IMMA Privacy reference architecture

www.beterbenutten.nl/imma
IMMA Privacy reference architecture
Foreword

It is vitally important to stimulate a change in the behaviour of road users in order to optimise use of the road network. If road users choose different travelling times and routes or other means of transport, we can all make optimal use of our road network. The success of peak-traffic avoidance and bicycle incentive projects shows that travellers are sensitive to this type of stimulation. That is why, based on the Optimising Use programme, we want to facilitate these demand-influencing projects and traffic surveys with IMMA, Integral Mobility Management Architecture.

Based on the lessons learned from demand-influencing projects, IMMA is developing trusted products that can be used to organise and implement demand-influencing projects and traffic surveys in a more uniform, efficient and verifiable way. These products include a Programme of Requirements with clear qualifications for market parties. They also include the joint development of innovative technologies in order to recruit participants and stimulate and reward certain behaviour. IMMA is developing quickly and the project is very successful. This shows that the project is meeting the needs of market parties and the public authorities.

Innovative technologies and behavioural change in mobility are closely related to safety and privacy. When innovative technologies are used to change behaviour, they must comply with statutory requirements in the area of privacy and personal protection and, where possible, they must also respond to new European requirements. But how can you as a public authority or market party do this? Which rules and conditions apply and who is responsible?

This IMMA Privacy reference architecture unambiguously specifies and clearly explains the numerous statutory requirements related to privacy. It includes examples that can be used to translate the requirements to your specific situation. This guide was created in close co-operation with Considerati (legal advisors).

In this way, IMMA projects give travellers the assurance that their privacy will be fully protected at all times. We wish you the very best with your IMMA projects.

Katya Ivanova
Programme Manager Maastricht-Bereikbaar, urban region for IMMA.
# Table of contents

## 2 Background 9

## 3 Glossary 10

## 4 General explanation privacy legislation 12

4.1 Dutch Data Protection Act 13

4.2 General Data Protection Regulation 14

4.3 Dutch Cookie Law 14

## 5 Privacy by Design 15

## 6 Overview IMMA privacy requirements 17

6.1 Responsibility 18

6.2 Legitimate objective and legal basis 18

6.3 Data minimisation 18

6.4 Purpose limitation 18

6.5 Information and transparency 19

6.6 Sharing data with third parties 19

6.7 The rights of the data subject 19

6.8 Information security 19

6.9 Storing and destroying data 19

6.10 Data export 19

## 7 Responsibility 20

7.1 Requirement 21

7.2 Statutory provisions 21

7.3 Explanation 21

7.4 Examples 22

## 8 Legitimate objective and legal bases 26

8.1 Requirement 27

8.2 Statutory provisions 27

8.3 Explanation 27

8.3.1 Objective 27

8.3.2 Legal bases 28

8.4 Examples 32

## 9 Data minimisation 36

9.1 Requirement 37

9.2 Statutory provisions 37

9.3 Explanation 37

9.4 Examples 39

## 10 Purpose limitation 41

10.1 Requirement 42

10.2 Statutory provisions 42

10.3 Explanation 42

10.4 Examples 44
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>Information and transparency</td>
<td>46</td>
</tr>
<tr>
<td></td>
<td>11.1 Requirement</td>
<td>47</td>
</tr>
<tr>
<td></td>
<td>11.2 Statutory provisions</td>
<td>47</td>
</tr>
<tr>
<td></td>
<td>11.3 Explanation</td>
<td>47</td>
</tr>
<tr>
<td></td>
<td>11.4 Examples</td>
<td>49</td>
</tr>
<tr>
<td>12</td>
<td>Sharing personal data with third parties</td>
<td>51</td>
</tr>
<tr>
<td></td>
<td>12.1 Requirement</td>
<td>52</td>
</tr>
<tr>
<td></td>
<td>12.2 Statutory provisions</td>
<td>52</td>
</tr>
<tr>
<td></td>
<td>12.3 Explanation</td>
<td>52</td>
</tr>
<tr>
<td></td>
<td>12.4 Example</td>
<td>53</td>
</tr>
<tr>
<td>13</td>
<td>Rights of the data subject</td>
<td>55</td>
</tr>
<tr>
<td></td>
<td>13.1 Requirement</td>
<td>56</td>
</tr>
<tr>
<td></td>
<td>13.2 Statutory provisions</td>
<td>56</td>
</tr>
<tr>
<td></td>
<td>13.3 Explanation</td>
<td>56</td>
</tr>
<tr>
<td></td>
<td>13.4 Example</td>
<td>59</td>
</tr>
<tr>
<td>14</td>
<td>Information security</td>
<td>60</td>
</tr>
<tr>
<td></td>
<td>14.1 Requirement</td>
<td>61</td>
</tr>
<tr>
<td></td>
<td>14.2 Statutory provisions</td>
<td>61</td>
</tr>
<tr>
<td></td>
<td>14.3 Explanation</td>
<td>61</td>
</tr>
<tr>
<td></td>
<td>14.4 Examples</td>
<td>62</td>
</tr>
<tr>
<td>15</td>
<td>Storing and destroying data</td>
<td>64</td>
</tr>
<tr>
<td></td>
<td>15.1 Requirement</td>
<td>65</td>
</tr>
<tr>
<td></td>
<td>15.2 Statutory provisions</td>
<td>65</td>
</tr>
<tr>
<td></td>
<td>15.3 Explanation</td>
<td>65</td>
</tr>
<tr>
<td></td>
<td>15.4 Examples</td>
<td>66</td>
</tr>
<tr>
<td>16</td>
<td>Data export</td>
<td>67</td>
</tr>
<tr>
<td></td>
<td>16.1 Requirement</td>
<td>68</td>
</tr>
<tr>
<td></td>
<td>16.2 Statutory provisions</td>
<td>68</td>
</tr>
<tr>
<td></td>
<td>16.3 Explanation</td>
<td>68</td>
</tr>
<tr>
<td></td>
<td>16.4 Example</td>
<td>69</td>
</tr>
<tr>
<td>17</td>
<td>Data breach notification</td>
<td>70</td>
</tr>
<tr>
<td></td>
<td>17.1 Requirement</td>
<td>71</td>
</tr>
<tr>
<td></td>
<td>17.2 Statutory provisions</td>
<td>71</td>
</tr>
<tr>
<td></td>
<td>17.3 Explanation</td>
<td>71</td>
</tr>
<tr>
<td></td>
<td>17.4 Examples</td>
<td>73</td>
</tr>
<tr>
<td>18</td>
<td>Appendix: Articles of law by chapter</td>
<td>74</td>
</tr>
</tbody>
</table>
2 Background

The Optimising Use Programme of the Ministry of Infrastructure and the Environment is aimed at facilitating the development of mobility and peak-traffic avoidance projects and making the results widely applicable within the limits of the law. It is within this framework that the Integral Mobility Management Architecture (IMMA) is being drawn up.

This architecture facilitates a more uniform, efficient and verifiable way of implementing demand-influencing projects and traffic surveys. The processing of personal data and the requirements stipulated in the Dutch Data Protection Act play an important role in the legal framework for mobility projects. This Privacy reference architecture was drawn up as part of the IMMA to make sure that new projects to be developed also comply, with the applicable privacy legislation and regulations. The basic principle must be that the service providers of mobility and peak-traffic avoidance projects start regarding data protection as a licence to operate.

This reference architecture specifies the ‘baseline’ with which projects must comply in order to be privacy compliant. More specifically, it means that the Privacy reference architecture formulates privacy principles, standards and requirements that should be complied with by mobility and peak-traffic avoidance projects on the basis of the applicable legal framework (Dutch Data Protection Act, the forthcoming European General Data Protection Regulation and the Dutch Cookie Law).

It is important to note that the IMMA Privacy reference architecture does not stipulate any new requirements for projects and applications that are not already laid down by law. The reference architecture is intended solely to clarify the obligations of the various parties. In addition, the architecture simply sketches a framework and does not prescribe any specific measures because these should always be assessed by the controller on the basis of the specific application. The controller must take all the specified requirements into account and must be able to justify why certain choices were made when those requirements were being interpreted.

To make this Privacy reference architecture more accessible and easier to use for applicants, examples and, where possible, best practices are included for each requirement.
3 Glossary

Controller
The natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data.

Cookie
Small text files that can be placed on the computer, mobile phone, tablet or other device of a user with the aim of identifying the device.

Data subject
The person to whom the data relates. This can be a consumer (the customer of a peak-traffic avoidance app, for example) but also an employee of a company (for example, an employee whose movements are being followed in the context of fleet management).

Dutch Data Protection Act (Wet bescherming persoonsgegevens (Wbp))
The Dutch implementation of European Directive 95/46/EC, which is aimed at the protection of personal data.

Dutch DPA
Dutch Data Protection Authority (Autoriteit Persoonsgegevens (AP)), the Dutch supervisory authority responsible for monitoring privacy compliance.
**Personal data**
Any information relating to an identified or identifiable natural person.

Identified means that a natural person can be uniquely distinguished from other persons on the basis of identifying data (for example, name and address), or that the person can be singled out in a group.

Identifiable means that a person has not yet been identified, but that identification by the controller and/or third parties is reasonably possible.

**Processing personal data**
Any operation or set of operations which is performed upon personal data. This includes the entire process followed by personal data, from the point of collection to the point of destruction.

**Processor**
The party that processes personal data on behalf of the controller. It does that in accordance with the instructions of the controller and under its (explicit) responsibility, without being under the direct authority of that party. The processor is therefore a person or institution outside the controller’s organisation that has a principal/contractor relationship rather than a hierarchical relationship with the controller.

**Receiver**
The third party to whom personal data is passed on.

**Third party**
The party that is not the data subject, the controller or the processor.
General explanation privacy legislation

For IMMA, the following two laws are important in the area of privacy: the Dutch Data Protection Act and the Dutch Cookie Law. The Dutch Data Protection Act stipulates the rules for the careful processing of personal data. The Dutch Cookie Law (Article 11.7a of the Dutch Telecommunication Act) stipulates that the user must in principle give his/her consent for information to be placed on his/her or her terminal equipment and for information to be retrieved from that terminal equipment.
In the framework of IMMA, two items of legislation specifically play an important role: the Dutch Data Protection Act and the Dutch Cookie Law.

### 4.1 Dutch Data Protection Act

The Dutch Data Protection Act determines when personal data may be processed. The essence of the law is that personal data may only be processed for explicitly defined and legitimate objectives. An objective is legitimate if it can be based on one of the legal bases in the Dutch Data Protection Act (see Article 8 of the Dutch Data Protection Act).

Data may be processed when there is a legitimate objective, but only if it also complies with the procedural requirements laid down in the Dutch Data Protection Act. That relates to security, transparency and respect for the rights of the individual.

In a diagram, the logic of the Dutch Data Protection Act can be displayed in the following way:
4.2 General Data Protection Regulation

The European Union is currently developing legislation that will replace the Dutch Data Protection Act: the General Data Protection Regulation. This law stipulates a number of stricter requirements for the controller, particularly in relation to responsibility and accountability. Because this law has not yet been definitively passed, the new requirements will not yet be included in this reference architecture. Where relevant, however, this reference architecture does look ahead to the requirements of the Regulation so that you can prepare for them.

4.3 Dutch Cookie Law

Article 11.7a of the Dutch Telecommunication Act, popularly known as the Dutch Cookie Law, stipulates that placing information on the terminal equipment of a user (the data subject) or retrieving information from that terminal equipment is in principle only possible if that user has given his/her consent. This does not apply to situations where placing/retrieving data is technically necessary, or where placing/retrieving data results in only a minor infringement of privacy.¹

Because placing a cookie is the most frequently-used way for placing data on terminal equipment and retrieving it, this law is called the Dutch Cookie Law. However, this law explicitly applies to all methods of placing data on terminal equipment and retrieving it from them. This might include the use of Software Development Kits (SDKs), beacons and device fingerprinting. Where we refer to cookies in this document, we explicitly also mean all of these other possibilities.

In addition, ‘terminal equipment’ is a very broad term. It means that the definition includes not just computers but also smartphones, smartwatches, navigation units and even cars.

¹ Besides the use of cookies, the Telecommunication Act also regulates the use of location data. These provisions only apply to the providers of public telecommunication networks and services and are not within the scope of this brochure.
In the future, the Dutch Data Protection Act will be replaced by the European General Data Protection Regulation. Based on this regulation, the design of IT systems and business processes must already take the protection of privacy into account.
On the basis of the upcoming European General Data Protection Regulation, all applications in which personal data is processed must be ‘Privacy by Design’. This means that privacy will be taken into account in the design of IT systems and business processes.

The rule for IMMA projects is that the requirements from the privacy reference architecture as described below need to be included in the design of IMMA applications.

To find out more about the risks of your application, you can conduct or commission a Privacy Impact Assessment (PIA). Based on the results of the PIA, you can take the necessary measures in the area of Privacy by Design. When the Regulation becomes applicable, PIAs will be mandatory for processing operations that present high risks.
6 Overview IMMA privacy requirements

Every IMMA project must comply with eleven requirements in the area of privacy and the protection of personal data. This includes requirements for responsibility and data minimisation and requirements for storing and destroying personal data. In this chapter, we briefly discuss these requirements. In the following chapters, we examine the requirements in more depth.
Every IMMA project must comply with the following requirements in the area of privacy and the protection of personal data:

6.1 Responsibility

- The party responsible for the data processing must be clearly identified
- The controller must make agreements with the processor(s) about the safe and careful processing of personal data.

6.2 Legitimate objective and legal basis

- The reason for processing personal data in the framework of the IMMA application (the processing objective) must be determined in advance and must be described sufficiently clearly
- It must be possible to base the processing of personal data on one of the legal bases of the Dutch Data Protection Act (Article 8 of the Dutch Data Protection Act)
- When unambiguous consent (Article 8a of the Dutch Data Protection Act) is used as a legal basis, it must be requested before the personal data is processed
- When data for the application is placed on the user’s terminal equipment, or information is retrieved from it, this must be done with the consent of the user or the use of the data must be based on one of the exceptions in 11.7a of the Dutch Telecommunication Act.

6.3 Data minimisation

- For the application, no more data than necessary may be used to achieve the application objectives.

6.4 Purpose limitation

- Data may only be processed for the objective for which it was collected, unless the new purpose is compatible with the original objective.

6.5 Information and transparency

- It must be clear to the data subject which personal data will be processed and for which purposes it will be used.
6.6 Sharing data with third parties

• Data may only be shared with third parties if there is a legitimate basis for doing so.

6.7 Rights of the individual

• The application must take the rights of the data subject into consideration and must respect them.

6.8 Information security

• The application must be adequately protected by taking appropriate technical and organisational measures against loss or any other type of unlawful processing.

6.9 Storing and destroying data

• Data must be assigned a retention period
• Data is destroyed or made anonymous when it is no longer required for the processing objectives.

6.10 Data export

• Data may not be sent to a country that does not have an adequate level of privacy protection.

6.12 Data breach notification

• The controller must notify the Dutch DPA about a security breach which results in (a significant chance of) a serious negative impact on the protection of personal data.
• The controller must also notify the data subject about the abovementioned security breach if it can have a negative impact on his or her privacy.
On the basis of the Dutch Data Protection Act, you must clearly identify the party responsible for the data processing. The controller is the natural or legal person which alone or jointly with others determines the purposes and means of the processing of personal data. Both the principal and the contractor can be regarded as the controller. In a joint venture, numerous legal entities can be responsible. A number of examples demonstrate how you can determine responsibility in practice.
7.1 Requirement

- The party responsible for the data processing must be clearly identified.
- The controller must make agreements with the processor(s) about the safe and careful processing of personal data.

7.2 Statutory provisions

This requirement is based on the following statutory provisions:
- Article 1 under d of the Dutch Data Protection Act
- Article 4 of the Dutch Data Protection Act
- Article 14 of the Dutch Data Protection Act.

7.3 Explanation

The controller

The controller is the natural or legal entity that is responsible for processing the data. Because the Dutch Data Protection Act applies to the controller, it is very important to be clear about the identity of the controller, particularly where it involves joint ventures.

The controller is the party that determines the purposes and means of the processing of personal data. Therefore, when data is processed in the framework of a project, it must be specified who the party is that ultimately determines which data should be processed, for which purpose it will be done and which means (money, people, IT facilities) will be used to do it.

In tendering processes, the principal can be the controller, but so can the contractor; this must be examined on a case-by-case basis. In the case of a tender, this does not automatically mean that the principal is also the controller.

Note: The controller is not an individual in an organisation but the organisation (the legal entity) itself.
When there are several controllers – for example, in a joint venture – the mutual relationships and agreements related to this responsibility or co-responsibility must be clearly recorded.

**Processors**
When the controller hires a third party to process personal data at his request, the controller is obliged to make contractual agreements with the processor about how to treat the personal data. In particular, agreements about the security of personal data are important.

### 7.4 Examples

#### Example 1
SnellerThuis BV is developing a peak-traffic avoidance application for public transport. SnellerThuis is granting individuals a discount if they travel outside the peak traffic period. SnellerThuis is collecting the names and addresses, account numbers and travel behaviour of individuals, among other things. SnellerThuis has asked SoftwareBouwer BV to develop the app. The app runs on GoedeHost BV. In this example, SnellerThuis is the controller: it will determine the objective (to collect the data for a peak-traffic avoidance project) and the means (creating an app and hiring third parties for this purpose). In this scenario, SoftwareBouwer BV is not relevant for the Dutch Data Protection Act; GoedeHost BV is a processor.

#### Example 2
One example of a privacy policy in which the controller has been clearly identified is MyOV’s privacy policy. MyOV is a website and app that keeps track of the rail trips made by users and provides discounts or special offers if users travel outside the peak-traffic period. In its privacy policy, Data-Lab B.V. has clearly indicated its identity and business location and the fact that it is the controller for the processing of personal data by this app.

MyOV privacy policy

In order to provide you with the best possible service, we need to process a certain amount of your personal data. Data-lab takes your privacy very seriously and therefore treats your data with the greatest care.

MyOV is a rush-hour avoidance programme that is supplied to you by Data-Lab B.V., Stationsplein 61, 3818 LE Amersfoort. Data-Lab B.V. is the party responsible for processing personal data for MyOV in accordance with the Personal Data Protection Act.
**Example 3**

Another example involves the privacy policy of Praktijkproef Amsterdam, an initiative which, under the name Amsterdam Onderweg, is advising travellers about which route to take if they want to avoid the peak traffic period in Amsterdam. Here, not only the controller is clearly identified, but the processor is also named.

---

De Praktijkproef Amsterdam (PPA) is an initiatief van de gemeente Amsterdam, provincie Noord-Holland, Rijkswaterstaat en de stadsregio Amsterdam. De PPA is een grootschalige proef die zich richt op het verminderen van files in de regio Amsterdam. Tijdens de proef wordt gebruik gemaakt van innovatieve technologieën in de auto en op de weg.

Rijkswaterstaat West-Nederland Noord, gevestigd te Haarlem, is de opdrachtgever van Amsterdam onderweg en is verantwoordelijk voor de verwerking van persoonsgegevens. Amsterdam onderweg, een samenwerking van TNO en ARS Traffic & Transport Technology, gevestigd te Den Haag, is de opdrachtnemer van de PPA en de bewerker van persoonsgegevens.

---

Praktijkproef Amsterdam (PPA) is an initiative of Amsterdam City Council, the Province of North Holland, Rijkswaterstaat and the City Region of Amsterdam. PPA is a large-scale trial that focuses on the reduction of traffic congestion in the Amsterdam region. During the trial, innovative technologies are being used in cars and on the road.

Rijkswaterstaat West-Netherlands North, located in Haarlem, is Amsterdam Onderweg’s principal and is responsible for processing the personal data. Amsterdam Onderweg, a joint venture between TNO and ARS Traffic & Transport Technology, located in The Hague, is PPA’s contractor and the processor of personal data.
**Example 4**

The new app from transport company Syntus enables users to plan their trip, buy tickets and save points by avoiding the peak traffic period when travelling by train. The privacy policy clearly states that Syntus is the controller and its contact data and Chamber of Commerce number are also specified.

---

**General**

The Syntus app is a smartphone app that can be used to plan a trip and buy tickets. The app has an integrated programme in which users can save points by travelling outside the rush-hour. Syntus B.V. (Syntus) supplies the Syntus app, is located on Visbystraat 5, 7418 BE Deventer and is registered with the Chamber of Commerce under trade register number 09102634. In the sense of the Personal Data Protection Act, Syntus is the party responsible for processing personal data for the Syntus app.
8 Legitimate objective and legal basis

The Dutch Data Protection Act stipulates that you may only process personal data for a specified and explicit objective. Moreover, the data processing must have a legal basis, such as the consent of the data subject or the necessity for the performance of a contract. In this chapter, the various legal bases are described and explained. It clearly states which conditions apply to obtaining consent from the user and when data processing is necessary. Examples demonstrate how consent for processing personal data is arranged in practice and how an objective should be clearly described.
8.1 Requirement

• The reason for processing personal data in the framework of the IMMA application (the processing objective) must be determined in advance and be sufficiently specified.

• The processing of personal data must be based on one of the legal bases in the Dutch Data Protection Act (Article 8 of the Dutch Data Protection Act).

• When unambiguous consent (Article 8a of the Dutch Data Protection Act) is used as a legal basis, the consent must be requested prior to processing the personal data.

• When data for the application is placed on the user’s terminal equipment, or information is retrieved from the device, this must be done with consent or its use must be based on one of the exceptions in Article 11.7a of the Dutch Telecommunication Act.

8.2 Statutory provisions

This requirement is based on the following statutory provisions:

• Article 7 of the Dutch Data Protection Act
• Article 8 paragraph a and paragraph f of the Dutch Data Protection Act
• Article 11.7a of the Dutch Telecommunication Act.

8.3 Explanation

8.3.1 Purpose
The intended processing should have a specific, explicit and legitimate purpose. It is not permitted to collect data without first having determined a precise description of the purpose. The description may not be too vague or too broadly formulated. It is, however, permitted to formulate several objectives for each application.
It is also important that the necessity to process personal data is assessed. This means that the controller must ask itself whether the purpose can also be achieved with less data or in a way that requires less personal data to be processed.

8.3.2 Legal bases
For a purpose to be legitimate, it must be possible to base the purpose on one of the legal bases in Article 8 of the Dutch Data Protection Act. If the processing of the data cannot be justified on the basis of one of these objectives, it is not permitted.

The six legal bases are:

a) The data subject has given its unambiguous consent.

b) The processing is necessary for the performance of a contract to which the data is subject or is party.

c) The processing is necessary for compliance with a legal obligation to which the controller is subject.

d) The processing is necessary in order to protect the vital interests of the data subject.

e) The processing is necessary for the performance of a task carried out in the public interest by the controller.

f) The processing is necessary for the purposes of the legitimate interests pursued by the controller, which outweighs the infringement on the individual's privacy.

For IMMA projects, Articles 8a, 8b and 8f of the Dutch Data Protection Act will be particularly relevant.¹

Article 8a of the Dutch Data Protection Act: Unambiguous consent given by the data subject
When processing is not per se necessary, the data may only be processed if the data subject has given its consent to do so.

¹ The ‘legal obligation’ legal basis relates to a statutory obligation that rests with the controller, such as supplying data to the Tax and Customs Administration to implement the tax legislation. Although this legal basis can apply, it will not necessarily be the basis for implementing a mobility project. The ‘protection of vital interest’ legal basis relates to life-and-death situations and will not apply to mobility projects. The ‘the performance of a task carried out in the public interest’ legal basis can only be deployed by public-law organisations such as Ministries and implementing bodies.
If you use the unambiguous consent of the data subject as the legal basis for processing, this consent must comply with the following requirements:

- The consent must be given freely. This means that refusal of consent may have no negative consequences for the data subject. Bear in mind that in most cases employees cannot give consent. They are not free because they have a dependent relationship with the employer. For telematics and fleet management, for example, consent is therefore a less suitable legal basis.

- The consent must be based on clear information. The data subject must know what he/she is giving consent for – for example, that his/her location data will be used to map out the traffic flows on his/her route. This information must also be easily accessible. For example, it is not permitted to conceal the information in the general conditions and then ask the data subject to agree with those conditions.

- The previous requirement also means that the consent must be concrete and specific. It is only when the purpose is sufficiently specific that consent can be given. For example “we are processing your data to improve our business operations and improve mobility in the Netherlands” is too vague. The data subject should have no doubts about what he/she is giving his/her consent for.

- The consent must be given before the data is processed. In other words, the data may not be processed (not even collected) before consent has been given. When something substantial changes in the processing (more personal data, new objectives), you must renew the consent.

- The consent must be unambiguous. This means that it must be clear that the data subject has given consent and for what. No procedural requirement applies to the consent, but the consent must be expressed. Implied consent (silence means consent, for example) is not valid. There must be positive action by the data subject on the basis of which you can assume that consent has been given. This can be verbal, written or behaviour-based. A pre-checked box is not allowed, for example. The data subject must check the box himself/herself, and only then is it clear that the data subject has actually expressed his/her wish.
The burden of proof for having obtained the consent and for acknowledgement by the data subject of the information that is provided lies with you as the controller. You must therefore be able to show that there was no possibility that the data subject had any doubt about the purposes of the processing and the giving of consent. It is therefore important that your ‘opt-in flow’ is sufficiently clear. In addition, document this ‘opt-in flow’ properly so that you can show how the consent was obtained. Here, version management is also important: if the consent for your 1.0 app was different to the consent for your 2.0 app (for example, you are processing data for new purposes), then you should record the differences between the various versions.

Lastly, remember that the data subject can withdraw his/her consent at any time. The consequence of this is that, as the controller, you no longer have a legal basis for processing this data subject’s personal data. In specific terms, this means that you may no longer use this individual’s data for the objective for which you obtained it unless there is another legal basis on which you can base the processing of data (for example, you have a statutory obligation to keep the data available for the Tax and Customs Administration).

*Article 11.7a of the Dutch Telecommunication Act: Consent for cookies and similar technologies*

If you are using cookies or similar technologies in your application, you must also ask for consent in a number of cases. Please note that this consent specifically relates to placing the cookies (and retrieving them). This consent is in addition to the legal basis for the processing of personal data. You must therefore ask permission to place the cookies, but then you must also have a legitimate objective for the data that you collect with this cookie (for example, permission once again).

For consent based on the Dutch Cookie Law, the requirements specified above also apply.

With regard to placing cookies or similar technologies, there are three exceptions to the consent requirement. In the following three cases, the requirement to obtain consent does not have to be complied with:

- Technically necessary cookies, such as load balancing cookies.
- Functional cookies: these cookies are necessary because if they are not placed the requested service will function badly or not at all. For example, paying at a webshop, language settings and currency settings.
• Cookies for measuring the effectiveness and quality of a service. For example:
  - analytical cookies that analyse and map out use of the app so that quality and/or effectiveness can be improved;
  - affiliate cookies: to keep track of which advertisement leads to the purchase of a particular product, so that the party that displayed that advertisement (the affiliate) can receive a particular reward from the advertiser.

*Article 8b of the Dutch Data Protection Act: necessary for the performance of a contract*
The data may be processed when it is necessary for the performance of a contract with the data subject. For example: processing name and address data and an account number in order to transfer the payments for peak-traffic avoidance.

*Article 8f of the Dutch Data Protection Act: Necessary for the purposes of your legitimate interests*
If you base the use of the application on this legal basis, you should give careful consideration to the balance between your legitimate interest and the privacy interest of the data subject. When making this consideration, the following aspects play a role:
• The nature of your legitimate interest
• The sensitivity of the data
• The impact on the data subject and his/her reasonable expectation of what will happen with his/her data, as well as the nature of the data and how it is processed
• Additional safeguards that can minimise the impact for the data subject, such as data minimisation and privacy-enhancing technologies.

Geo-location data, for example, is regarded as sensitive data because it accurately depicts the habits and patterns of the data subject. When you use this data for purposes other than implementation of the agreed mobility services, the balance will generally be in favour of the data subject. If, for example, you want to use the geo-location data for marketing or analysis purposes, the unambiguous consent is therefore more self-evident.

In addition, the processing should be necessary in order to represent your interests. This means that your interests cannot be served in another way with less drastic means or with less data (subsidiarity).

---

3 N.B.: This exception only applies if the cookie has no impact or only a minor impact on the privacy of the data subject. More than a minor impact includes the (unintended) forwarding of the data to third parties.
When do you have a legitimate interest?

If you cannot do your job properly without processing personal data, you have a legitimate interest. One example of a legitimate interest involves conducting good business operations. A legitimate interest is not limited to your core activities but can also relate to activities that are closely related to them. However, you must be able to justify your interest to the data subject.

8.4 Examples

Example 1 (consent)

Screenshot of the Apple App Store. Before downloading the application (Angry Birds 2), Rovio’s privacy policy can be consulted. Although this complies with the information requirements, no unambiguous consent for processing the personal data may be derived from downloading the application.
**Example 2 (consent)**

A good example of an app that clearly and unambiguously requests consent after installation of the app (but before the personal data is processed) is the TomTom App.

After installation, the app clearly asks for consent before data is processed. The app first defines the exact data that will be collected (location), why it will be collected (the purpose of collecting the data), and then asks for the user’s consent and clearly indicates where more information can be found.

---

**Your data**

We need to know your location …

… to display traffic information about your route.

May this app send your data, when necessary?

- No
- Yes

More information >
**Example 3 (consent)**

Example of an opt-in using the inbuilt consent in iOS. Before using and processing the data, this weather app asks whether the user will allow his/her location data to be processed. This consent is sufficiently specific and concrete.

**Example 4 (definition of the purpose)**

A good example of a processing purpose that has been described sufficiently clearly can be found when registering on the website for the Spitsmijden Galecopperbrug peak-traffic avoidance project.

---

Yes, I would like to take part in Spitsmijden Galecopperbrug!
Licence number*:

Choose an option*:
- purchased the car before 1 January 2015.
- purchased the car on or after 1 January 2015, namely on:
Date of registration: 2015-01-01
Date format: yyyy-mm-dd. Example: 2015-04-25

Explanation: Spitsmijden Galecopperbrug needs this information with respect to the measurements we made over recent months. Based on these measurements, we have determined the rush-hour(s) in which you regularly drive and why you are therefore taking part in Spitsmijden Galecopperbrug.
Example 5 (consent)
Another example is the MyOV app, which, before registration in the app, reiterates the reason why the data is being processed.

Conditions
travels outside the rush-hour. We need to obtain your personal data and your travel behaviour through your OV-chipkaart.nl account or through your corporate card publisher in order to: enable this app to work, give you points and travel advice, apply for your refund if you forget to check out or to process it if you are delayed, give you personal travel advice, present you with personal offers and implement our anonymous analyses. By logging on to this app, you give us permission to process your personal data for the above objectives. See our privacy policy for more information.

I agree with the general conditions
Continue

Example 6 (consent for zero measurement)
The following is an example of the correct way to formulate consent as the legal basis for a zero measurement:

“I agree with the collection of my data, consisting of X, Y, Z, which is aimed at taking measurements on the basis of which I may be selected for a peak-traffic avoidance project.”

This opt-in is separate from all other possible consents that are necessary (for any other purposes of the app or application). Ideally, this should also be requested separately and must not be included in any other consent.
9 Data minimisation

Personal data may only be processed when that data is strictly necessary for the processing purpose. This is the essence of the data minimisation requirement. This chapter also deals with the anonymous processing of personal data or processing under a pseudonym. The Dutch Data Protection Act does not apply to anonymous data. By way of clarification, we include two practical examples of data minimisation.
9.1 Requirement

*For the application, no more data than necessary to achieve the purposes of the application may be used (without the consent of the data subject).*

9.2 Statutory provisions

This requirement is based on the following statutory provisions:

* Article 11, section 1 of the Dutch Data Protection Act.

9.3 Explanation

By law, data may only be processed if it is required to achieve the purpose (see requirement legitimate purpose and legal basis). Data that is not strictly necessary for the processing purpose may not be processed.

*Note: At the same time, it is important to ensure that not too little data is collected (there must be sufficient data)!*
**Processing data anonymously and under a pseudonym**

In the context of data minimisation, besides the non-collection of data the concepts of processing data anonymously and under a pseudonym are also relevant.

Anonymous data is data with which the person cannot be identified by you or a third party, taking into account all plausible technologies that can be used in order to identify a person.

Numerous technologies are available for processing data anonymously, but the Dutch Data Protection Act does not prescribe a specific technology. The optimal choices should be made on a case-by-case basis.

When data is processed completely anonymously, the following three criteria must be met:
1. it is no longer possible to remove an individual from a data set
2. it is no longer possible to link the data to an individual
3. no information about an individual can be derived.

The Dutch Data Protection Act does not apply to anonymous data (because it is not personal data).

**Processing data under a pseudonym**

Processing data under a pseudonym involves replacing identifying characteristics (family name, first name, etc.) with non-identifying data items (X, Y, Z or 1, 2, 3, etc.) This makes it possible to process extra data related to the data subject without revealing his/her identity. This reduces the possibility of linking the data set to the individual. The difference between processing data under a pseudonym and processing data anonymously is that pseudonymisation enables you as the controller to reverse the process (the controller possesses the ‘key’). Processing data under a pseudonym is therefore not a way of realising data minimisation.
9.4 Examples

To map out the traffic on a particular route, only the location data of the vehicles needs to be registered. It is therefore not necessary, for example, to register the licence number and the name and address of the data subject, unless the intention is to make this person eligible for an invitation for a peak-traffic avoidance programme based on his/her location data.

Example 1
The MyOV app processes personal data in order to provide personal travel advice. However, MyOV also uses travel data to find out more about travel movements. Given that this purpose does not require data that can be traced to an individual, MyOV has made this anonymous. This safeguards the principle of data minimisation.

Why does MyOV need my travel data?
We analyse your travel behaviour so that we can give you personal travel advice. This primarily involves the possibility of avoiding the rush-hour. If there is relevant information available about your route (such as information about capacity, malfunctions or the weather), we can also include this information and gear your personal travel advice to it. In this way, we can recommend a more comfortable or faster alternative.

Your travel data is also necessary to process your refund applications if you forget to check out or are delayed.

Anonymous use of travel data
Your travel data and that of other travellers is made anonymous, merged and used to gain a better understanding of people’s travel movements. This statistical information can be useful for transporters – for example, to improve the deployment of materials, timetables, location of check-in/out columns, etc.

We wish to emphasise that the data that we collect for this purpose cannot be traced back to you in any way whatsoever. We make all the data about travel movements anonymous and this cannot be reversed.
**Example 2**

The Syntus app processes personal data in order to provide personal travel advice and present travellers with special offers. However, Syntus also uses this travel data to find out more about travel movements. Given that this purpose does not require data that can be traced to a person, Syntus has made this anonymous. This safeguards the principle of data minimisation.

---

**Anonymous use of travel data**

Your travel data and that of other travellers is made anonymous and merged to gain a better understanding of people’s travel movements. Syntus can analyse this statistical information, for example, to deploy materials, improve timetables, etc. We wish to once again emphasise that the data that we collect for this purpose cannot be traced back to you in any way whatsoever and can also no longer be reversed.
In principle, you may only process personal data for the purpose for which it was collected. Further processing is only permitted when the new purpose is compatible with the original purpose. This is assessed on the basis of various factors, such as the sensitivity of the personal data and the consequences of further processing for the user. This chapter discusses five factors that are important for a good assessment.
10.1 Requirement

*Data may only be processed for the purpose for which it was collected unless the new purpose is compatible with the original purpose.*

10.2 Statutory provisions

This requirement is based on the following statutory provisions:

- Article 7 of the Dutch Data Protection Act
- Article 9, sections 1 and 2 of the Dutch Data Protection Act
- Article 11, section 1 of the Dutch Data Protection Act.

10.3 Explanation

The intended processing should have a specific, explicit and legitimate objective. It is important that the necessity of the processing of personal data is assessed. This means that the controller must ask itself whether the purpose can also be achieved with less data or in a way that requires less personal data to be processed. In addition, the data may not be processed further in a way that is incompatible with the original purpose.
To assess whether further processing is permitted, all the relevant circumstances of the case must be taken into consideration. In particular, the following important factors must be taken into account:

- The degree of similarity between the original purpose and the purpose of further processing. The more similar the two purposes (or, rather, the more closely related they are), the sooner the further processing will be compatible with the purpose for which the data was collected.

- The context in which the data was collected and the reasonable expectation of the data subject regarding the further use of his/her data.

- The nature of the data. The more sensitive the data for the data subject, the less quickly you should assume that this data may also be used for other purposes. By sensitive data is not only meant the special categories of data but also data that is generally regarded as sensitive, such as geo-location data.

- The consequences of the further processing on the data subject; i.e., that further processing will be particularly incompatible if a particular decision is made about the data subject as a consequence of the further processing.

- The safeguards that were realised by the controller to ensure that the data is being processed properly and carefully and that avoids any unnecessary impact on the data subject.

You must include all of the above factors in your assessment. One factor does not necessarily weigh more than another.
10.4 Examples

Example 1

A supermarket introduces a personal loyalty card for its customers. Customers with the loyalty card receive a discount on their shopping. In exchange, the supermarket registers all the customer’s purchases by name and on that basis makes specific special offers. Customers give consent for this purpose. The supermarket then decides to sell the data to an insurance company. This purpose is not compatible with the original purpose for which the data was collected.

Register
Welcome to Amsterdam Onderweg, which is part of Praktijkproef Amsterdam!

Now that you are a participant, the Superroute app will soon provide you with reliable travel times, congestion information, departure recommendations and a choice of alternative routes. You will also receive feedback about your trip and travel times for your chosen route and alternative routes to your destination. Besides your commuting route from A to B, you can also use the Superroute app for travel advice to events in the Amsterdam region.

Good luck!

Yes, I would like to take part in Amsterdam Onderweg, part of the unique Praktijkproef Amsterdam!

Please fill in your email address:
Email address:
Register

4. Collecting, managing and processing personal data

Personal data is collected, managed and processed in accordance with the Dutch Data Protection Act. The smartphone app registers the route driven by a participant. The exact departure location cannot be traced. Participants can check their journey registrations on their personal page (see 9). Aggregated, anonymous analyses of the project results are shared with the client and the responsible party, RWS. RWS has no access to the personal data related to the travel behaviour of the PPA participants. RWS may only access the personal data of participants (such as name, address and telephone number) to recruit ‘mystery users’. The specified data may only be used for this objective and only after participants have given their explicit permission. In addition, the individual travel behaviour data that is linked to survey results is shared with the Ministry of Infrastructure and Environment (Directorate General Mobility). This is done so that the effects of the mobility projects in Netherlands can be analysed and compared. This data flow is also anonymous and does not contain any personal data.

Processing is limited to the data that is relevant for the processing objective.
Example 2
When you register with Amsterdam Onderweg, the following screen is displayed. If a password must be entered later, the user is asked to agree with the privacy policy. This notice specifies that the controller, RWS, may only process user data in order to recruit ‘mystery users’. It may therefore not use this data for other purposes – for example, for marketing purposes.
11 Information and transparency

The Dutch Data Protection Act and the Dutch Telecommunication Act stipulate that a user must be aware of which personal data you are processing about him and for which purpose you are processing it. Users are entitled to receive complete information. This chapter lists the subjects about which you must provide users with exact information and how you can formulate that information properly. For example, you must display easily legible information in a visible location. In addition, the transparency requirements for cookies and similar technologies will also be reviewed.
11.1 Requirement

*It must be clear to the data subject which personal data is being processed and for which purposes it will be used.*

11.2 Statutory provisions

This requirement is based on the following statutory provisions:

- Article 33 of the Dutch Data Protection Act
- Article 34 of the Dutch Data Protection Act
- Article 11.7a of the Dutch Telecommunication Act.

11.3 Explanation

The data subject must be provided with all essential information about what you are doing with the data you are collecting. This means that they must be informed about the processing purpose and their rights before their personal data is processed.

The data subjects must be notified about the following:

- The identity of the controller
- The purposes of the application
- Which data is being processed
- The purpose for which the data is being used
- Third parties to whom you are supplying data
- For how long the data will be stored
- How the data subject can exercise his/her rights (see Chapter 13).
The following requirements also apply:

- The information must always be displayed in an (immediately) visible location. Examples include an easy-to-find link on a website or an app or a special screen displayed during the installation process.
- The information must be in a language that the target group understands. In any case, make sure that the reading level of the texts is B1 Dutch, where possible, and avoid complicated legal texts.
- A global reference to general conditions, privacy and/or permission statements is not enough information.
- Make sure that the information is well structured so that the user can easily understand it. One good example of this is a layered privacy statement. You should also take the type of device into account. For example, a link to a privacy statement on a website is often not very easy to read on a smartphone’s smaller screen.

**Special regime for cookies and similar technologies**

If you are using cookies or similar technologies in your application, before placing the cookie you should notify the data subjects in a privacy or cookie policy about the following aspects:

- Which cookies are being placed.
- The types of personal data that are being collected and processed with the cookies.
- The purpose of the data processing.
- Third parties to whom you are supplying the data.
- The life span of the cookie.

There are three exceptions to the information requirement for placing cookies or similar technologies. You are not obliged to supply information about the use of technical cookies that are strictly necessary, functional cookies that the user has requested and analytical cookies with a minor impact on privacy. You therefore do not have to ask the data subject for consent to place these cookies.

---

4 For more information, go to: https://www.acm.nl/nl/onderwerpen/telecommunicatie/internet/cookies/
11.4 Examples

Example 1
An example of a layered privacy statement. The blocks outline what happens with the data, when clicking the ‘read more’ button more detailed information can be found.
Example 2
Example of a cookie message (NPO). The objectives are clearly indicated and there is an option to refuse advertising cookies.

The Dutch Public Broadcaster (NPO) uses cookies. We make a distinction between functional cookies and cookies for managing web statistics, advertisements and social media. NPO uses functional and analytical cookies to monitor the operation and effectiveness of its websites. The data collected in this way is not used to track the activities of individual users. The advertisement and social media cookies of third parties may also collect data outside the websites of the NPO. You can use the settings displayed opposite to refuse these cookies. By clicking on I Agree or by continuing to use this website, you give your permission for the use of cookies when you visit NPO’s websites. Would you like to know more about these cookies, or do you want to change the cookie settings for our websites? Then click on More Information.
Sharing personal data with third parties

A legal basis is required to share personal data with third parties. For example, Article 8c of the Dutch Data Protection Act can apply as a legal basis if you are legally obliged to share particular personal data. But in most cases the user’s consent is required to share personal data with third parties.
12.1 Requirement

Data is only shared with third parties if there is a legitimate legal basis for it.

12.2 Statutory provisions

This requirement is based on the following statutory provisions:

- Article 8 of the Dutch Data Protection Act
- Article 17, section 3 of the Dutch Data Protection Act
- Article 19, section 2 of the Dutch Data Protection Act
- Article 20, section 2 of the Dutch Data Protection Act.

12.3 Explanation

Because sharing data with third parties is a form of data processing, a legal basis is also required for this. When it is necessary to share data for the performance of a contract, Article 8b of the Dutch Data Protection Act can be applied. When the controller has a legal obligation, Article 8c of the Dutch Data Protection Act can serve as a legal basis. In most cases, however, the consent of the data subject will be required to supply data to third parties (Article 8a of the Dutch Data Protection Act).

Note: Bear in mind that when apps are being developed components from third parties (such as software development kits) or APIs from third parties are used and that data can also be sent to these third parties. Make sure that you sign agreements with your app builder about the use of these types of components and check which data is exchanged using plug-ins and APIs.
12.4 Example

Example 1
When a user uses the Facebook button in Angry Birds 2, a large amount of data is shared between Rovio and Facebook. The user must give his/her consent for this.

Register with Facebook

Angry Birds 2 receives the following information: your public profile, a list of your friends, your email address and your date of birth.

Edit specified information

In this way, you ensure that the app cannot post any messages on Facebook.
Example 2
The Syntus app has clearly indicated in its privacy policy that, in principle, data is not passed on to third parties. If data is indeed supplied to third parties, Syntus ensures that this is based on a legitimate legal basis: either on the user’s explicit consent (Article 8a of the Dutch Data Protection Act) or to comply with a legal obligation (Article 8c of the Dutch Data Protection Act).

Passing on data to third parties
Syntus does not pass on your personal data to third parties unless this is legally required or you have been asked for your explicit consent.
If a user's personal data is being processed, he/she has a right to access, a right to correction and in some cases a right to object. Based on these rights, he/she can object to inaccurate or incomplete personal data. In this chapter, we describe how to properly deal with a request for access and a request for correction, and how you must assess and handle an objection to the processing of personal data. We use an example to show how a clear access procedure might look.
13.1 Requirement

_In the application, the rights of the individual are taken into account and complied with._

13.2 Statutory provisions

This requirement is based on the following statutory provisions:

- Article 35 of the Dutch Data Protection Act
- Article 36 of the Dutch Data Protection Act
- Article 40 of the Dutch Data Protection Act.

13.3 Explanation

The data subject has particular rights with regard to the processing of his/her personal data. This is to ensure that the data subject knows which data related to him will be processed, that he/she can object to incorrect or incomplete data and make sure that data that is no longer relevant is deleted.

*Right to access*

The data subject has the right to access his/her personal data. The data subject may make such a request at reasonable intervals. To protect the privacy of third parties, it is important to properly confirm the identity of the data subject so that no personal data is made available to the wrong person. Unless the identity of the data subject can be confirmed in a less drastic way (for example, by asking predefined audit questions), the data subject can be asked to show an ID when making a request. However, you should tell the data subject not to use his/her passport photograph, social insurance number or machine-readable zone (MRZ) (the bottom row of numbers and letters on a passport) because this sensitive data is not necessary for identification.
Any request for access must be answered in writing within four weeks.

The answer to the request must contain the following components:
- A full overview of the processed data belonging to the data subject
- A description of:
  - The purpose of the data processing
  - The categories of data to which the processing relates
  - The receivers or categories of receivers.
- All the available information about the origin of the data.

The data subject is also entitled to access possible profiles that are based on his/her location data.

You must supply the data in an ‘understandable format’. You must therefore be able to indicate which data it involves and how it will be used. The meaning of ‘understandable’ depends on the particular situation. For example, a user may have difficulty interpreting a printed list of GPS coordinates. In such case, it is helpful to plot the GPS coordinates on a map for the user.

It cannot be excluded that access to data may also reveal data that relates to other people. As the controller, at the point at which that you can reasonably expect a third party to have any reservations you must notify that third party about the request for access.

At the point at which the access also reveals data related to third parties, as the controller you will have to weigh up the various interests. Where relevant, you can refuse access and invoke Article 43, section e of the Dutch Data Protection Act (in the interest of protecting the rights and freedoms of others).

**Right to correction**
In addition, the data subject can ask for the data to be improved, complemented, deleted or blocked. You must respond to this request in writing within four weeks. Such a request only needs to be granted if the data is factually incorrect, incomplete or not relevant to the processing purpose or is being processed in a way that is contrary to a provision of the Dutch Data Protection Act or another law.
The right to object

If the processing is based on the legal principle ‘necessary for the purposes of the legitimate interests pursued by the controller’, the data subject is entitled to object to data processing in relation to special personal circumstances. This objection must be assessed, and if the objection is justified you should stop processing the data of the data subject. During this test, you should take a close look at how you have designed aspects such as proportionality, subsidiarity and measures to protect privacy.

ACCESS TO YOUR REGISTRATION

>> About your registration

Contact us
If would like more information about your registration, please email a copy of your identity document and your data by pressing the button below.

Retrieve your data here
To prevent other people from retrieving your data, Experian should confirm that you are the person to whom the data relates. This is only possible with a copy of your driving licence, passport, identity card or other proof of identity.

It is important both for you and for us that your information is correct. After all, Dutch Data Protection Act obliges Experian to treat your data conscientiously and carefully.

We wish to point out that the Dutch Data Protection Act entitles you to block out your social security number and passport photograph on the copy of the identity document that you send us. In the examples below, you can see which data you can block out.

Retrieve your data here.
If would like more information about your registration, please email a copy of your identity document and your data.

About your registration
Here you can find the most frequently asked questions and answers about your right to access.

Frequently-asked questions

Information about your registration
Telephone:
0800-experian/0900-397 374 28
(45ct/pm)

Mail:
PO Box 16604
2600 BP The Hague
13.4 Example

Example 1
Data company Experian has a clear access procedure that can easily be accessed by the data subjects. In addition, it shows how a data subject can prove his/her identity online without having to share sensitive data with Experian.
To prevent loss or the unlawful processing of personal data, appropriate physical, technical and organisational measures are required. The weight of these measures depends on the risks and the nature of the personal data and on the (technical) possibilities and costs. We recommend that you comply with the recognised standards for these measures. In this chapter, you can read more about the specific measures that you can take, from the security policy to making processor agreements.
14.1 Requirement

The application must be sufficiently protected by appropriate technical and organisational measures to prevent loss or any other type of unlawful processing.

14.2 Statutory provisions

This requirement is based on the following statutory provisions:

- Article 13 of the Dutch Data Protection Act
- Article 14 of the Dutch Data Protection Act.

14.3 Explanation

You should take appropriate physical, technical and organisational measures to prevent loss or the unlawful processing of personal data. To do this, you should weigh up the risks and the nature of the data, taking into account the state of the technology and the costs. Appropriate security measures prevent unnecessary processing. In addition, the security should be adequate; you should therefore regularly check whether the security needs to be adapted to technological developments. You are advised to realise security in accordance with recognised standards such as ISO 27001 and 27002. If you are processing credit card data, you must also comply with the PCI standard.5

The Dutch DPA has drawn up guidelines for the security of personal data that provide a framework for the efficient protection of personal data.6 However, the Dutch DPA does not have a predefined standard for security as this is governed by the ISO standards.

and [https://www.pcisecuritystandards.org](https://www.pcisecuritystandards.org)

Processor agreement
If you are using a processor, you must sign a processor agreement with that party which stipulates that:
• The processor shall only process the data on your instructions
• The processor must comply with your security obligations in accordance with the Dutch Data Protection Act
• Entitles you to check that the processor is complying with the security obligations.

14.4 Examples
A number of examples of the types of measures that you can take are specified below. Bear in mind that the level of security must always be related to the sensitivity of the data and the possible risks to an individual’s privacy if this data is leaked. The meaning of 'adequate security' therefore depends on your specific situation. This list is not exhaustive and is included purely as an example. Standards such as the ISO 27001 and 27002 include a full overview of measures in the framework of information security.

Physical measures:

Access security
Access control (badges, cameras) can be used to deter unauthorised persons.

Secure spaces for IT systems
You should ensure that there is extra security in the areas where the data is actually stored and that only the persons charged with the management and maintenance of the IT systems may enter those areas.
Organisational measures:

Security policy
The starting point for effective security is a security policy or security plan. In the security plan, responsibility for security is specified, measures are described and activities such as monitoring and enforcement are defined.

Incident response
No security system is 100% secure. Security incidents can therefore never be ruled out and personal data can sometimes be inadvertently leaked. You must record the way you deal with these types of situations in an incident response plan. In this plan, you can also specify when and how a security infringement must be reported to the supervisory authority.

Security awareness
Good security depends on the level of awareness among the employees. Make sure that everybody is aware of the risks and dangers and of the measures that are in place to prevent those risks and dangers. This includes training courses, workshops, etc.

Technical measures:

Security of IT facilities
Make sure that all of your IT facilities are secure. This includes passwords for all devices, a patch policy to ensure that all systems are always up to date and the encryption of important files and databases. Another important aspect of security is access control: who is allowed access to which data? Make sure, therefore, that you have a clear authorisation policy.

Network security
Make sure that your network is protected against attackers. This includes anti-virus software and firewalls. For more sensitive data, you should install intrusion detection systems (IDS) and permanently monitor the data.

Logging and monitoring
Keep a record of the use of and the access to systems so that you can identify irregularities afterwards (or in real-time).
15 Storing and destroying data

You may not store personal data for longer than is necessary to realise the purpose. When you define the purpose of processing personal data, you must also define the retention period. When this period has elapsed, you must destroy the personal data or make it anonymous. You must also specify the retention period in the privacy statement.
15.1 Requirement

- Data is assigned a retention period
- Data is destroyed or made anonymous when it is no longer necessary for the processing purposes.

15.2 Statutory provisions

This requirement is based on the following statutory provisions:
- Article 10 of the Dutch Data Protection Act.

15.3 Explanation

The personal data may not be stored for longer than necessary to achieve the processing purpose. When defining the purpose, the retention period should also be specified. If it is no longer necessary to store the data, the data must be deleted or all identifying characteristics must be deleted (made anonymous). You should also specify the retention periods in your privacy statement.
15.4 Examples

Example 1
When a user cancels the service provided by SnellerThuis BV, the retention period begins. Account data that is not relevant enough to be stored, such as the user’s profile photograph, is destroyed immediately. SnellerThuis BV stores invoice data for seven years to be in compliance with the Tax and Customs Administration’s statutory retention obligations.

Example 2
The privacy policy for the Spitsmijden Galecopperbrug peak-traffic avoidance project stipulates that data is deleted after ten working weeks.

Storing your personal data
Retrieved personal data about motorists who often use the project route but do not respond to the invitation or one-off reminder to take part in ‘Spitsmijden Galecopperbrug’ are deleted from the Spitsmijden Galecopperbrug database within ten working weeks after registration, notwithstanding unforeseen circumstances.

Statistical data that Rijkswaterstaat uses for traffic research (for example, for measures to reduce traffic congestion) may be stored for a longer period. This data is anonymous and cannot be traced back to any natural person.
You may not export personal data to countries that do not have an adequate level of privacy protection. This means that personal data may only be processed inside the European Economic Area (member states of the EU, Iceland, Norway and Liechtenstein), and in countries deemed by the European Commission to offer an adequate level of protection. For data export to other countries, the user’s consent or a permit from the Dutch Data Protection Authority is required, or you can use ‘standard contractual clauses’.
16.1 Requirement

Data may not be exported to a country that does not offer an adequate level of privacy protection.

16.2 Statutory provisions

This requirement is based on the following statutory provisions:

• Article 76 of the Dutch Data Protection Act.

16.3 Explanation

The basic principle is that personal data may only be processed in countries that offer an adequate level of privacy protection. Countries with an adequate level of protection are:

1. The countries in the European Economic Area
2. Countries deemed by the European Commission to provide an adequate level of protection.

Ad 1)
The European Economic Area consists of the member states of the European Union plus Iceland, Norway and Liechtenstein.
Ad 2)
The countries that offer an adequate level of protection at the time of the publication of this reference architecture are: Andorra, Argentina, Canada, Switzerland, the Faroe Islands, Guernsey, Israel, the Isle of Man, Jersey, Uruguay and New Zealand.

The United States does not currently have an adequate level of privacy protection because on 6 October 2015 the European Court of Justice ruled that the Safe Harbor framework is invalid. Organisations that had committed themselves to this framework were deemed to provide an adequate level of privacy protection. The US and the EU are currently working on a new framework that will replace the Safe Harbor framework: the EU-US Privacy Shield.

If a country does not offer an adequate level of protection and you still want data to be processed in that country, you must use one of the exceptions stipulated in Article 77 of the Dutch Data Protection Act. The main exceptions are the consent of the data subject, or the possession of an export permit.

You can apply to the Dutch DPA for an export permit. You do not need to apply for a permit if you are using 'standard contractual clauses'. These clauses in the contract with another controller or a processor are aimed at safeguarding the privacy of the data subject. If these contractual clauses have been included, the data may also be forwarded.7

16.4 Example

Example 1
SnellerThuis BV wants to host its application and related customer database in India. Because India is not a country with an appropriate level of protection, one of the exceptions must be used.

7 For more information, see: https://www.cbpweb.nl/nl/onderwerpen/internationaal-dataverkeer/doorgifte-binnen-en-buiten-de-eu
When a data breach occurs, personal data is lost or there is a risk that the data will be unlawfully processed. The Dutch Data Protection Act stipulates that you must notify a data breach to the Dutch Data Protection Authority when the breach involves sensitive personal data such as financial data or login data or when the scale of data breach is considerable.

If a data breach is liable to adversely affect the privacy of the data subjects, you are obliged to notify them about the data breach immediately. This chapter explains when and to whom you must notify a data breach.
17.1 Requirement

The controller must notify the Dutch DPA about a security breach which can result in (a significant chance of) a serious negative impact on the protection of personal data.

The controller must also notify the data subject about the abovementioned security breach if it can have a negative impact on his or her privacy.

17.2 Legal stipulations

This requirement is based on the following legal basis:

• Article 34a Dutch Data Protection Act

17.3 Explanation

Notification to the Dutch Data Protection Authority
If you have a serious data breach, you should notify to the Dutch DPA as soon as possible, preferably within 72 hours. A data breach is a security incident where personal data is lost or where unlawful processing cannot be reasonably excluded. Examples of a data breach include the loss of a USB stick, a hack by a hacker, a malware infection or a fire at a data centre.

You only need to notify a data breach if the breach results in (a significant chance of) a serious negative impact on the protection of personal data. Here, the nature and the scale of the personal data play an important role. As a rule, you must always notify the loss of sensitive personal data. This includes special categories of personal data (such as data about a person’s religion or personal beliefs, race, political persuasion, health, sexual orientation, membership of a trade union or criminal record), data about the financial or economic situation of the data subject, data that can lead to the stigmatisation or social exclusion of the data subject, user names, passwords and other login data and data that can be misused for the purpose of (identity) fraud.
When assessing whether you must notify a data breach, the amount of personal data per person and/or the number or people whose personal data has been breached also play a role.

To notify the data breach to the Dutch DPA you must fill in the web form on the Dutch DPA’s website. If you cannot use the web form, you can send the message to the Dutch DPA by fax.

**Notification to the data subject**

When you are obliged to notify a data breach to the Dutch DPA, you must assess whether you should also notify the data breach to the data subject. You are obliged to notify the data breach to the data subject immediately if the data breach could have a negative impact on his or her privacy. This means that the data breach could damage the data subject’s interests. Examples include unlawful publication, defamation of character and reputation, (identity) fraud or discrimination. If there is a data breach that involves sensitive data, you can assume that you should notify it to the data subject.

When you notify the data subject about the data breach, the data subject can take measures to protect himself/herself against the consequences of the data breach. You must therefore notify the data subject as soon as possible so that he/she can act without delay to protect himself/herself.

You can decide not to notify the data subject if you had already taken appropriate security measures to ensure that the personal data was incomprehensible or inaccessible for unauthorised persons. Examples include encryption and hashing. In each case, you must assess whether the security measures that were taken provide a sufficient level of protection as a result of which it is not necessary to notify the data subject.

When you notify a data breach to the data subject, you must in any case specify the following: the nature of the data breach, the organisations that can provide the data subject with more information about the data breach, and the measures that you advise the data subject to take in order to limit the negative impact of the data breach.
Policy rules for assessing whether incidents must be reported

The Dutch DPA has drawn up policy rules for assessing whether a security incident must be reported to the Dutch DPA and, where relevant, to the data subject. These policy rules are also included on the Dutch DPA website.  

17.4 Examples

Example 1
Hackers break into the SnellerThuis BV database and make a copy of the data. The database contains the unencrypted login data of all users of the SnellerThuis BV app.

SnellerThuis BV uses the web form to notify this data breach to the Dutch DPA within 72 hours. SnellerThuis BV also notifies all of its users about the data breach and also tells them to change their passwords.

Example 2
A malware notification is sent to the computer of a SnellerThuis BV employee. It turns out that SnellerThuis BV’s systems are infected with a virus that is enabling unauthorised persons to access the encrypted login data of the users of SnellerThuis BV’s app, but which does not give them access to the key to decrypt the login data. SnellerThuis BV uses the web form to notify this data breach to the Dutch DPA within 72 hours. SnellerThuis BV is not obliged to notify all of its users about this data breach because the login data was adequately encrypted. This means that the data breach will have no negative impact on the protection of the users’ privacy.

For more information, see: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/beleidsregels_meldplicht_datalekken.pdf
Appendix: Articles of law by chapter

For the sake of readability we only included references to the law provisions in the previous chapters. In this appendix, the law provisions are integrally included as reference material for each chapter.

1. Responsibility

This requirement is based on the following statutory provisions:

**Article 1d Dutch Data Protection Act**
Controller: the natural or legal person, public authority, or any other body which alone or jointly with others determines the purposes and means of the processing of personal data.

**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 the controller in the Netherlands.

2. This Act applies to the processing of personal data by or on behalf of a controller that is not established in the European Union, and who makes use of equipment, automated or otherwise, situated in the Netherlands, unless such equipment is used only for the purposes of transit of personal data.

3. In the circumstances referred to in paragraph 2, the controller must A controller as specified in the second section is prohibited from processing personal data unless it designates a representative established in the Netherlands that acts on its behalf in accordance with the
provisions in this Act. For the application of this Act and the provisions pursuant to it, that party shall be regarded as the controller.

**Article 14 Dutch Data Protection Act**

1. If the controller has personal data processed by a processor on its behalf, it shall ensure that that processor provides sufficient guarantees of the technical and organisational security measures with respect to the processing operations to be carried out and with respect to notification of a security breach, as stipulated in Article 13, which can result in a significant chance of a serious negative impact or results in a serious negative impact on the protection of the personal data that it is processing. The controller shall supervise compliance with those measures.

2. The implementation of processing operations by a processor shall be regulated in an agreement or in pursuance of another legal act, giving rise to an undertaking between the processor and the controller.

3. The controller shall ensure that the processor:
   a. processes the personal data in accordance with Article 12, first section;
   b. complies with the obligations resting with the controller in pursuance of Article 13, and
   c. complies with the obligations resting with the controller with respect to the obligation to report a security breach as stipulated in Article 13 that leads to the significant chance of a serious negative impact or has a serious negative impact on the protection of the personal data it is processing.

4. If the processor is domiciled in another country in the European Union, the controller shall ensure that the processor acts in accordance with the law in that other country, notwithstanding the third section, under b and c.

5. With a view to saving the evidence, the components of the agreement or the legal act that relate to the protection of personal data, the security measures, as stipulated in Article 13, and the obligation to report a security breach that leads to a significant chance of a serious negative impact or has a serious negative impact on the protection of the personal data it is processing, shall be recorded in writing or in another similar format.
2. Legitimate purpose and legal basis

This requirement is based on the following statutory provisions:

Article 7 of the Dutch Data Protection Act
Personal data is collected for specified, explicit and legitimate purposes.

Article 8, sections a and f of the Dutch Data Protection Act
Personal data may only be processed if:

a. the data subject has given unambiguous consent for the data to be processed
f. it is necessary to process the data to serve the legitimate interest of the controller or a third party to which the data is being supplied, unless the interest or the fundamental rights and freedoms of the data subject, particularly the right to the protection of privacy, prevail.

Article 11.7a of the Dutch Telecommunication Act
1. Without prejudice to the Dutch Data Protection Act, an electronic communication network may only be used to store or access information in a user’s terminal equipment on condition that the relevant user:
   a. is provided with clear and full information in accordance with the Dutch Data Protection Act, in any case about the purposes for which this information will be used, and
   b. has given his/her consent for this to be done.

2. The requirements specified in the first section under a and b also apply if, in a way other than by means of an electronic communication network, information is stored or access is granted to information stored on the terminal equipment by means of an electronic communication network.

3. The stipulations in the first section do not apply if it involves storage or access:
   a. with the sole objective of communicating over an electronic communication network
b. that is strictly necessary to provide the information provider’s service as requested by the subscriber or user or – provided that this has little or no consequences for the privacy of the relevant subscriber or user – to obtain information about the quality or effectiveness of a service provided by the information provider.

4. A procedure as specified in the first section, which is aimed at the collection, combination or analysis of data related to the use of the information provider’s services by the user or the subscriber so that the relevant user or subscriber can be treated differently, is assumed to involve the processing of personal data as stipulated in Article 1, section b, of the Dutch Data Protection Act.

5. Access by the user to a service of the information provider that is provided by or on behalf of a legal entity appointed in accordance with public law is not made dependent on the giving of consent as stipulated in the first section.

6. In or in pursuance of a general order in council, further rules can be specified in consultation with the Dutch Ministry of Security and Justice for the requirements stipulated in the first section, under a and b, and the exceptions stipulated in the third section. The Dutch Data Protection Authority is being asked for its opinion about a draft of that general order in council.

3. Data minimisation

This requirement is based on the following statutory provisions:

*Article 11, section 1 of the Dutch Data Protection Act*

Personal data is only processed insofar as it is adequate, relevant and not excessive, having regard for the purposes for which it is collected or is then processed.
4. Purpose limitation

This requirement is based on the following statutory provisions:

*Article 7 of the Dutch Data Protection Act*
Personal data is collected for specified, explicit and legitimate purposes.

*Article 9, sections 1 and 2 of the Dutch Data Protection Act*
1. Personal data may not be further processed in a way that is incompatible with the purposes for which it was obtained.

2. When assessing whether processing is incompatible as stipulated in the first section, the controller must in any case take the following into account:
   a. the similarity between the purpose of the intended processing and the purpose for which the data was obtained
   b. the nature of the data concerned
   c. the consequences of the intended processing for the data subject
   d. the way in which the data was obtained, and
   e. the degree to which appropriate safeguards are being taken to protect the data subject.

*Article 11, section 1 of the Dutch Data Protection Act*
Personal data is only processed insofar as it is adequate, relevant and not excessive, having regard for the purposes for which it is collected or is then processed.

5. Information and transparency

This requirement is based on the following statutory provisions:

*Article 33 of the Dutch Data Protection Act*
1. If personal data is obtained from the data subject, before the point at which the data is obtained the controller must provide the data subject with the information stipulated in the second and third sections, unless the data subject already has that information.
2. The controller must inform the data subject about its identity and the intended purpose of processing the data.

3. The controller must supply detailed information insofar as – given the nature of the data, the circumstances under which it is obtained or the way it is used – it is necessary to guarantee the data subject that the data will be processed properly and carefully.

**Article 34 of the Dutch Data Protection Act**

1. If personal data is obtained in a way other than stipulated in Article 33, the controller must provide the data subject with the information stipulated in the second and third sections unless the data subject is already aware of it:
   a. when the data related to the data subject is being recorded, or
   b. when the data is to be provided to a third party, at the latest at the point of the first provision.

2. The controller must inform the data subject about its identity and the intended purpose of processing the data.

3. The controller must supply detailed information insofar as – given the nature of the data, the circumstances under which it is obtained or the way it is used – it is necessary to guarantee the data subject that the data will be processed properly and carefully.

4. The first section does not apply if it is found to be impossible to provide the information to the data subject or if it requires a disproportionate effort. In that case, the controller must confirm the origin of the data.

5. The first section also does not apply if the recording or the provision of the data is prescribed by or in pursuance of the law. In that case, when requested by the data subject, the controller should inform him/her about the statutory regulation that has led to the recording or provision of the relevant data.
Article 11.7a of the Dutch Telecommunication Act

1. Without prejudice to the Dutch Data Protection Act, it is only permitted to use an electronic communication network to store or access information in a user’s terminal equipment on condition that the relevant user:
   a. is provided with clear and full information in accordance with the Dutch Data Protection Act, in any case about the purposes for which this information will be used, and
   b. has given his/her consent for this to be done.

2. The requirements stipulated in the first section under a and b also apply if it is ensured other than by means of an electronic communication network that information is stored or access is granted to information on the terminal equipment by means of an electronic communication network.

3. The stipulations in the first section do not apply if it involves storage or access:
   a. with the sole objective of communicating over an electronic communication network
   b. that is strictly necessary to provide the information provider’s service as requested by the subscriber or user or – provided that this has little or no consequences for the privacy of the relevant subscriber or user – to obtain information about the quality or effectiveness of a service provided by the information provider.

4. A procedure as specified in the first section, which is aimed at collecting, combining or analysing data about the use of the information provider’s services by the user or the subscriber so that the relevant user or subscriber can be treated differently, is assumed to involve the processing of personal data as stipulated in Article 1, section b, of the Dutch Data Protection Act.

5. Access by the user to a service of the information provider that is provided by or on behalf of a legal entity appointed in accordance with public law does not depend on the giving of consent as stipulated in the first section.

6. In or in pursuance of a general order in council, further rules can be specified in consultation with the Dutch Ministry of Security and Justice for the requirements specified in the first section under a and b and the exceptions stipulated in the third section. The Dutch Data Protection Authority is being asked for its opinion about a draft of that general order in council.
6. Sharing personal data with third parties

This requirement is based on the following statutory provisions:

**Article 8, sections a and f of the Dutch Data Protection Act**
Personal data may only be processed if:
- a. the data subject has given unambiguous consent for the data to be processed
- f. necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject particularly the right to the protection of privacy.

**Article 17, section 3 of the Dutch Data Protection Act**
1. The ban on processing personal data related to a person's religion or philosophical principles as stipulated in Article 16 does not apply if the data is processed by:
   - a. church denominations, independent components thereof or other spiritual organisations insofar as it involves the data of persons belonging to them
   - b. religious or philosophical institutions, insofar as, given the aim of the institution, it is necessary for the realisation of its principles, or
   - c. other institutions, insofar as it is necessary for the spiritual care of the data subject, unless he/she has lodged a written objection.

2. In the cases stipulated in the first section under a, the ban also does not apply to personal data related to the religion or principles of the family members of the data subject, insofar as:
   - a. the relevant institution is in regular contact with those family members by virtue of its objective and
   - b. those family members have made no written objection to this.

3. In the cases stipulated in the first and second sections, no personal data may be supplied to third parties without the consent of the data subject.
**Article 19, section 2 of the Dutch Data Protection Act**

1. The ban on the processing of personal data related to a person's political persuasion as stipulated in Article 16 does not apply if the data is being processed:
   a. by institutions on a political principle regarding their members or their employees or other persons belonging to the institution, insofar as, given the institution's objective, this is necessary for the realisation of that principle, or
   b. to comply with the requirements that can be reasonably defined in relation to political persuasion in connection with the performance of functions in administrative bodies and advisory boards.

2. In the case stipulated in the first section under a, no personal data may be supplied to third parties without the consent of the data subject.

**Article 20, section 2 of the Dutch Data Protection Act**

1. The ban on processing personal data related to a person's membership of a trade union as stipulated in Article 16 does not apply if the data is processed by the relevant trade union or the trade union federation of which that union is a member, insofar as this is necessary given the objective of the trade union or federation.

2. In the case stipulated in the first section, no personal data may be supplied to third parties without the consent of the data subject.
7. Rights of the individual

This requirement is based on the following statutory provisions:

**Article 35 of the Dutch Data Protection Act**

1. The data subject is free to contact the controller at reasonable intervals to request notification about whether personal data related to him/her is being processed. The controller must inform the data subject in writing within four weeks about whether personal data related to him/her is being processed.

2. If such data is being processed, the notification must include a full overview of that data in a comprehensible format, a description of the objective or the purposes of the processing, the categories of data to which the processing relates and the receivers or categories of receivers, as well as the available information about the origin of the data.

3. Before a controller sends a notification as stipulated in the first section about which a third party might be expected to have reservations, it must give that third party the opportunity to express his/her views if the notification contains data that relates to it, unless this is found to be impossible or it requires a disproportionate effort.

4. When requested, the controller must provide notification about the logic on which the automated processing of his/her data is based.

**Article 36 of the Dutch Data Protection Act**

1. The party that is notified in pursuance of Article 35 about personal data related to him/her can ask the controller to improve, augment, delete or block that data if it is factually incorrect or is incomplete or not pertinent to the objective or the purposes of the processing or is otherwise being processed in a manner that is contrary to a statutory regulation. The request must contain the changes to be made.

2. The controller must notify the appellant in writing within four weeks of receipt of the request about whether or to which extent it is complying with the request. A refusal must state the reasons on which that refusal is based.
3. The controller must ensure that a decision to improve, augment, delete or block the data is implemented as soon as possible.

4. If the personal data has been recorded on a data carrier in which no changes can be made, the controller must take the measures necessary to notify the user of the data about the impossibility to improve, augment, delete or block the data despite the fact that there are grounds for adapting the data in pursuance of this article.

5. The stipulations in the first to fourth sections do not apply to the public registers established by law, if that law includes a special procedure for improving, augmenting, deleting or blocking data.

**Article 40 of the Dutch Data Protection Act**

1. If data is the subject of processing based on Article 8 under e and f, the data subject may at all times lodge an objection with the controller in relation to his/her special personal circumstances.

2. Within four weeks of receiving the objection, the controller must assess whether the objection is legitimate. If the objection is legitimate, the controller must immediately stop processing the data.

3. The controller can demand a fee for handling an objection that may not exceed an amount to be determined in or in pursuance of a general order in council. The fee will be returned if the objection is found to be justified.

4. This Article does not apply to public registers established by law.
8. Information security

This requirement is based on the following statutory provisions:

**Article 13 of the Dutch Data Protection Act**
The controller must take appropriate technical and organisational measures to protect personal data against loss or unlawful processing of any kind. Taking into account the state of the technology and the costs of the implementation, these measures guarantee an appropriate level of security given the risks related to the processing and the nature of the data to be protected. The measures are partly focused on preventing the unnecessary collection and further processing of personal data.

**Article 14 Dutch Data Protection Act**
1. If the controller has personal data processed by a processor on its behalf, it shall ensure that that processor provides sufficient guarantees of the technical and organisational security measures with respect to the processing operations to be carried out and with respect to notification of a security breach, as stipulated in Article 13, which can result in a significant chance of a serious negative impact or results in a serious negative impact on the protection of the personal data that it is processing. The controller shall supervise compliance with those measures.

2. The implementation of processing operations by a processor shall be regulated in an agreement or in pursuance of another legal act, giving rise to an undertaking between the processor and the controller.

3. The controller shall ensure that the processor:
   a. processes the personal data in accordance with Article 12, first section;
   b. complies with the obligations resting with the controller in pursuance of Article 13, and
   c. complies with the obligations resting with the controller with respect to the obligation to report a security breach as stipulated in Article 13 that leads to the significant chance of a serious negative impact or has a serious negative impact on the protection of the personal data that it is processing.
4. If the processor is domiciled in another country in the European Union, the controller shall ensure that the processor acts in accordance with the law in that other country, notwithstanding the third section, under b and c.

5. With a view to saving the evidence, the components of the agreement or the legal act that relate to the protection of personal data, the security measures, as stipulated in Article 13, and the obligation to report a security breach that leads to a significant chance of a serious negative impact or has a serious negative impact on the protection of the personal data it is processing, shall be recorded in writing or in another similar format.

9. Storing and destroying data

This requirement is based on the following statutory provisions:

**Article 10 of the Dutch Data Protection Act**
1. Personal data may not be stored in a format that makes it possible to identify the data subject longer than is necessary to realise the purposes for which it is being collected or then processed.

2. Personal data may be stored for longer than stipulated in the first section insofar as it is being stored for historical, statistical or scientific purposes and the controller has taken the necessary measures to ensure that the relevant data is used only for these specific purposes.

10. Data export

This requirement is based on the following statutory provisions:

**Article 76 Dutch Data Protection Act**
1. Personal data that is subjected to processing or that is intended to be processed after it has been forwarded is only forwarded to a country outside the European Union if, without prejudice to the observance of the Act, that country guarantees an appropriate level of protection.
2. Notwithstanding the first section, personal data that is processed or that is intended to be processed after being forwarded to a country outside the European Union can be forwarded if that country is party to the Oporto Agreement on the European Economic Zone (Treaty Series 1992, 132) entered into on 2 May 1992, unless the forwarding of this data is restricted or prohibited in pursuance of a decision by the Commission of the European Community or the Council of the European Union.

3. The appropriate character of the level of protection shall be evaluated on the basis of the circumstances that affect the forwarding of data or a category of data forwarding. In particular, account shall be taken of the nature of the data, the purpose or purposes and the duration of the intended processing or processing operations, the country of origin and the country of final destination, the general and sectoral legal provisions that apply in the third country in question, and the regulations of the professional sector and the security measures observed in those countries.

11. Data breach notification

This requirement is based on the following statutory provisions:

Article 34a Dutch Data Protection Act

1. The controller shall immediately notify the Board [Ed.: the Dutch Personal Data Authority] of a breach in security as stipulated in Article 13 that leads to a significant chance of a serious negative impact or has a serious negative impact on the protection of personal data.

2. The controller as stipulated in the first section shall immediately notify the data subject of the breach as stipulated in the first section if the breach could have a negative impact on his or her privacy.

3. The notification to the Board and the data subject shall in any case describe the nature of the breach, the organisations from which more information about the breach can be obtained and the recommended measures to limit the negative impact of the breach.
4. The notification sent to the Board shall also include a description of the identified and probable impact of the breach on the processing of personal data and the measures that the controller has taken or proposed in order to rectify this impact.

5. The notification sent to the data subject shall be structured in such a way that, taking into account the nature of the breach, its identified and factual impact on the processing of personal data, the group of data subjects and the costs of execution, an adequate and careful supply of information shall be guaranteed.

6. The second section does not apply if the controller has taken appropriate technical protection measures to ensure that the personal data concerned is incomprehensible or inaccessible to anybody who is not authorised to access that data.

7. If the controller does not notify the data subject, the Board, if it believes that a breach is likely to have a negative impact on the privacy of the data subject, can order the controller to nevertheless send notification.

8. The controller shall maintain an overview of every breach that leads to a significant chance of a serious negative impact or has a serious negative impact on the protection of personal data. The overview shall in any case include facts and data related to the nature of the breach as stipulated in the third section as well as the text of the notification sent to the data subject.

9. This Article does not apply if the controller, in its capacity as a provider of a public electronic communication service, has sent notification as specified in Article 11.3a, first and second sections, of the Telecommunication Act.

10. The second and seventh sections do not apply to financial organisations as specified in the Dutch Financial Supervision Act.

11. Further regulations can be stipulated with regard to the notification by means of an Order in Council.
Colophon

IMMA Privacy reference architecture is a publication of the Ministry of Infrastructure and the Environment, Optimising Use programme, March 2016

Text and content
Considerati, Legal partners in a digital world, Amsterdam

Design and layout
Lexenzo, Voorburg

Printing
SandeDruk, Nootdorp
IMMA Privacy reference architecture

www.beterbenutten.nl/imma