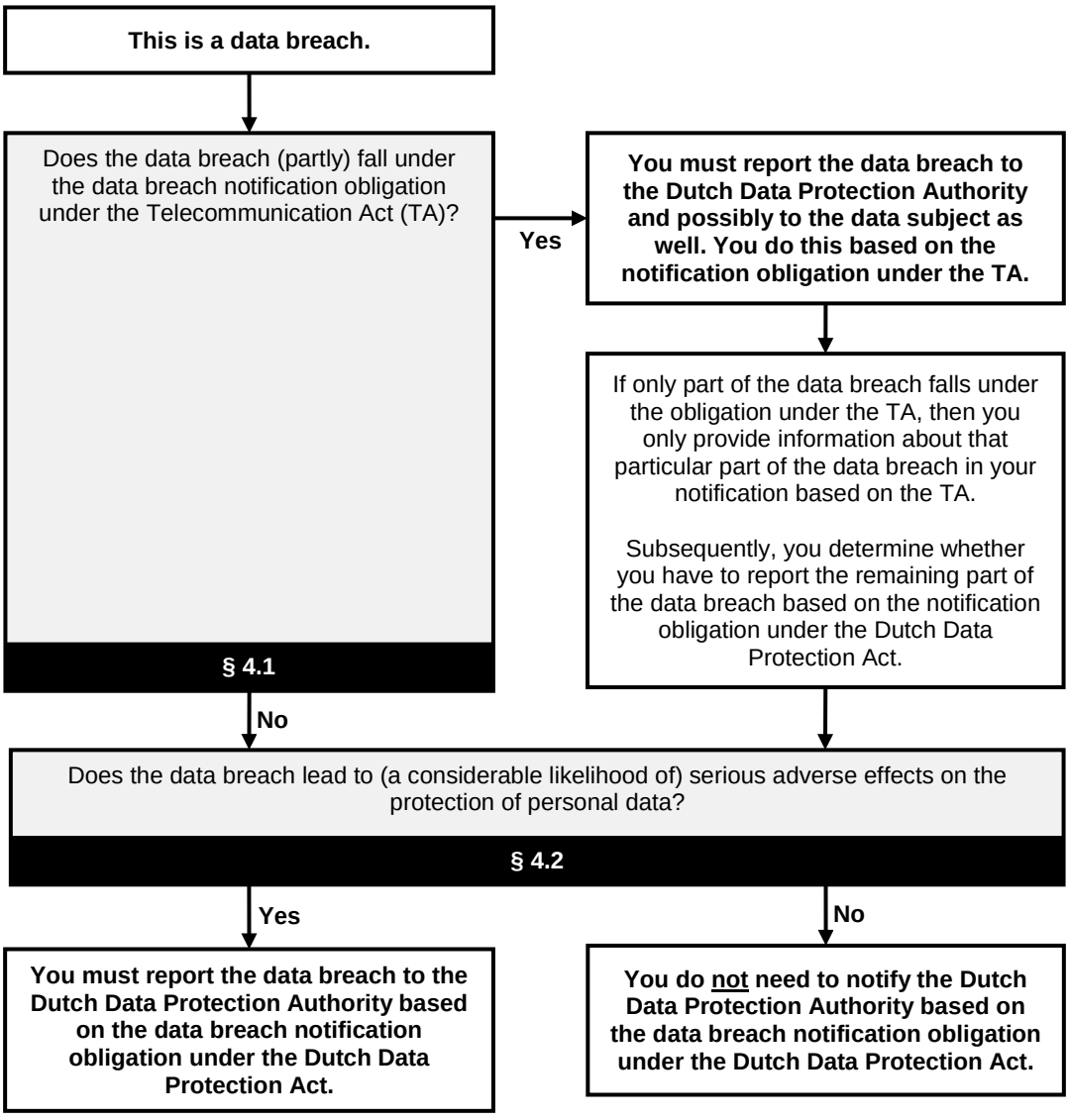
In case of a malware infection you should assume that there may be a data breach. Certain types of malware search the infected device for valuable personal data such as email addresses, usernames, passwords and credit card data, and to subsequently pass on the data found to a server of the hacker. Such a malware infection exposes the affected personal data to unauthorised access and other types of unlawful processing. Other types of malware make the files inaccessible to the rightful owner by blocking them ('ransomware') or encrypting them ('cryptoware'). Therefore, personal data

[13] Parliamentary Documents II 2012/13 33 662, no. 3, p. 5-6.
[14] Parliamentary Documents II 2014/15, 33 662, no. 11, p. 4.
[15] Source: Article 29-Working group, Recommendation 03/2014 on notification of breaches related to personal data, adopted on 25 March 2014, Case 3.

affected by these types of malware are exposed to unauthorised impairment or modification.

4. DO I HAVE TO REPORT THIS DATA BREACH TO THE DUTCH DATA PROTECTION AUTHORITY?

The diagram below illustrates the questions you have to answer in order to determine whether you must report a specific data breach to the Dutch Data Protection Authority. Each question in the diagram corresponds to a paragraph in the remainder of this chapter. The starting point is that there has been an incident which you have already determined to be a data breach. If you have not yet established this to be the case, work through the questions in chapter 3 first.



4.1. Does the data breach (partly) fall under the data breach notification obligation as laid down in the TA?

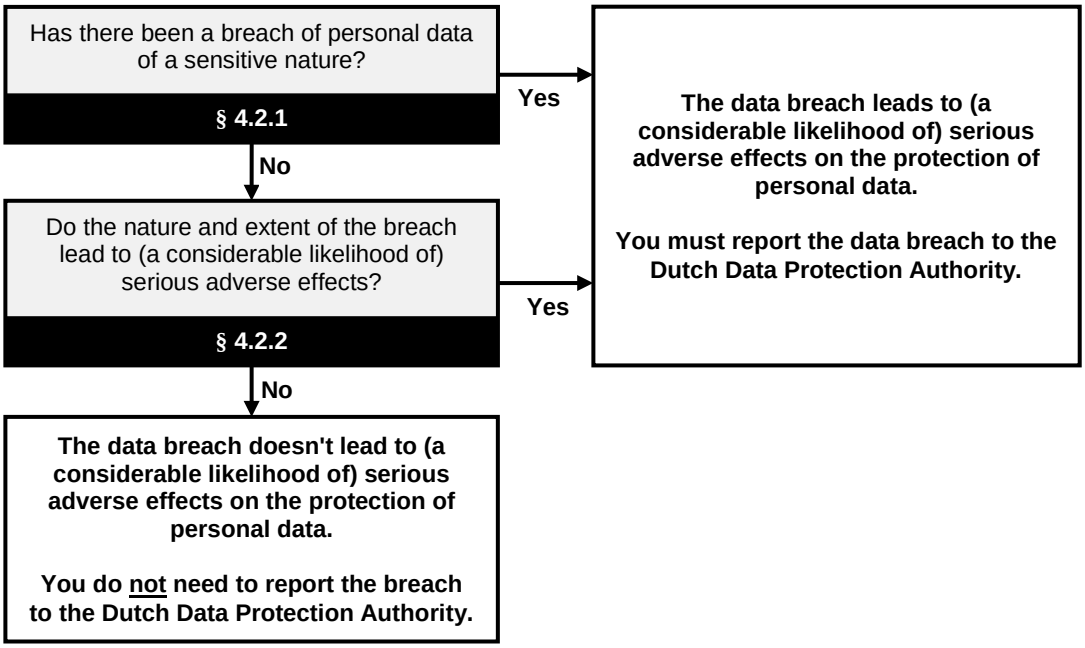
If you are a provider of a public electronic communication service, you have to deal with two data breach notification obligations: the already existing notification obligation provided in the TA and the obligation provided in the Dutch Data Protection Act.

The assumption is that once you have reported a data breach in accordance with the TA, you do not need to report it again on the basis of the Dutch Data Protection Act (article 34a, paragraph 9, Dutch Data Protection Act).
It may be that a data breach is partially related to personal data which fall under the notification obligation provided in the TA, but also partially to personal data that fall outside of that scope. An example of such a situation is the theft of a laptop which contains both customer data and personnel data. The theft of the customer data falls under the notification obligation provided in the TA and the theft of the personnel data falls under the data breach notification obligation provided in the Dutch Data Protection Act. It is possible that in such a case you need to submit two notifications: one based on the obligation under the TA and one based on the data breach notification obligation under the Dutch Data Protection Act.

4.2. Does the data breach lead to (a considerable likelihood of) serious adverse effects on the protection of personal data?

There is a stipulated data breach notification obligation which means that you only have to report a breach if it leads to (a considerable likelihood of) serious adverse effects or to serious adverse effects on the protection of personal data (article 34a, paragraph 1, Dutch Data Protection Act).

It is up to you to determine whether a data breach that you have discovered in your organisation falls within the scope of the data breach notification obligation to the Dutch Data Protection Authority. The objective of the remainder of this paragraph is to support this consideration.[16]



Every question from the diagram above corresponds to one of paragraphs below. Prior to that, please find a number of relevant examples below.

[16] Parliamentary Documents I 2014/15, 33 662, no. C, p. 17.

Examples of data breaches which must be reported to the Dutch Data Protection Authority (1)[17]

- In a hospital it is discovered that through faltering security (technical failure) medical data have been accessed by unauthorised persons;
- A current affairs programme confronts a company with the fact that because of a security breach unauthorised persons have had access to personal data of employees on the company's server such as copies of passports, driving licences, banking data and passwords;
- An employee loses a laptop containing unencrypted, financial customer data;
- A company is confronted with a hack involving the theft of customer data and passwords;
- A public database containing sensitive personal data is hacked and unauthorised persons have gained access to these data.

Examples of data breaches which must be reported to the Dutch Data Protection Authority (2)[18]

1. Four laptops are stolen from a health centre for children. The laptops contain sensitive data on health and welfare and other personal data of more than 2000 children.
2. At a life insurance company personal data were subjected to unauthorised access as a result of a vulnerability in a web application, causing the disclosure of names, addresses and forms with medical information of 700 persons.
3. An employee of an internet provider has given his login/password information to a third party, thereby virtually giving him unlimited access to all customer data (over a 100,000). It cannot reasonably be excluded that personal data were actually lost or processed unlawfully.
4. An envelope with credit card payment information of 800 people was inadvertently not fragmented, but thrown into a dustbin. A third person pulled the data from the garbage on the streets and gave them to other persons.
5. The encrypted laptop belonging to a financial advisor is stolen from his car. Financial data (mortgages, salaries, loans) of 1000 persons are involved. Although the password of the laptop is not compromised, there is no backup available.
6. On the website of a telephone company customers can log in and view their financial information and telephone data. A third party has gained access to the database with login names and corresponding hashes of passwords. However, it is possible to recover the original passwords.
7. An Internet service provider offers users the ability to examine the details of their account, including other historical search data and frequently visited websites. Due to an error in the website, through a simple trick everyone had the opportunity to have a look at the accounts of other users. Without a comprehensive logging it is not possible to determine whether this actually happened and what data were consulted.

All the above examples are based on parliamentary history. The latter examples originally are from Recommendation 03/2014 from the Article 29-Working group. A

[17] Parliamentary Documents II 2014/15 33 662, no. 11, p. 11.

[18] For the sake of completeness, examples that relate to the telecommunication sector have also been included. The examples are quoted in Parliamentary Documents I 2014/15, 33 662, no. C, p. 24, and are derived from Recommendation 03/2014 on notification of breaches related to personal data, adopted on 25 March 2014, from the Article 29-Working group. The quoted examples also specify that for the cases 1 up to 5 this relates to breaches resulting in adverse effects and in the cases 6 and 7 to breaches with a considerable likelihood of adverse effects.

number of these examples refer to large numbers of people. However, the notification obligation may also apply to a data breach which involves only one person.

Examples of incidents not subject to the notification obligation

- A letter containing personal data is sent to the wrong address, but is returned unopened.
- In a train, someone leaves a suitcase containing personal data behind. The suitcase has a sound lock and via lost and found it is returned, unopened, to its rightful owner.
- The loss or hacking of the membership records of a sports club will usually lead to quite some discomfort for the club and its members, but will not easily give cause for a notification to the Dutch Data Protection Authority.[19] This may however be different if the club focuses on people with a specific belief or sexual orientation, or when fraud susceptible data were exposed.
- If hospital staff uses the password of a doctor to gain access to medical personal data, then this is not really a data breach but actually a breach of the internal rules, in which case disciplinary measures are more appropriate.[20]

4.2.1. HAVE PERSONAL DATA OF A SENSITIVE NATURE BEEN EXPOSED?

When answering the question whether the data breach leads to (a considerable likelihood of) serious adverse effects on the protection of the processed personal data, you should at least look at the nature of the affected data. Are these special personal data, or personal data that may be sensitive in another way?[21] In the latter example you could think of payment arrears.[22]

In a number of categories of personal data, in this context referred to as personal data of a sensitive nature, loss or unauthorised processing may lead to stigmatisation or exclusion of the data subject, damage to health, financial damage or (identity) fraud. The following personal data categories should in any case be included:

- *Special personal data as referred to in article 16 Dutch Data Protection Act*
  This includes personal data about a person's religion or beliefs, race, political opinion, health, sexual life, trade Union membership, as well as criminal personal data and personal data relating to unlawful or objectionable behaviour in connection with a ban imposed in respect of such behaviour.
- *Data about the financial or economic situation of the data subject*
  This includes, for example, data about (problematic) debts, salary and payment details.
- *(Other) data that may lead to stigmatisation or exclusion of the person concerned*
  This includes, for example, data about gambling addiction, school performance or relational problems.

[19] Parliamentary Documents II 2012/13, 33 662, no. 3, p. 7.

[20] Official Reports II 2014/15 no. 9, p. 51-9-32.

[21] Parliamentary Documents II 2013/14, 33 662, no. 6, p. 19.

[22] Official Reports II 2014/15, no. 51, item 9, p. 24.

- *User names, passwords and other login data*
  The possible impact on those involved will depend on the processing of the personal data to which the login data give access. In your considerations you should include that many people reuse their passwords for different applications.
- *Data which can be misused for (identity) fraud*
  This also includes biometric data, copies of identity documents and the Citizen Service Number (CSN).

Also data from DNA databanks, data subjected to a special certain statutory confidentiality and data subjected to (medical) professional secrecy within the meaning of article 9, paragraph 4, Dutch Data Protection Act should be considered as data of a sensitive nature.

Example of a hack of personal data of a sensitive nature
By means of SQL injection (a common form of hacking), a hacker succeeds in visiting the website of a local sports club and in gaining access to the names and mail addresses of around 20 subscribers to a newsletter.
Normally speaking, this does not involve personal data of a sensitive nature. This is different when the newsletter focuses on people with, for example, specific beliefs, political opinions or sexual orientation.

4.2.2. DO THE NATURE AND EXTENT OF THE DATA BREACH LEAD TO (A CONSIDERABLE LIKELIHOOD OF) SERIOUS ADVERSE CONSEQUENCES?

The explanatory memorandum indicates that the nature and extent of the affected processing helps determine the answer to the question whether the data breach leads to (a considerable likelihood of) adverse effects on the protection of personal data. A data breach at organisations such as the Tax Office, the Social Insurance Bank or at a commercial bank or insurer may lead to financial damage for the data subject or of a compromise of data that are protected by an obligation to confidentiality.[23] Security flaws in the extensive processing of personal data held by public authorities may also have severe consequences for those involved.[24]

Apart from the sensitive nature of the personal data processed, which was already discussed in the preceding paragraph, with respect to the serious adverse effects on the protection of personal data, the following is relevant as well:

- The extent of the processing referred to above means that data breaches may involve many personal data per person, or data from large groups of data subjects. Both these factors make a exposed dataset attractive for abuse by criminal circles. In this respect, the chance that the exposed dataset is resold increases with the result that those involved suffer longer from the data breach.

[23] Parliamentary Documents II 2012/13, 33 662, no. 3, p. 7.
[24] Parliamentary Documents II 2012/13, 33 662, no. 3, p. 20.

- As the decisions taken on the basis of the processed data become more radical, the impact of loss or unlawful processing increases as well. For example: if an organisation uses financial data to determine a person's creditworthiness, the consequences of loss and unlawful alteration of the data are more radical than when the data are used for marketing purposes.
- Extensive data processing operations by the government often involve personal data that are shared within chains. This means that the consequences of loss or unauthorised alteration of personal data may occur through the entire chain. For those involved this means that it is more difficult to oversee any consequences of a data breach and to avoid them wherever possible.

If the nature and extent of the affected processing meet the above criteria, then you should assume that the data breach leads to (a considerable likelihood of) serious adverse effects on the protection of personal data.

Except for the nature and extent of the affected processing, parliamentary history also draws attention to the position of vulnerable groups.[25] For data subjects in vulnerable groups, loss or unlawful processing of personal data may entail additional risks. For the majority of people, the consequences of unauthorised access to personal details (name/address) will be limited, but this is different for people who are confronted with stalking or who are staying in a Women's Shelter. For certain categories of data subjects, such as children or people with intellectual disabilities, it may be more difficult to deal adequately with the consequences of a data breach. For example, they are more likely to become the victim of phishing or fraud.

If you know that you are processing data related to people in vulnerable groups, for example because the processing is specifically directed to persons belonging to such groups, then you should assume that a data breach would lead to (a considerable likelihood of) serious adverse effects on the protection of the processed personal data.

Example of vulnerable groups
By means of SQL injection (a common form of hacking), a hacker succeeds in visiting the website of community centre and in gaining access to a file containing the names and mail addresses of around 20 subscribers to an electronic newsletter. The newsletter focuses on local residents aged 65 years or older who take classes in the community centre to become familiar with the use of computers and the internet. In this case, the nature of the target group leads to additional risks for those involved. Given the inexperience of these data subjects with digital communication, there is a substantial risk of them becoming the victim of attempted phishing or fraud.

In case of a data breach as a result of (non-ethical) hacking (art. 138ab of the Dutch Criminal Code), it is important to be aware of the nature of the exposed data and the risks of abuse of these personal data for those involved. In case of a hack, timely notification is logical and appropriate, given the risks of abuse of the personal data. In case of a hack, reporting the hack to the police stands to reason in relation to tracing the offenders.[26]

[25] Official Report II 2014/15, no. 51, item 9, p. 23-24.

[26] Parliamentary Documents II 2013/14, no. 6, p. 19.

5. How do I have to report the data breach to the Dutch Data Protection Authority?

The Dutch Data Protection Authority makes a web form available for the purpose of reporting data breaches.[27] Please find enclosed a summary of the questions contained in this web form in an appendix to these policy rules.

If you are not able to use the web form, you may send the required information via fax to the Dutch Data Protection Authority. By doing so you need to be able to demonstrate that you have sent your notification in time.

By return of fax you will be sent an acknowledgement of receipt.

In case of notifications that give rise to further action by the Dutch Data Protection Authority, the latter will contact you in order to verify the origin of the notification. The Dutch Data Protection Authority will eventually be connected to eRecognition or other current authentication means.

[27] Autoriteitpersoonsgegevens.nl.

6. WHEN DO I HAVE TO REPORT THE DATA BREACH TO THE DUTCH DATA PROTECTION AUTHORITY?

You are required to give notice of the data breach to the Dutch Data Protection Authority without delay (article 34a, paragraph 1, Dutch Data Protection Act).

Giving notice without delay implies that after the discovery of the potential data breach, you may take some time for further investigation in order to avoid unnecessary notification.

What should be considered as 'without delay' in a specific case will depend on the circumstances of the case. Listed below are the principles which are applied by the Dutch Data Protection Authority for the purpose of its supervisory and enforcement powers.[28]

The time period for giving notice of the data breach starts running at the moment that you, or a data processor engaged by you, become aware of an incident that may fall under the data breach notification obligation.

Without undue delay, and if possible not later than 72 hours after the discovery, you file a notification with the Dutch Data Protection Authority, unless at that time your investigation has already shown that the incident does not fall under the data breach notification obligation. In case you report the incident to the supervisory authority later than 72 hours after the discovery, you can give reasons for the delay of the notification when requested.[29]

It is possible that 72 hours after the discovery of the incident you still do not fully understand what has happened and which personal data are involved. In that case you file the notification based on the information available to you at that moment. Optionally, you can either supplement or withdraw the notification afterwards.

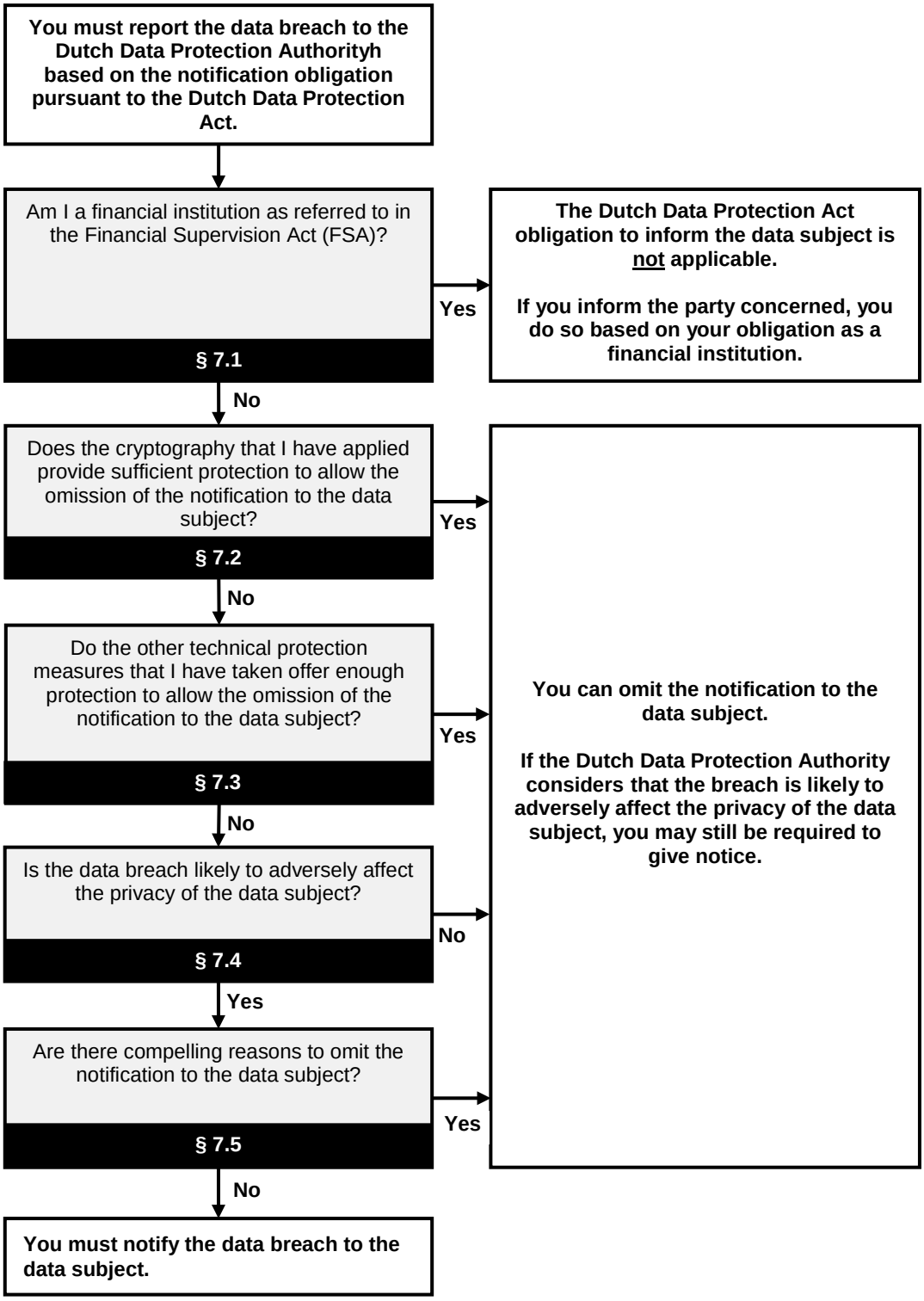
In order to be able to report data breaches in due time, you will have to make proper agreements with data processors possibly engaged by you, so they can inform you timely and adequately about all relevant incidents.

[28] Parliamentary Documents II 2013/14, 33 662, no. 6, p. 16.

[29] See art. 31, paragraph 1, of the draft General Privacy Regulation, from the text as amended by the Council of the European Union: "In case of a breach regarding personal data […] the controller shall report this breach to the competent supervisory authority in accordance with article 51 without undue delay and if possible not later than 72 hours after becoming aware of it. When the notification to the supervisory authority does not take place within 72 hours, it needs to be accompanied by a justification."

7. DO I HAVE TO REPORT THE DATA BREACH TO THE DATA SUBJECT?

The diagram below illustrates the questions that you must answer in order to determine whether you need to report a specific data breach to those affected. Every question from the diagram corresponds to a section in the remainder of this chapter.



The starting point of this chapter is that you have already determined that you must notify the relevant data breach to the Dutch Data Protection Authority under the data breach notification obligation of the Dutch Data Protection Act. If you have not yet come to that conclusion, go through the first steps in Chapter 4.

In case you have not reported the data breach to the data subject and the Dutch Data Protection Authority considers that the breach is likely to adversely affect the privacy of the party concerned, the Authority may require you to notify the data subject after all (Article 34a, paragraph 7, Dutch Data Protection Act). This is equivalent to a binding instruction.[30] In case of failure to comply with a binding instruction, the Dutch Data Protection Authority may impose an administrative penalty not exceeding the amount of the fine of the sixth category of Article 23, paragraph 4 of the Dutch Criminal Code (Article 66, paragraph 5 Dutch Data Protection Act).

7.1. Am I a financial institution as referred to in the Financial Supervision Act?

An exception from the obligation to report the data breach to the data subject is made for financial institutions as referred to in the Financial Supervision Act (FSA) (article 34a, paragraph 10, Dutch Data Protection Act). If you notify the parties concerned, you do so based on your obligation as a financial institution.

7.2. Does the cryptography that I have applied provide sufficient protection to allow the omission of the notification to the data subject?

If you have taken the appropriate protection measures to render the relevant personal data incomprehensible or inaccessible to anyone who has no right to take knowledge of that information, than you can omit the notification to the data subject (article 34a, paragraph 6, Dutch Data Protection Act).

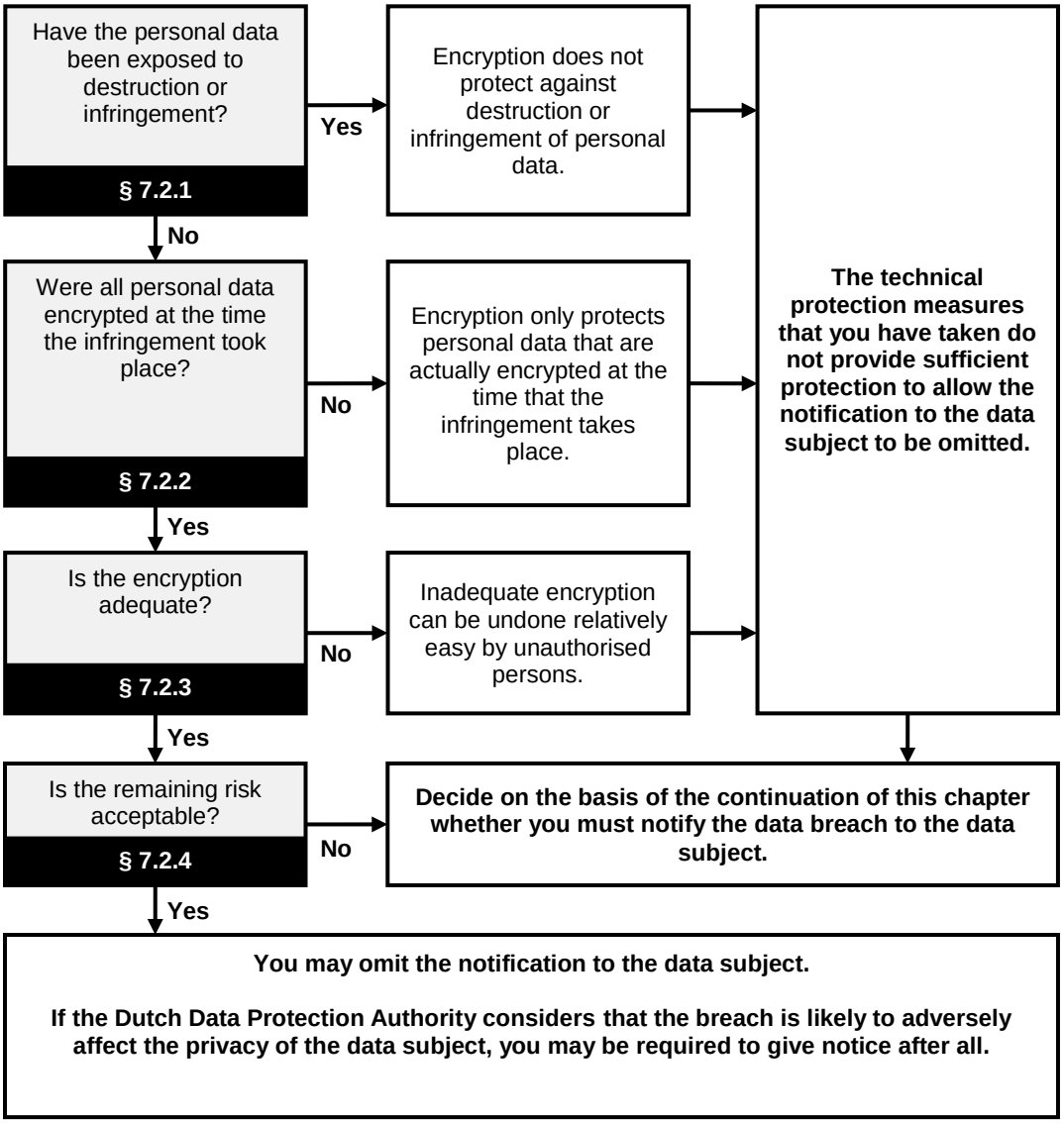
From legislative history, the application of cryptography emerged as the prime example of a technical protection measure within the meaning of paragraph 6 of article 34a Dutch Data Protection Act. Also, article 4 of the European Regulation 611/2013, which includes a similar exception to the obligation to report data breaches to data subjects for the telecom sector, is based on the use of cryptography as a technical protection measure. This paragraph discusses the use of cryptography as a technical protection measure to render personal data incomprehensible or inaccessible to unauthorised persons. Other technical protection measures will be addressed in the remainder of this chapter.

This paragraph discusses the two cryptographic operations: encryption and hashing (converting data into a unique code). Characteristic for encryption is that this operation is reversible: by use of the correct key, the original information can be obtained (decryption). Encryption is used inter alia to protect data stored on portable devices and on removable media such as USB sticks. Hashing is an adaptation of information which, regardless of the length, makes a unique hash code which always has the same length (the length is dependent on the hashing method used). Hashing is

[30] Parliamentary Documents I 2014/15, 33 662, no. C, p. 23.

used inter alia in the storage and handling of passwords: at the moment the user selects a (new) password, the corresponding hash code is stored. When the user logs in, the hash code of the password entered is compared with the stored hash code and if the codes match the user gets access to the information.

If the cryptographic operations applied by you have rendered the exposed personal data incomprehensible or inaccessible to unauthorised persons, you do not have to notify the data subject. This is a strict standard, which you must apply in each case based on the current state of technical developments. If in doubt about the adequacy of the technical protection measures you have taken, you must report the data breach to the data subject. The aim of the rest of this paragraph is to support you in making this consideration.[31]



Every question from the above diagram corresponds to one of the paragraphs below.

[31] Parliamentary Documents II 2014/15, 33 662, no. 11, p. 9-10.

7.2.1. HAVE THE PERSONAL DATA BEEN EXPOSED TO DESTRUCTION OR INFRINGEMENT?

Personal data which have been adequately encrypted can still be destroyed in case of a data breach, and even infringement or unauthorised modification is still possible (for instance by so-called 'cryptoware', whereby the already encrypted data are encrypted once again with a key that can only be obtained by the controller against payment).

A data breach involving adequately encrypted personal data which have not only been exposed to unauthorised disclosure, but also to loss or other forms of unlawful processing, may adversely affect the privacy of the data subject and might therefore have to be reported to him or her.

Example of technical protection measures in case of loss of personal data[32]

The encrypted laptop of a financial consultant is stolen from the trunk of his car. The laptop contains the financial files of 1000 data subjects, involving details about mortgages, salaries and applications for loans. Because of this theft, these data are exposed to unauthorised disclosure. The financial consultant comes to the conclusion that all data on the hard drive have been encrypted adequately, and that the remaining risk is acceptable. In principle, the notification to the data subjects could be omitted.
However: the financial consultant does not have a back-up (back-up copy) of the personal data on the hard drive. This means that this case does not only involve unauthorised disclosure, but also loss of the personal data affected.
As the financial consultant no longer has those data available, he will again have to address the data subjects to retrieve that information. The delay thus created may lead to the situation that deadlines for the submission of documents or applications are not met, which eventually may cause the parties concerned to receive fines, to suffer loss of revenue or anticipated profits, termination of purchase agreements or other serious consequences.
In spite of the technical protection measures taken, it is obvious that in this case the data subjects should be notified of the data breach. The notification should in any case include the request to provide the data again to the financial consultant and an explanation about the potential consequences and negative effects of the infringement.

7.2.2. WERE ALL PERSONAL DATA ENCRYPTED AT THE TIME THE INFRINGEMENT TOOK PLACE?

Encryption can only protect personal data that are actually encrypted at the time that an infringement takes place. A data breach whereby (also) unencrypted personal data are involved, may adversely affect the privacy of the data subject and might therefore have to be reported to him or her.

Example of personal data that were not encrypted at the time the infringement took place.

The hard drive of a laptop contains a file with personal data. The file itself is not encrypted. The laptop is locked automatically when it is not used for some time, and by the automatic locking the contents of the hard disk is encrypted. The laptop has come into the hands of a hacker who by means of technical means simulates the use of the keyboard, thereby

[32] Source: Article 29-Working group, Recommendation 03/2014 on notification of breaches related to personal data, adopted on 25 March 2014, Case 5.

preventing the automatic locking function to be activated and thus preventing the data on the hard drive to be encrypted.

Example whereby not all affected personal data were encrypted, and the remaining personal data were not encrypted at the time of the infringement[33]
An employee gives a third party the username and password which gives access to all customer data of all customers of the company where he works. These include the names, addresses, email addresses, phone numbers, access and other identifying information (usernames, hashed passwords and account numbers) and encrypted payment data (including account numbers and credit card information). For two reasons, the controller must inform this data breach to the data subject:

- only part of the personal data was encrypted (passwords and payment data);
- the payment data were stored in an encrypted manner, however if the third party logs in with the data provided he will get access via the user interface to the unencrypted data.

7.2.3. IS THE ENCRYPTION ADEQUATE?

It is primarily up to you to judge whether the encryption is strong enough, and whether it has been carried out correctly.[34]

Both encryption and hashing can basically be 'hacked', meaning that unauthorised persons are able to get access to the original data. Hacking is counteracted by the use of (combinations of) modern cryptographic techniques and by the application of so-called salts (extra information is added to the original data in order to make it difficult to hack the hash code). This field is constantly developing and it is very possible that a cryptographic operation that is safe enough in the current situation, will no longer be so in the near future. When using cryptographic operations you will therefore have to make a periodical assessment whether they still provide adequate protection.

The European Regulation 611/2013 gives further substance to adequate encryption. According to this regulation you may consider data to be incomprehensible if:

- they have been safely encrypted with a standard algorithm, the key for decryption has not run any infringement risk and the key for decryption was generated in such a manner that persons without authorised access are not able to find the key with the available technological means; or
- they have been replaced by a hash value which was computed by a cryptographically encoded hash function, the key that was used has not run any infringement risk and the key used for data hashing was generated in such a manner that persons without authorised access are not able to find the key with the available technological means.[35]

[33] Source: Article 29-Working group, Recommendation 03/2014 on notification of breaches related to personal data, adopted on 25 March 2014, Case 3.
[34] Parliamentary Documents II 2013/14, 33 662, no. 6, p. 31-32.
[35] Article 4 Regulation 611/2013.

When making this assessment you will need to make the following considerations:

- The algorithm itself, or the way in which it is applied, may show vulnerabilities because of which the encryption or hashing you applied does not provide the expected protection.
- Encryption is reversible. An unauthorised person who has the right key, or who can find that key without too much difficulty, will be able to decrypt the exposed data.
- Hashing is repeatable. If no salt was used in data hashing, or if an unauthorised person has the right salt or is able to find it without too much difficulty, he can apply the proper hashing method to a list of common values and by doing so he may be able, for instance, to discover stolen passwords.

General information on algorithms and their applications can be found for example in the publications of the European Union Agency for Network and Information Security Agency (ENISA) and the National Cyber Security Centre (NCSC). In drawing up these policy guidelines, the most recent publication of ENISA in this area was the 'Algorithms, key sizes and parameters Report - 2014 ', which was published in November 2014.[36]

In addition to the used algorithm itself, it is also important that it is applied in the proper way in order to create adequate encryption. An expert's assessment may offer you a definite answer in this respect. Preferably, this evaluation is made before a data breach takes place so that, at the time that a data breach occurs, you can easily determine whether the encryption or hashing you applied offers sufficient protection.

Finally, it is important that the key or salt you applied has not been exposed. You will need to determine this on a case by case basis.

7.2.4. IS THE REMAINING RISK ACCEPTABLE?

By answering the previous questions you will most likely have understood by now to what extent the technical protection measures that you applied offer protection against unauthorised disclosure of the exposed personal data. For each individual case you will need to assess whether the protection provided is sufficient to allow the notification to the data subject to be omitted.

Apart from what is stated above, you should also take into account what consequences it may have for the privacy of the data subject if a hacker, now or in the future, manages to have access to the affected personal data after all.

Example: notification to the data subject can be omitted in case of encryption
A laptop containing a file with personal data on the hard drive is stolen. The controller investigates the incident and concludes that he may omit sending a notification to the data subject pursuant to article 34a Dutch Data Protection Act. His considerations are the following:

[36] http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-size-and-parameters-report-2014.

- a combination of algorithm and key length was used for the encryption of the file which is rated as 'future-secure' for the next 10 to 50 years by ENISA in a current guideline (which has not been outdated by a recent publication);
- no vulnerabilities are known in relation to the applied algorithm and its implementation;
- the implementation has been successfully evaluated by an expert;
- the file itself was encrypted, so the encryption did not depend on the automatic lock which may not have worked in the relevant case;
- the key was not exposed;
- given the nature of the data breach, the processing and the exposed data, the remaining risk is acceptable.

7.3 Do the other technical protection measures that I have applied offer sufficient protection to allow the notification to the data subject to be omitted?

Besides encryption, Dutch legal history mentions yet another technical protection measure that can protect personal data from unauthorised disclosure: remote wiping of the data stored on a device (remote wiping). By wiping the data they will become inaccessible for unauthorised persons, since after a successful remote wipe a possible hacker will still have access to the device that contained the information, but not to the information itself. However, a remote wipe can only be successful if a number of preconditions have been met. The first precondition is that the remote wipe should be started in time, so that a hacker has not yet had a chance to inspect the data. Additionally, at that time the device concerned should still be intact and operational, so it is still able to carry out the remote wipe and to erase the data. Moreover, the application used to erase the data should function properly, so all data concerned are actually removed and there are no traces left behind from which the original data can be reconstructed.

If you are using remote wiping, you will have to determine on the basis of the specific circumstances of the case whether it meets the strict standard of paragraph 6 of article 34a Dutch Data Protection Act. You may use the above paragraphs as a guideline.

Even if the exposed data were pseudonymised, you will have to determine on the basis of the specific circumstances of the case whether the strict standard of paragraph 6 of article 34a Dutch Data Protection Act has been met. Pseudonymisation means that you have taken technical measures to prevent that personal data are linked to the original identity of the person concerned. Successful pseudonymisation makes the relevant personal data unintelligible for unauthorised persons to a certain degree and as a consequence the likelihood that a data breach will have adverse effects on the privacy of the data subject is reduced as a result. Imperfections in the manner in which the personal data are pseudonymised, however, can lead to unauthorised access to the original identity of the data subjects, possibly by using other data that the unauthorised persons already had in their possession or which data have come into their possession after all.

As with remote wiping, in case of exposure of pseudonymised data to unauthorised disclosure, you will also need to determine based on the specific circumstances of the case whether the strict standard of paragraph 6 of article 34a Dutch Data Protection Act is met. You may use the following paragraphs as a guideline. When making an

evaluation, it is also advisable to use the recommendation on anonymising techniques that was issued by the cooperating European supervisory authorities in 2014.[37]

7.4. Is it likely that the data breach will adversely affect the privacy of the data subject?

The data breach should be notified to the data subject if the breach is likely to adversely affect his privacy (article 34a, paragraph 2 Dutch Data Protection Act).

The interests of those involved may be harmed by the loss, misuse or abuse of their personal data. The damage can be tangible or intangible. In the latter example, you should think of unauthorised publication, defamation of character and reputation, identity fraud or discrimination.[38] Identity fraud can not only lead to intangible consequences, but may also have material consequences.
It is up to you to assess whether you need to report a data breach to the data subject.

If personal data of a sensitive nature have exposed, you should proceed on the assumption that not only you have to report the data breach to the Dutch Data Protection Authority, but also to the data subject. Loss or unlawful processing of such data may have consequences that involve stigmatisation or exclusion of the person concerned, damage to health, financial loss, or (identity) fraud. More information can be found in paragraph 4.2.1 of this policy rule.

In all other cases you will have to make a balance, based on the circumstances of the case.

Informing the person concerned about the data breach that has occurred is especially necessary in situations where real negative effects may be feared for his or her privacy. After receiving the notification, the subject will be on the alert for the potential consequences of the data breach and he or she, as far as possible, may put up a defence for instance by taking additional precautions (such as alteration of a pass word) or by purchasing services or products from another commercial entity.[39]

Examples of data breaches that must be reported to the data subject[40]

1. Four laptops are stolen from a health centre for children. The laptops contain sensitive data on health and welfare and other personal data of more than 2000 children. *Given the potential consequences of the data breach, notification to those concerned is required. In addition, it is important to keep in mind the age and maturity of the children involved. Apart from notifying the child itself, insofar as it is appropriate, in this*

[37] Article 29-Working group, *Recommendation 5/2014 on anonymising techniques*, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_nl.pdf.
[38] Parliamentary II 2013/14, 33 662, no. 6, p. 19.
[39] Parliamentary Documents II 2014/15, 33 662, no. 11, p. 6.
[40] For the sake of completeness, examples that relate to the telecommunications sector have also been included. These examples are derived from Recommendation 03/2014 on notification of breaches related to personal data, adopted on 25 March 2014, by the Article 29-Working group. This Recommendation provides a more detailed elaboration of each example, including measures that could have prevented the data breach or which could have limited its negative effects.

case it may be more appropriate to inform a parent or guardian who is already actively involved in the medical care of the child. Due to the loss of data, the integrity of the medical files may be violated, which might interfere with the treatment of the children. If the parents or caretakers are informed about the data breach, they may be attentive to any alterations in the medical care for their children, and contact the respective health professional.

2. At a life insurance company personal data were subjected to unauthorised access as a result of a vulnerability in a web application, causing the disclosure of names, addresses and forms with medical information about 700 persons.
   If the hacker publishes the stolen data on the internet, this may cause those involved to have more difficulty in finding a job as a result of the disclosure of information about health problems, pregnancy, etc. Data subjects may also have to deal with phishing or identity theft. The data breach is likely to have negative consequences for those involved, and therefore it is necessary to notify them.
3. An employee of an internet provider has given his login/password information to a third party, thereby virtually giving him unlimited access to all customer data (over 100,000). It cannot reasonably be excluded that personal data were actually lost or processed unlawfully.
   Among other information, the third party had access to payment details (including credit card information) and hash values of passwords of clients. Abuse of payment details may have financial consequences for the clients. It is also possible that the unauthorised third party is able to recover the original passwords of clients based on the stolen hash values. The data breach is likely to have adverse consequences for those involved, and therefore it is necessary to notify them.
   If the passwords are no longer safe, then the controller must require the clients to create a new password in a safe way. He must also ensure that the new passwords are generated by legitimate users, and not by third parties who have unlawfully obtained the login data. He must also inform the customer of the reason for the replacement of the password.
4. An envelope with credit card payment information of 800 people was inadvertently not fragmented, but thrown into a dustbin. A third person pulled the data from the garbage on the streets and gave them to other persons.
   The data breach could have financial consequences for those involved, if their credit card data are still valid and are being abused. Data subjects must therefore be informed of the data breach.
5. The encrypted laptop belonging to a financial consultant is stolen from his car. Financial data (mortgages, salaries, loans) of 1000 persons are involved. Although the password of the laptop is not compromised, there is no backup available.
   As the controller no longer disposes of the personal data that were on the laptop, they will again have to be provided by the individuals concerned. In itself, this will only have limited negative consequences for those involved: at most it will be a matter of frustration and wasted time because they must gather all the information again. In some cases, also deadlines for the submission of documents or claims might be exceeded, which can lead to financial losses for those affected. Data subjects must be informed of the data breach. The notification should indicate that the data must be provided to the financial consultant once more, and should also include an explanation of the potential consequences and possible negative impact of the data breach.
6. On the website of a telephone company customers can log in and view their financial information and telephone data. A third party has gained access to the database with login names and corresponding hashes of passwords. When hashing the passwords an outdated algorithm was used that provides inadequate protection against access by unauthorised persons. The result is that a third party will be able to recover the original passwords without too much difficulty.
   [This example relates to the telecommunications sector and therefore it does not come under the obligation to report data breaches as provided in the Dutch Data Protection Act. However, the considerations for informing the data subjects may also be applied outside the telecommunications sector.] The third party is able to recover the passwords of all subscribers. He also possesses the login names, and can thus have access to all accounts. Many people use the same combination of login name and

password to log into multiple websites. This means that the seized data will allow the third party to have access to other accounts of certain data subjects, which may include email accounts. This data breach is likely to have negative consequences for those involved, and notification is required. Customers must be informed of the data breach, accompanied by the urgent advice to modify the password of all accounts for which they use the same password. They must also be forced to change their password for logging in to the website in question. It must be ensured that the new passwords are generated by legitimate users, and not by third parties who have gained access to the login details.

7. An Internet service provider offers users the ability to examine the details of their account, including other historical search data and frequently visited websites. Due to an error in the website, through a simple trick everyone had the opportunity to have a look at the accounts of other users. Without a comprehensive logging it is not possible to determine whether this actually happened and what data were consulted.
   [This example relates to the telecommunications sector and therefore it does not come under the obligation to report data breaches as provided in the Dutch Data Protection Act. However, the considerations for informing the data subjects may also be applied outside the telecommunications sector.] The data can be used to send spam to the data subjects or for telephone sales or phishing. The seized data may also be used to draw up profiles of the customers or to record their conduct, which might reveal sensitive information. This data breach is likely to have adverse consequences for those involved, and should therefore be notified to them.

7.5. Are there any compelling reasons why the notification to the data subject should be omitted?

You may decide not to notify the data subject, if you have compelling reasons to do so (article 43 Dutch Data Protection Act). In addition, this implies that notification to the data subject may only be omitted if this is *necessary* in view of the interests mentioned in this article.
Pursuant to article 43, under e, Dutch Data Protection Act, the notification to the person concerned may be omitted to the extent that this is necessary in the interest of the protection of the person concerned.

Example of omitting the notification in order to protect the data subject
There has been a breach of data about medical and psychosocial care applications submitted by children who have done so without their parents being aware of this. The controller reports the data breach to the Dutch Data Protection Authority, and invokes article 43, under e, Dutch Data Protection Act, to allow the omission of the notification to those involved. The reason being that parents might become aware of the demand for care when receiving the notification.

Notification of data breaches to data subjects entails an administrative burden, but in itself that is no reason to omit the notification. Only when you are able to demonstrate that the administrative burden involved in notifying the data subjects of the data breach is disproportionate to such an extent that your rights or freedoms are violated or are threatened to be violated, you may invoke article 43, under e, Dutch Data Protection Act, to allow the omission of sending a notification to the data subject.

Example of omitting the notification in order to protect the rights and freedoms of the controller[41]

A listed company is involved in a takeover when a major data breach occurs. The company reports the data breach to the Dutch Data Protection Authority, and invokes article 43, under 3, Dutch Data Protection Act, to allow the (provisional) omission of sending a notification to the data subject.

[41] Parliamentary Documents II, 2013/14, 33 662, p. 8.

8. How do I have to report the data breach to the data subject?

The notification to the data subject should at least include: the nature of the infringement, the authorities where the data subject can obtain more information about the breach, and the measures that you recommend to the data subject to reduce the negative consequences of the data breach (article 34a, paragraph 3, Dutch Data Protection Act).

When informing about the nature of the infringement in most cases you only need to give a general description. You include your contact details so the person concerned may reach you if he or she has any questions about the data breach. Furthermore, you indicate what the data subjects can do themselves in order to reduce the negative effects of the data breach, such as changing user names and passwords when these have possibly been compromised by the infringement. You are free to add more information to the notification, but this is not obligatory.[42]

Example of notification to data subject and additional actions[43]

An energy supplier offers its customers an online account where they can log in to view recent billing and consumption information. The company discovers that a third party has obtained illegal access to the database with user names and passwords of their website. The passwords have not been adequately encrypted.

The energy supplier undertakes the following actions:

- he informs his customers about the data breach. He thereby recommends the customers to change the password of all accounts for which they are using the same password;
- he resets all passwords and forces all users to enter a new password. He does this in a safe way so that he is sure that these are his customers who create a new password, and not an unauthorised third party, and he also explains why the customer must create a new password;
- he makes adjustments to his systems, to ensure that all passwords used are being encrypted in an adequate manner.

Taking into account the nature of the infringement, the observed and the actual impact on the processing of personal data, the circle of people involved and the costs of enforcement, you shall give notice to the person concerned in such a way that a proper and careful provision of information is guaranteed (article 34a, paragraph 5, Dutch Data Protection Act).

In most cases you, as the controller, will have all contact details of the data subjects at your disposal, and therefore you will be able to inform those concerned individually.

In case of more extensive incidents, you can choose a combination of providing general information and informing the persons concerned on an individual basis. For example:

[42] Parliamentary Documents II, 2012/13, 33 662, no. 3, p. 21-22.

[43] Source: Article 29-Working group, Recommendation 03/2014 on notification of breaches related to personal data, adopted on 25 March 2014, Case 6.

- You send an email to the data subjects in which you briefly indicate what has happened and what the individual himself can do to counteract the negative effects.
- In the email to the data subjects you refer to your website for more detailed information. There you give a further explanation, if necessary, about the nature of the infringement and the measures that the data subject may take himself.
- In your email you also refer to a central information desk (email, telephone number) where the data subject may obtain more detailed information.

The important thing is that you reach as many data subjects as possible and provide them with information that might help to mitigate the consequences of the data breach for their privacy as much as possible. [44]

[44] Parliamentary Documents I, 2014/15, 33 662, no. C, p. 15.

9. WHEN DO I HAVE TO REPORT THE DATA BREACH TO THE DATA SUBJECT?

You are required to report the data breach to the data subject without delay (article 34a, paragraph 2, Dutch Data Protection Act).

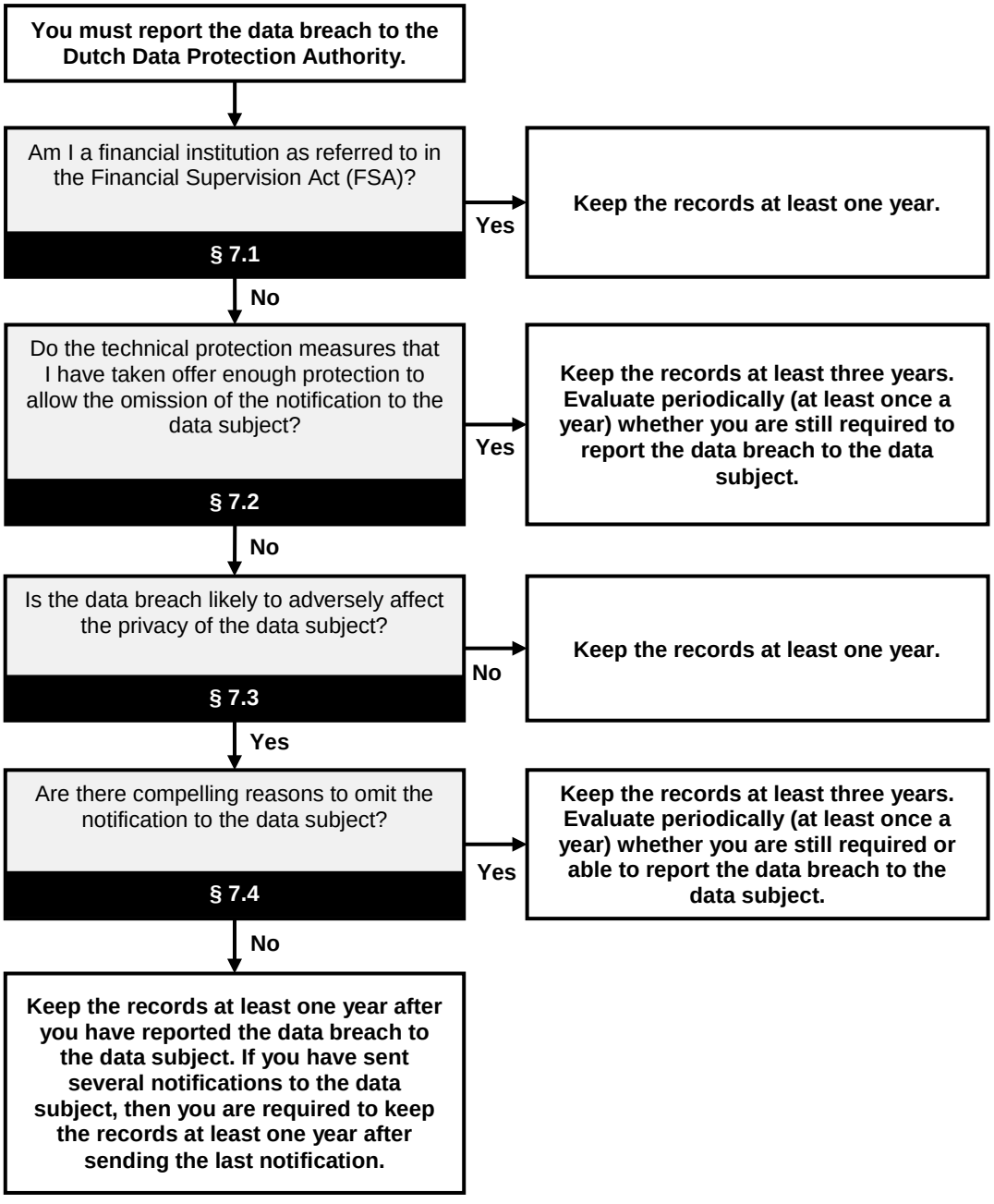
The immediate notification implies that, after discovering the data breach you may take some time for further investigation so that you can inform the data subject in a proper and careful manner. However, you must keep in mind that following your report the persons concerned need to take possible measures to protect themselves against the consequences of the data breach. The sooner you inform the data subjects, the sooner they can take action.

As with the notification to the Dutch Data Protection Authority, you may choose to inform the data subjects in the first instance based on the information you have at that time, so they can already take measures to protect themselves against the effects of the data breach, and to supplement this information at a later stage on the basis of further investigation. An example of such a situation is that you know that unauthorised persons have had access to a database with login data, but you are still investigating to find out whether the unauthorised persons have actually been able to see other personal data as well. In such a case you can immediately begin to reset the affected passwords and inform the data subjects, indicating that if they use the same login data elsewhere, they should change these without delay.

In the notification to the Dutch Data Protection Authority you should indicate whether you have already notified the data breach to the data subjects and, if not, when will you do so. You must also comply with the period specified in the notification to the Dutch Data Protection Authority. If later on you realise that you cannot meet this deadline, you must report this delay to the Dutch Data Protection Authority by means of a modification of the original notification.

10. WHICH INFORMATION DO I HAVE TO RECORD ABOUT THIS DATA BREACH?

You must keep a record of all data breaches that fall under the data breach notification obligation. For each data breach the record should at least include the facts and circumstances related to the nature of the infringement. If the data subjects have been notified about the breach, you are also required to include the text of the notification in your record (article 34a, paragraph 8, Dutch Data Protection Act).
The law does not prescribe how long you are required to keep these records. Basically, a retention period of **at least one year** will need to be observed. In some cases it might be necessary to observe a longer retention period.[45] The diagram below provides a decision-making model.



[45] Official report I 2014/15, no. 12, p. 5.

You are only required to record information about data breaches which are governed by the data breach notification obligation. If you have not yet established whether the data breach concerned comes under the notification obligation, then you will start by going through the steps of chapter 3 of these policy guidelines.

The questions set out in the diagram above are explained in more detail in chapter 7 of these policy guidelines.

The above diagram assumes that you store the records for the following purposes:

- to draw lessons from the data breach and the way in which you handled it;
- to be able to answer questions from data subjects and others;
- to report the data breach to the data subjects after all, if you have not done so in the first instance and the situation requires you to still notify those involved.

The latter may occur, for instance when in case of theft of an encrypted dataset you decide, on the basis of paragraph 6 of article 34a Dutch Data Protection Act, to withhold the notification to the data subject. In such a situation you must be aware that the introduction of new technologies may pose new risks and that new vulnerabilities in widely used encryption algorithms are discovered regularly. With the theft of the encrypted dataset in mind this means that you should be alert to these risks over a longer period of time. When signals of possible decryption occur, you should still consider notifying those concerned.[46]

Please note that a follow-up procedure after a data breach may include legal actions (civil or criminal) and that you, where appropriate, need to collect, save and present evidence in accordance with the provisions for evidence as defined for the relevant field of law.

You do not need to publish the list.

[46] Parliamentary Documents II, 2014/15, 33 662, no. 11, p. 10.

11. What does the Dutch Data Protection Authority do with my notification?

This chapter answers the question how the Dutch Data Protection Authority processes your notification regarding the data breach. This chapter also gives an explanation on enforcement in case of a violation of the notification obligation.

11.1 Administrative processing

After notification of the data breach you will immediately receive a confirmation of receipt.

If the notification calls for further action by the Dutch Data Protection Authority, they will contact you about this matter. In the first instance they will verify whether the notification was indeed sent by you, and possibly they will ask some substantive questions about the notification.

11.2 Actions to be taken

It is your responsibility to trace the cause of the data breach, and to take measures in order to prevent repetition. You are also required to determine whether you need to notify the data subjects and how you are going to proceed. One of the purposes of these guidelines is to support you in making this assessment. Being a supervisory authority, the Dutch Data Protection Authority does not offer assistance in handling the actual data breach.

Based on the data breach notification received, the Dutch Data Protection Authority will be able to see to it that data subjects are informed adequately about data breaches that affect them personally, or that might cause problems to those involved. If you have not reported the data breach to the data subject, the Dutch Data Protection Authority may require you to notify the data subject after all, in case the Dutch Data Protection Authority is of the opinion that the data breach might have negative results for the person involved (article 34a, paragraph 7, Dutch Data Protection Act). This is the equivalent of a binding instruction, and non-compliance may be sanctioned by the imposition of an administrative penalty.[47]

Furthermore, based on the data breach notification received, the Dutch Data Protection Authority will be able to take action to further promote the adequate protection of personal data.
If the received data breach notifications show that the protection of personal data may not be in order, it could give rise to the Dutch Data Protection Authority for further investigation into the compliance with the security requirements of the Dutch Data Protection Act.

[47] Parliamentary Documents I 2014/15, 33 662, no. C, p. 23.

11.3 Register of received data breach notifications

The Dutch Data Protection Authority keeps records of received data breach notifications. This register is not public, because the interest of keeping confidentiality with regard to information about the security of data processing or about exposed personal data prevents this. However, the Dutch Data Protection Authority may pay attention to data breaches in annual reports or other publications at anonymised and aggregated level based on the notifications received.[48]

The Dutch Data Protection Authority supervises compliance with the legal requirements for data protection. Among other actions, the Dutch Data Protection Authority may conduct an investigation into possible violations of the law (article 60, Dutch Data Protection Act). If any ongoing violations are discovered by the Dutch Data Protection Authority during their investigation, they can take enforcing actions (article 65 and 66, Dutch Data Protection Act). The Dutch Data Protection Authority is authorised to use information from received data breach notifications. In case of any publication of this information, the Policy rules on active disclosure by the Dutch Data Protection Authority are applicable.

The Dutch Data Protection Authority may make cooperation agreements with other supervisory authorities. These agreements will be laid down in a cooperation protocol, which is published in the Government Gazette (article 51a, paragraph 1, Dutch Data Protection Act). As part of these agreements, the Dutch Data Protection Authority may also forward information from data breach notifications to these other supervisory authorities (article 51a, paragraph 2, Dutch Data Protection Act).

11.4 Enforcement

Upon violation of the provisions under article 34a, Dutch Data Protection Act, the Dutch Data Protection Authority may impose an administrative penalty. The administrative penalty shall not exceed the amount of the sixth category of article 23, paragraph 4 of the Criminal Code (article 66, paragraph 2, Dutch Data Protection Act).

If there is a violation of the Dutch Data Protection Act which has been committed intentionally or was the result of serious culpable negligence, the supervisory authority may immediately impose an administrative penalty (article 66, paragraph 4, Dutch Data Protection Act). "[…] 'serious culpable negligence' is defined in the parliamentary history as: "[...] an abusive, considerably careless, negligent or injudicious act. If the same type of violation has occurred several times, it will be assumed sooner that a case of negligence has taken place."[49]

If there is no case of a violation of the Dutch Data Protection Act which has been committed intentionally or was the result of serious culpable negligence, a binding instruction will precede the imposition of an administrative penalty. The Dutch Data Protection Authority may set a deadline for complying with the instruction (article 66,

[48] Parliamentary Documents II 2013/14, 33 662, no. 6, p. 32-33.

[49] Parliamentary Documents II 2013/14, 33 662, no. 16, p. 1.

paragraph 3, Dutch Data Protection Act). In case of failure to comply with a binding instruction, the Dutch Data Protection Authority may impose an administrative penalty not exceeding the amount of the fine of the sixth category of Article 23, paragraph 4 of the Dutch Criminal Code (article 66, paragraph 5, Dutch Data Protection Act).

When imposing an administrative penalty, the Dutch Data Protection Authority will take into account all circumstances of the case. A circumstance of the case may include the fact that the information at issue has not been viewed by third parties and the privacy interests of those involved have not actually been harmed.[50]

[50] Parliamentary Documents II 2014/15, 33 662, no. 24.

APPENDIX: INFORMATION REQUIRED IN THE NOTIFICATION

This appendix refers to the information that you need to forward to the Dutch Data Protection Authority when you report a data breach. In drawing up the form, the questions as listed in appendix I to the European Regulation 611/2013 have been taken as a starting point. Within Europe the authorities are striving for harmonisation of the requirements for reporting data breaches in the telecommunications sector to the supervisory authority.[51] When this aspiration will lead to concrete results, the Dutch Data Protection Authority will of course join this effort.

Nature of the notification

1) Is this a follow-up on an earlier report? (Choose one of the following options.)
   a) Yes
   b) No
2) What is the number of the original notification? (Answer this question if you answered yes to question 1.)
3) What is the scope of the follow-up notification? (Answer this question if you answered yes to question 1, choose one of the following options.)
   a) To add information to or modify information from the earlier report
   b) Withdrawal of the earlier report
4) What is the reason for the withdrawal? (Answer this question if you have chosen option b in question 3.)

Legal framework for the notification

5) Under which legal provision do you make this notification?[52]
   a) article 34a, paragraph 1, Dutch Data Protection Act
   b) article 11.3a, paragraph 1, TA

General information and contact details

6) Which company or organisation do you refer to? (Enter details below.)
   a) Name of the company or organisation
   b) (Office) address
   c) Postal code
   d) City
   e) Chamber of Commerce registration number
7) Who reports the data breach? (Enter details below)
   a) Name of the reporting person
   b) Function of the reporting person
   c) Email address of the reporting person
   d) Telephone number of the reporting person
   e) Alternative telephone number of the reporting person

[51] Regulation 611/2013, preamble 11.

[52] See paragraph 4.1 of these guidelines.

8) Who may be contacted by the Dutch Data Protection Authority to receive further information about the notification? (Fill in the information below if this is a different person than the person reporting the data breach.)
   a) Name of contact person
   b) Position of the contact person
   c) Email address of the contact person
   d) Telephone number of the contact person
   e) Alternative telephone number of the contact person
9) In which sector does the company or organisation operate? (Choose one of the options mentioned below.)
   a) ...[53]

Information about the data breach

10) Please provide a summary of the incident that caused the data breach.
11) How many people are personally involved in the breach? (Fill in the numbers.)
   a) Minimum: (fill in)
   b) Maximum: (fill in)
12) Describe the group of people whose personal data are involved in the breach.
13) When did the data breach take place? (Choose one of the following options and make additional comments if necessary.)
   a) On (date)
   b) Between (starting date) and (end date)
   c) Not yet known
14) What is the nature of the breach? (You can tick multiple options.)
   a) Reading (confidentiality)
   b) Copy
   c) Modification (integrity)
   d) Removal or destruction (availability)
   e) Theft
   f) Not yet known
15) What type of personal data are involved? (You can tick multiple options.)
   a) Name and address details
   b) Telephone numbers
   c) Email addresses or other addresses for electronic communication
   d) Access or identifying information (e.g. user name / password or account number)
   e) Financial data (e.g. account number, credit card number)
   f) Citizens Security Number (BSN) or Social Security number
   g) Passport copies or copies of other identity documents
   h) Special personal data (e.g. race, ethnicity, criminal information, political beliefs, trade union membership, religion, sexual orientation, medical data)
   i) Other information, i.e. (complete)

[53] The purpose of this question is to be able to match media reports and other signals about data leaks which have occurred with the received data breach notifications in the best possible way.

16) What impact could the breach have on the privacy of those involved? (You can tick multiple options.)
    a) Stigmatisation or exclusion
    b) Damage to health
    c) Exposure to (identity) fraud
    d) Exposure to spam or phishing
    e) Other, i.e. (complete)

Follow-up actions in response to the data breach

17) Which technical and organisational measures has your organisation taken to address the breach and to prevent further violations?

Notifying the data subjects

18) Have you notified those involved about the breach or do you have the intention to do so? (Choose one of the following options.)
    a) Yes
    b) No
    c) Not yet known
19) When did you notify the data subjects about the data breach, or when are you going to do so? (Answer this question if you have answered yes to question 18. Choose one of the following options and complete where needed.)
    a) I notified the data subjects about the data breach on (date)
    b) I am going to notify the data subjects about the data breach on (date)
    c) Not yet known
20) What are the contents of the notification to the data subjects? (Literal representation, answer this question if you have answered yes to question 18.)
21) How many data subjects have you notified or are you going to notify? (Answer this question if you have answered yes to question 18.)
22) Which means of communication are you using or going to use to notify the data subjects? (Answer this question if you have answered yes to question 18.)
23) Why did you decide not to inform the data subjects? (Answer this question if you have answered no to question 18. Choose one of the following options and complete where needed.)
    a) The technical protection measures that I have taken offer sufficient protection to allow the notification to the person concerned to be omitted. [54]
    b) It is unlikely that the data breach will adversely affect the privacy of the data subject, because: (complete)[55]
    c) I have serious reasons for not notifying the data subject about the data breach, because: (complete)[56]
    d) Other, i.e. (complete)

[54] See paragraph 7.2 of these guidelines.

[55] See paragraph 7.3 of these guidelines.

[56] See paragraph 7.4 of these guidelines.

Technical protection measures

24) Have the personal data been encrypted, hashed or otherwise made incomprehensible or inaccessible for unauthorised persons?[57] (Choose one of the following options and complete where needed.)
    a) Yes
    b) No
    c) Partly, i.e. (complete)
25) If the personal data have wholly or partly been made incomprehensible or inaccessible, in what way was this done? (Answer this question if you have chosen option a or option c in question 24. If you have made use of encryption, please also specify the way in which this was done.)

International aspects

26) Does the data breach relate to persons in other EU countries? (Choose one of the following options.)
    a) Yes
    b) No
    c) Not yet known
27) Did your company or organisation report the data breach to supervisory authorities in one or more other EU countries?
    a) Yes, i.e. (complete)
    b) No

Follow-up notification

28) Is this notification form complete according to your opinion? (Select one of the options below.)
    a) Yes, the required information has been provided and there is no need for a follow-up notification.
    b) No, a follow-up notification with additional information about this breach will be forwarded at a later date.

[57] See paragraph 7.2 of these guidelines.

APPENDIX: TEXT OF THE QUOTED ARTICLES OF DUTCH LAW

This appendix contains the complete text of the law articles referred to in the above.

Article 1 Dutch Data Protection Act

For the purposes of this Act and the provisions based upon it:

a. "personal data" shall mean: any information relating to an identified or identifiable natural person;
b. "processing of personal data" shall mean: any operation or any set of operations concerning personal data, including in any case the collection, recording, organisation, storage, updating or modification, retrieval, consultation, use, dissemination by means of transmission, distribution or making available in any other form, merging, linking, as well as blocking, erasure or destruction of data;
c. "file" shall mean: any structured set of personal data, regardless of whether or not this data set is centralised or dispersed along functional or geographical lines, that is accessible according to specific criteria and relates to different persons;
d. "controller" shall mean: the natural person, legal person, administrative body or any other entity which, alone or in conjunction with others, determines the purpose of and means for processing personal data;
e. "processor" shall mean: the person or body which processes personal data for the controller, without coming under the direct authority of that controller;
f. "data subject" shall mean: the person to whom the personal data relate;

[…]

q. binding instruction: the independent obligation imposed for an offence;
r. Independent obligation: the single obligation to perform certain acts as referred to in article 5:2, paragraph 2, of the General Administrative Law Act to promote compliance with legal provisions.

Article 2 Dutch Data Protection Act

1 . This Act applies to the fully or partly automated processing of personal data, and the non-automated processing of personal data entered in a file or intended to be entered therein.
2. This Act does not apply to the processing of personal data:
   a. in the course of a purely personal or household activity;
   b. by or on behalf of the intelligence or security services referred to in the Intelligence and Security Services Act 2002 *(Wet op de inlichtingen- en veiligheidsdiensten 2002)*;
   c. for the purposes of implementing the police tasks defined in articles 3 and 4, paragraph 1, of the Police Act 1993;
   d. governed by or under the Municipal Database (Personal Records) Act;

e. for the purposes of implementing the Judicial Documentation Act and
f. for the purposes of implementing the Electoral Provisions Act.

3. This Act does not apply to the processing of personal data by the armed forces where Our Defence Minister so decides with a view to deploying or making available the armed forces to maintain or promote the international legal order. Such a decision shall be communicated to the Dutch Data Protection Authority as quickly as possible.

Article 3 Dutch Data Protection Act

1. This Act does not apply to the processing of personal data for exclusively journalistic, artistic or literary purposes, except where otherwise provided in this Chapter and in articles 6 to 11, 13 to 15, 25 and 49.
2. The prohibition on processing personal data referred to in article 16 does not apply where this is necessary for the purposes referred to under paragraph 1.

Article 4 Dutch Data Protection Act

1. This Act applies to the processing of personal data carried out in the context of the activities of an establishment of a controller in the Netherlands.
2. This Act applies to the processing of personal data by or for controllers who are not established in the European Union, whereby use is made of automated or non-automated means situated in the Netherlands, unless these means are used only for forwarding personal data.
3. The controllers referred to in paragraph 2 are prohibited from processing personal data, unless they designate a person or body in the Netherlands to act on their behalf in accordance with the provisions of this Act. For the purposes of application of this Act and the provisions based upon it, the said person or body shall be deemed to be the controller.

Article 13 Dutch Data Protection Act

The controller shall implement appropriate technical and organisational measures to secure personal data against loss or against any form of unlawful processing. These measures shall guarantee an appropriate level of security, taking into account the technical developments and the costs of implementation, and having regard to the risks associated with the processing and the nature of the data to be protected. These measures shall also aim at preventing unnecessary collection and further processing of personal data.

Article 14 Dutch Data Protection Act

1. If the controller has personal data processed for his purposes by a processor, the controller shall make sure that the processor provides adequate guarantees concerning the technical and organisational security

measures for the processing to be carried out and the notification of a breach of security as referred to in article 13 that leads to a considerable likelihood of serious adverse effects or that has significant adverse effects on the protection of personal data. The controller shall make sure that these measures are complied with.

2. The carrying out of processing by a processor shall be governed by an agreement or another legal act whereby an obligation is created between the processor and the controller.
3. The controller shall make sure that the processor:
   a. processes the personal data in accordance with article 12, paragraph l,
   b. complies with the obligations incumbent upon the controller under article 13, and
   c. complies with the obligations resting on the controller regarding the notification obligation of a breach of security - as referred to in article 13 – that leads to a considerable likelihood of serious adverse effects or has serious adverse effects on the protection of personal data which are processed by him.
4. Where the processor is established in another country of the European Union, the controller shall make sure that the processor complies with the laws of that other country, notwithstanding the provisions of paragraph 3 under b and c.
5. For the purpose of preserving the evidence, those parts of the agreement or legal act relating to personal data protection and the security measures referred to in article 13, and the notification obligation of a breach of security - as referred to in article 13 – that leads to a considerable likelihood of serious adverse effects or that has serious adverse effects on the protection of personal data which are processed by him, shall be set down in writing or in another equivalent form.

Article 34a Dutch Data Protection Act

1. The controller shall, without undue delay, notify the Dutch Data Protection Authority of a breach of security as referred to in article 13 that leads to a considerable likelihood of serious adverse effects or that has serious adverse effects on the protection of personal data.
2. The controller, as referred to in paragraph 1, shall, without undue delay, notify the data subject of the breach, as referred to in paragraph 1, if the breach is likely to have adverse effects on his privacy.
3. The notification to the Dutch Data Protection Authority and the data subject shall at least describe the nature of the breach, the contact points where more information can be obtained, and shall recommend measures to mitigate the possible adverse effects of the personal data breach.
4. The notification to the Dutch Data Protection Authority shall, in addition, describe the actual and likely consequences of, and the measures proposed or taken by the controller to address, the personal data breach.

5. The notification to the data subject shall be made in such a way that, taken into account the nature of the breach, the identified and actual effects on the processing of personal data, the circle of those involved and the costs of enforcement, a proper and careful provision of information is guaranteed.
6. Paragraph 2 shall not apply if the controller has implemented appropriate technological protection measures by which the personal data concerned by the security breach have been rendered unintelligible or inaccessible to any person who is not authorised to access it.
7. If the controller is not notifying the data subject the Dutch Data Protection Authority, if it finds that the breach is likely to have adverse effects on the data subject's privacy, may require the controller to do so.
8. The controller shall maintain an inventory of every personal data breach that leads to a considerable likelihood of serious adverse effects or that has serious adverse effects on the protection of personal data. The inventory shall at least comprise facts and data regarding the nature of the breach, as referred to in paragraph 3, as well as the text of the notification to the data subject.
9. This article shall not apply if the controller, in his capacity as the provider of a public electronic telecommunication service, has made a notification as referred to in article 11.3a, paragraphs 1 and 2, of the Telecommunication Act (TA).
10. Paragraphs 2 and 7 shall not apply to financial institutions as referred to in the Act on Financial Supervision.
11. By order in council, further rules can be set with respect to the notification.

Article 43 Dutch Data Protection Act

The controller may exclude the application of articles 9, paragraph 1, 30, paragraph 3, 33, 34, 34a, paragraph 2, and 35 to the extent that this is necessary in the interest of:

a. State security;
b. prevention, detection and prosecution of criminal offences;
c. important economic and financial interests of the State and other public bodies;
d. supervision of the compliance with legal provisions established in the interests referred to under b and c; or
e. protection of the data subject or the rights and freedoms of others.

Article 51a Dutch Data Protection Act

1. The Dutch Data Protection Authority is authorised to make agreements with other supervisory authorities in the interest of efficient and effective supervision of the processing of personal data and to establish, together with those authorities, cooperation protocols for that purpose. A cooperation protocol shall be published in the Government Gazette.
2. The Dutch Data Protection Authority and the supervisory authorities as referred to in paragraph 1, are authorised, on their own initiative and, upon request, obliged to provide each other with information about the processing of personal data necessary for the performance of their duties.

Article 60 Dutch Data Protection Act

1. The Dutch Data Protection Authority, acting in an official capacity or at the request of an interested party, may initiate an investigation into the manner in which the provisions laid down by or under the Act are being applied with respect to the processing of data.
2. The Dutch Data Protection Authority shall present its provisional findings to the attention of the controller or group of controllers who are involved in the investigation, and allow them to give their views thereon. Should the provisional findings be related to the implementation of any Act, the Dutch Data Protection Authority shall also relay the information to the Minister concerned.
3. In the case of an investigation initiated at the request of an interested party, the Dutch Data Protection Authority shall inform the aforesaid party of its findings, unless providing such information would be incompatible with the purpose of the data processing or the nature of the personal data, or unless important interests of parties other than the requester, including the controller, would sustain disproportionate harm as a consequence. In the event that the Dutch Data Protection Authority does not inform the interested party of its findings, it shall send the aforesaid party such information as it deems appropriate.

Article 65 Dutch Data Protection Act

The Dutch Data Protection Authority is authorised to apply administrative measures of constraint pursuant to the obligations laid down by or under this Act.

Article 66 Dutch Data Protection Act

1. The Dutch Data Protection Authority may impose an administrative penalty not exceeding the amount of the fine of the fourth category of article 23, paragraph 4, of the Criminal Code regarding violations under or pursuant to articles 4, paragraph 3, or 78, paragraph 2, heading and under a.
2. The Dutch Data Protection Authority may impose an administrative penalty not exceeding the amount of the fine of the sixth category of article 23, paragraph 4, of the Criminal Code regarding violations under or pursuant to articles 6 up to and including 8, 9, first and paragraph 4, 10, paragraph 1, 11 up to and including 13, 16, 24, 33, 34, first, second and paragraph 3, 34a, 35, paragraph 1, second sentence, second, third and paragraph 4, 36, second, third and paragraph 4, 38 up to and including 40, second and paragraph 3, 41, second and paragraph 3, 42, first and paragraph 4, 76, 77 or 78, third and paragraph 4, as well as of article 5:20 of the General Act on Administrative Law.
3. The Dutch Data Protection Authority does not impose an administrative penalty for a violation under or pursuant to the articles mentioned in article 66, paragraph 2, unless it has given a binding instruction. The Dutch Data Protection Authority may set a deadline for the violator within which the instruction must have been followed.

4. Paragraph 3 does not apply if the violation was committed intentionally or was the result of serious culpable negligence.
5. The Dutch Data Protection Authority may impose an administrative penalty not exceeding the amount of the fine of the sixth category of article 23, paragraph 4, of the Criminal Code in case of non-compliance with binding instruction. Article 23, paragraph 7, of the Criminal Code shall apply mutatis mutandis.

Article 1.1 Telecommunication Act (TA)

For the purposes of this Act and the provisions based upon it, the following terms shall be understood to have the meanings assigned to them below:
[…]

f. electronic communications service: a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals via electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but excluding services providing, or exercising editorial control over, content transmitted using electronic communications networks and services. It does not include services provided by the information society, as defined in Article 1 of the Notification Directive, which do not consist wholly or mainly in the conveyance of signals via electronic communications networks;
g. publicly available electronic communications service: an electronic communications service that is available to the public;

Article 11.3a TA

1. The provider of a publicly available electronic communications service shall notify the Dutch Data Protection Authority immediately of any breach of security within the meaning of article 11.3 that has negative consequences for the protection of personal data processed in connection with the provision of a publicly available electronic communications service within the European Union.
2. The provider, as referred to in paragraph 1, shall immediately notify the party whose personal data are concerned of a breach in connection with personal data if that breach is likely to have adverse consequences for the personal privacy of the data subject.
3. The notification to the Dutch Data Protection Authority and to the person whose personal data are concerned shall comprise in any case the nature of the breach in connection with personal data, the bodies from which more information can be acquired regarding the breach, and the recommended measures to limit the negative consequences of the breach. The notification to the Dutch Data Protection Authority shall also comprise the consequences of the breach for the personal data and the measures that the provider proposes or has taken in order to deal with the breach.
4. If the provider of a publicly available electronic communications service fails to provide notification within the meaning of paragraph 2, the Dutch Data

Protection Authority, if it considers that the breach in connection with personal data is likely to have adverse consequences for the personal privacy of the person whose personal data are concerned, may require the provider to notify the data subject after all.

5. The notification within the meaning of paragraph 2 shall not be required if the Dutch Data Protection Authority considers that the provider has taken appropriate technical protection measures whereby the personal data concerned are encrypted or otherwise incomprehensible for any party that is not entitled to access those data.
6. The provider of a publicly available electronic communications service shall keep an overview of all breaches in connection with personal data. Said overview shall in any case comprise the facts and the data within the meaning of paragraph 3.
7. Specific rules may be set by or pursuant to a general administrative order regarding the requirements within the meaning of the present article for the provision of information and the notification.

Article 4 Regulation No. 611/2013

1. In derogation from article 3, paragraph 1, notification of a personal data breach shall not be required if the provider has demonstrated to the satisfaction of the competent national authority that it has implemented appropriate technological protection measures, and that those measures were applied to the data affected by the security breach. Such technological protection measures shall render the data unintelligible to any person who is not authorised to access those data.
2. Data shall be considered unintelligible if:
   a) they have been securely encrypted with a standardised algorithm, the key used to decrypt the data has not been compromised in any security breach, and the key used to decrypt the data has been generated so that it cannot be ascertained by available technological means by any person who is not authorised to access the key; or
   b) they have been replaced by their hashed value calculated with a standardised cryptographic keyed hash function, the key used to hash the data has not been compromised in any security breach, and the key used to hash the data has been generated in a way that it cannot be ascertained by available technological means by any person who is not authorised to access the key.
3. After having consulted the competent national authorities via the Article 29 Working Group, the European Network and Information Security Agency and the European Data Protection Supervisor, the Dutch Data Protection Authority may publish an indicative list of appropriate technological protection measures, referred to in paragraph 1, according to current practices.