PRIVACY BASELINE

ENGLISH

MEXON TECHNOLOGY

Inhoudsopgave

Translation of the Privacy Baseline by Mexon Technology.

This is the English translation of the Dutch Privacy Baseline. This translation is made by Mexon Technology.

In some articles, Member States have the possibility to determine their own specification. For all those articles the Netherlands has made its specifications in the Implementation Act (Uitvoeringswet). This is often in line with the original GDPR (for instance the maximum age of children is the same, see article 8), but can also deviate (for instance the processing of the national identification number is changed to reflect the use of the Dutch Burger Service Nummer (BSN), see article 87). The CIP Privacy Baseline is based on these Dutch specifications. Therefore, this English translation will also mention the specifications of the Netherlands.

This translation is based on version 3.1 of the Privacy Baseline, which is based on the conceptual version of the Implementation Act. The next version of the Privacy Baseline will use the actual versions. So this translation is best used as an exact translation of the Dutch Privacy Baseline.

An English translation is useful/applicable when :

1. Your organization is based in the Netherlands or conducts work for a Dutch company and needs to implement governance for Privacy and the language in which business is conducted is English.

2. Your Dutch organization is supported by external service-parties or outsourcing-partners who communicate in English and these parties/partners need to understand what goals & measures are to be met according to the Privacy Baseline (or when these goals & measures are their responsibility).
3. Your organization is a non-Netherlands organization which wants to implement governance for Privacy and wants to make use of all the hard work the CIP network has put into creating the Dutch Baseline.

The original Dutch Privacy Baseline refers to Dutch law(s) and regulations including but not restricted to the AVG (which is itself more or less translated from GDPR) which makes it important to understand that:

1. There may be specific laws in other countries which need to be referred to instead of the Dutch Laws mentioned in this English version of the Baseline.
2. There are a few local GDPR details which are slightly different from the Dutch AVG (for example the maximum age of children may differ).
3. For ease of reference this translation has not always translated the Dutch AVG Law texts into English literally, but has where possible taken the appropriate English GDPR text, to make sure no confusion occurs when comparing with the GDPR publications.

In advance

Dealing with personal data the right way can be a challenge for organizations. What, where, by whom and in which way things must be arranged in order to guarantee privacy in the right way is not always clear to (employees of) organizations. This is why the Privacy Baseline has been developed: the Privacy Baseline provides organizations with concrete tools to protect personal data the right way. In the Privacy Baseline, the requirements of the General Data Protection Regulation (GDPR) have been translated into concrete, manageable standards that make it clear what organizations must do to ensure the privacy of those involved in accordance with the law.

The first edition of the Baseline had the “Wet bescherming persoonsgegevens” (Wbp) as a starting point. That document (version 2.0) was valid until may 25th, 2018. On that day the current national law (Wbp) expired and organizations now have to adhere to the European GDPR. The “Uitvoeringswet Algemene verordening gegevensbescherming” and the “Memorie van toelichting” are part of a broader package, that as a whole, will execute and implement EU/2016/679 and legislation EU/2016/680.

This edition of the Baseline (version 3.0) is the first edition that uses the General Data Protection Regulation as a starting point. The GDPR is the first European legislation on privacy and became effective on May 26th , 2018. On the Regulation has been worked for five years and it still contains many concessions to the Member States.

For the time being, further elaboration is left to the national legislation of the member states. For the Netherlands this takes shape in the “Uitvoeringswet AVG”. This law fills in the blanks left to the Member States in the European GDPR. The ambition of CIP is to eventually let this Baseline fully correspond with both. In this document we refer to this implementation act plus the explanatory memorandum as: “Uitvoeringswet AVG”.

The format of the Privacy Baseline is that of the standards frameworks, as they have been used for years in the field of information security. It has become a 'privacy framework' and that does not make it an easily readable document. Rather, it is a reference work with which the controller can check to what extent he complies with privacy laws and regulations and is able to make judgments about the activities that, according to the Baseline, he still has to do.

Grip on privacy

[[Afbeelding:Thema Privacy - invulling van de ACT privacydoelstellingen.png|thumb|left|500px|none|alt=”Invulling van de ACT privacydoelstellingen”|link=Wikipagina]]

The Privacy Baseline is part of a set of related documents under the heading 'Grip on privacy'. In addition to this Baseline, the CIP has also published the following four documents grafted on it:

- Privacy by Design
- Privacy Governance
- Het Privacy Volwassenheidsmodel (The Privacy Maturity Model)
- The Privacy Self-Assessment

The first two documents are guidelines for applying the right measures and setting up the organization with which "Grip on privacy" can be reached in the most efficient and effective way.

They are explanatory treatises about:

- How you can ensure that the privacy aspect does not have to be applied afterwards, but is included in the development of software from the beginning (Privacy by Design).
- How you implement, guarantee, maintain and improve privacy in all relevant business processes (governance).

With this Baseline comes a special maturity model, that is based on it. By actively using privacy as a qualitative element in business operations, organizations can use privacy to raise the service to customers to a higher level (privacy as a 'unique selling point') and by doing so reach a higher level of maturity. This aspect is explained in the document 'Privacy Maturity Model', a practical guide for establishing and increasing the organization maturity in relation to the handling of personal data.

The Privacy maturity model is also a reference model, derived from conventional 5-layer maturity models. The model specifies 5 levels on the aspect of privacy based on the extent to which the thirteen criteria of the Privacy Baseline are met.

How mature does the organization deal with privacy? What level does the organization want to pursue and what is needed for this? The Privacy self-assessment tool (PriSa) provides answers to these questions. The tool indicates what remains to be done to reach the intended level of maturity (chosen at the beginning).

Grip on Privacy offers concrete tools to ensure the correct handling of personal data, to ensure and to fit the privacy policy appropriately, effectively and efficiently into the business. It is not about the standards. The point is to realize the ACT principles: Protection, Quality and Transparency (in Dutch Afscherming, Corrigeerbaarheid en Transparantie) and thus to respect the data subject in his privacy. This is discussed in detail later in the document.

Support through broad input from the CIP network.

The 'Grip on Privacy' method and its individual documents have been developed through close collaboration with and between various parties in the CIP network. The authors would like to thank all CIP-ers, interviewed experts, members of the CIP Privacy Domain, the Pb2Avg Working Group and the Privacy By Design Working Group, who contributed to the composition of the method. Their contributions and the fact that a wide range of organizations enable them to do so give the authors the confidence that the 'Grip on privacy' method has sufficient support for a broad application and further development.

About CIP

CIP is the Centre for Information Security and Privacy Protection of, by and for government organizations. It has developed into a public-private network organization, in which specialized market organizations also participate as knowledge partners.

The centre was established for the exchange of information and knowledge sharing, to improve the information security of government services. The CIP network now consists of a large number of government organizations and (private) knowledge partners. Knowledge present in these organizations in the area of information security and privacy protection is shared and made accessible in various ways within the CIP context.

The production of theme documents with as much input from the network as possible is one of them. Affiliated organizations learn from each other's solutions and working methods and can come together to reach agreement on this. By doing more together, the CIP also contributes to the optimal use of government resources. The products of the CIP are made available for free.

Leusden, July 2018

PBENG-0 Introduction

PBENG-0.01 Pragmatics as a starting point

At the end of 2014 CIP received the request from the CIP community to document "How to do that, that privacy thing". The question did not originate from naivety, but from the abundance of information and opinions about privacy.

We found our answer in a pragmatic approach: look at privacy as organizations and companies would do. After all, laws and regulations apply to all, and the discussion about whether it must and what needs to be done has already passed. With the transition from the "Wet Bescherming Persoonsgegevens" (Wbp) to the General Data Protection Regulation (GDPR) or in Dutch "de Algemene Verordening Gegevensbescherming" (AVG), not everything has been clearly stated. This Baseline version will therefore have to be adapted, but that has not prevented the CIP from making the current version available as a contribution to the efforts of organizations to regulate the handling of personal data in a responsible manner.

All other, otherwise very interesting, reflections that are possible on the concept of privacy take place in fields of philosophy, sociology and psychology, knows personal opinions and emotions and are place-, time- and culture-related. The GDPR including the GDPR Implementation Act (in Dutch "Uitvoeringswet AVG") and the accompanying Explanatory Memorandum (in Dutch "Memorie van toelichting" - Mvt) constitute the applicable privacy frameworks and regardless of what you think of them, you have to comply with them as a company or organization.

PBENG-0.02 Informational privacy as a reference point

Organizations can choose to "only" comply with the law. But the Privacy Act is not only an obstacle. By dealing responsibly and efficiently with privacy and finding the balance between legislation, the task of the organization and the privacy of the data subjects, 'privacy' can also be used as a quality characteristic. There are already commercial companies that consciously display their privacy policy in their marketing. In this respect, government organizations have to set a good example.

In this context it is certainly useful to also look at the non-legal aspects of privacy and to know how customers experience 'privacy'. We also pay attention to this in the other "Grip on privacy" documents. If you want to be transparent and clear about your policy as an organization and if you also want to comply correctly with legal requirements to prevent fines, damage to public image and claims, then you have to proactively work on the type of privacy that is called informational privacy.

Informational privacy is all about the protection of individuals in relation to information that is known about them or is applied to them. This is also called protection of personal data (or: data protection) and is anchored in the Constitution and further elaborated in the GDPR and the GDPR Implementation Act.

PBENG-0.03 The objective of this Privacy Baseline

The Privacy Baseline transforms the privacy legislation into concrete, manageable standards that clearly indicate what organizations need to regulate in their privacy policy, the implementation and the monitoring of that policy; the Privacy Baseline offers concrete tools for the correct handling of personal data.

Correct handling of personal data means that the organization meets the objectives of Protection, Quality and Transparency. These objectives help to adequately safeguard the informational privacy of data subjects and help the organization prevent red cards, binding instructions and / or fines from the Dutch Data Protection Authority (hereafter: AP). The Baseline is also the ideal tool that

enables organizations to meet the requirements for 'accountability', which means that compliance with the law must be demonstrated. Accountability implies a documentation obligation and this requirement is also addressed in the Baseline.

PBENG-0.04 Reading Guide

In Part I the principles of information privacy are discussed (the ACT goals) in relation to the law. They give the criteria in Part II connection and context. The Baseline itself (Part II: The Privacy Baseline: The Privacy Baseline) contains the standards or 'criteria' that must be met, 13 in total.

PBENG-0.05 Introduction - For whom is the Privacy Baseline written

From the GDPR the controller got the assignment to determine if and how personal data may be processed. The Privacy Baseline is a reference book that enables the controller to check to what extent the processing complies with the law. That implies that the Privacy Baseline is a document for professionals who work hands-on in organizations on privacy measures and on the safeguarding and control of those measures and for those who manage them. As the Baseline helps in the realization of documentation and accountability for the supervisory authority or the requesting citizen, the internal reporting for accountability can of course also be supported.

PBENG-0.06 Introduction - Part II: The Privacy Baseline

The Privacy Baseline is divided into three parts:

1. the Privacy policy of organizations (2.1 The Policy Domain);
2. the requirements for the execution of the GDPR (PBENG-U the Execution Domain), and:
3. the control of the Privacy Policy (2.3 the Control domain).

The whole describes which concrete requirements are imposed on organizations when dealing with personal data.

This Privacy Baseline aims to state in as much detail as possible what an organization must do to comply with the privacy legislation. We have achieved this by translating the legislation into concrete unambiguous standards. A privacy standards framework. The reader with expertise, the (privacy) professional familiar with information security, will recognize the format of the Privacy Baseline and will be able to appreciate 'standards' and translate them into practice.

Those who want to explore first or read more in-depth information, consult the two manuals: 'Privacy by design' and 'The safeguarding of privacy in organizations' (in Dutch ‘De borging van privacy in organisaties’) ('Privacy Governance').

The Baseline is a guide to handle personal data, but cannot be regarded as a substitute for the law. Accurate compliance with the Baseline does, however, bring an organization to the privacy maturity level 3; this level is usually sufficient to pass the compliancy test. Maturity levels will be addressed later.

PBENG-0.07 Introduction - Scope of this document

This Baseline focuses on the requirements that the privacy legislation sets for organizations and what organizations have to do. The authorization of the data protection authority (Autoriteit Persoonsgegevens, AP) - and the requirements imposed by law on the AP are not in scope of this document.

As far as the AP is concerned, the GDPR speaks consistently about "the competent supervisory authority". This has to be done because it is possible that the supervisor who deals with a violation is not always the supervisor for the country where the violation was found. Unless the context requires otherwise, we hereafter refer to the AP as the competent supervisory authority.

PBENG-0.08 Introduction - Sector-specific legislation and regulations

Organizations that want to or need to process personal data must in some cases (also) comply with sector-specific legislation. Think of the (Dutch) Telecommunications Act or the regulations for financial institutions. As the GDPR refers to specific member states 'laws and regulations' but does not actually deal with them, the Baseline Privacy also does not take into account any applicable sector-specific legislation and regulations.

PBENG-0.09 Introduction - When does the Baseline apply?

De Privacy Baseline applies to organizations that work with personal data. Before starting with this Baseline, consider the following:

Question 1: Do I want to/ do I have to process personal data? (Personal data contains information about an identified or identifiable natural, living person). Personal data can be directly or indirectly identifiable, (see PBENG-1.03.03).

A processing is an operation or a whole of operations relating to personal data and is a very broad concept (see PBENG-1.03.01).

If the answer is 'no', the GDPR - and therefore this Baseline - is not relevant.

Question 2: Is this processing based on one of the legitimate grounds of the privacy legislation the criterion PBENG-U.01 Purpose limitation of data processing?

If the answer to question 1 is 'yes', but the answer to question 2 is 'no', you are not allowed to process personal data.

These questions are based on the central principle of the GDPR that personal data may only be processed if the purpose of the processing cannot reasonably be achieved in another way. This means that you may only process personal data if the data is necessary to achieve the intended purpose. So always check whether the goal can also be achieved without using data that can be traced to a natural person.

PBENG-0.10 Introduction - Changes in version 3.0

In version 3.0, the Baseline is transformed to the amended privacy legislation that applies from 25 May 2018. This document is written with the knowledge of the legislation as of April 2017; in particular the “Uitvoeringswet AVG” is not yet definitive. The baseline criteria have also been ‘sanitized’ and the number has been reduced to 13. However, there is no question of a 'trend break'.

PBENG-0.11 Introduction - Changes in version 3.1

In this version mainly spelling mistakes have been removed and formulations have been altered. The latter to make it suitability for publication in the Nora wiki.

PBENG-0.12 Introduction - Reference literature

The actual text of the regulation, in which the recitals and articles are placed in unrelated order, is rather user-unfriendly. A quick search on the internet with "GDPR" (General Data Protection Regulation) delivers a series of titles that provide insight in this aspect. We mention several (Dutch). These publications are not freely available:

- http://www.bju.nl/juridisch/catalogus/tekstuitgave-privacyverordening-1
- https://www.managementboek.nl/boek/9789082083446/de-algemene-verordening-gegevensbescherming-editie-2017-arnoud-engelfriet
- http://www.nomos-shop.de/Albrecht-Jotzo-neue-Datenschutzrecht-EU/productview.aspx?product=27238

These references are from the CIP publication "20170425 Tussen Wbp en Avg, over de invoering van de Avg" (april 2017), to be found on www.cip-overheid.nl. On this site you will also find all documents of the method 'Grip op privacy'

PBENG-0.13 Introduction - Colophon

The original Dutch version Privacy Baseline is created by a taskforce within CIP ("Centrum voor Informatieveiligheid en Privacybescherming" -> Centre for Information security and Privacy protection).

This English version is the result of the translation by consultants of Mexon Technology.

1. PBENG-1 Principle of the GDPR and the baseline

For organizations that work with personal data, the GDPR and the "Uitvoeringswet AVG" offer the only 'hard' standard for implementing a concrete, effective and verifiable privacy policy, in accordance with the three objectives for Protection, Quality and Transparency (in Dutch ACT). ACT explicitly aims to protect the data subject. The GDPR formulates in article 5.1 with the same intention that personal data must be processed in a manner that is "lawful, fairly and transparent" with regard to the data subject. With some agility, this trio can easily be reconciled with the ACT trio (more on this in PBENG-1.03.04).

1.1 PBENG-1.01 Process personal data yourself or outsource

After we have determined that we have to process personal data to achieve a certain objective, we must also determine whether we do so in the role of controller or processor. A controller has to determine the purpose and means for the relevant processing (s) of personal data; a processor processes personal data on behalf of or for the benefit of a controller. These roles can coincide; an organization may also choose not to process (certain) personal data itself (including the choice not to collect and store (certain) personal data).

When outsourcing the processing or when processing personal data from another party, agreements must be made between the controller and the processor. These agreements can be recorded in a contract which we will call the 'Data Processing Agreement' in this Privacy Baseline. This is a common, but not official term from the GDPR. The agreements may also follow from another legal act under Union law or Member State law. It is important that, among other things, responsibilities are appointed, for example with is accountable and where data subject can find a contact point with regard to processing.

When exchanging data between two controllers, it is also advisable to include details in which the parties agree on the sharing of data, for example that the sharing of the data is lawful and takes place safely. There must always be a valid basis for the processing of the personal data: of course this also applies to processing for a different purpose. The receiving party is responsible for the technical and organizational measures necessary for the security of the data.

1.2 PBENG-1.02 Data Processing Agreement

Article 28 states 'Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller.'

We will use the term 'Data Processing Agreement' for that purpose. For data transfer between two processors (when personal data is transferred), we will use the term 'cooperation agreement', to distinguish the difference between agreement the controller and processor and the agreement between joint controllers.

1.3 PBENG-1.03 Working with personal data

Chapter II of the GDPR describes the principles of the processing of personal data. We limit ourselves here to explain what is meant by 'processing', 'personal data' and 'special categories' of personal data. Then we go into the ACT goals, we name risks and briefly explain the format in which the criteria are described in the next chapter.

1.3.1 PBENG-1.03.01 Processing of personal data

PBENG-1.03.01.T1 Processing of personal data concept
Processing is a broad concept. Processing includes everything you can do with personal data from collection to destruction. Viewing information is already processing data. In the definition of the GDPR: "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction".

1.3.2 PBENG-1.03.02 Controller and processor

PBENG-1.03.02.T1 Controller and processor definitions
In paragraph 1.1 we already discussed the controller and the processor. For completeness, the full definitions follow here:

- Controller: the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;
- Processor: a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

There is no harm in pointing out the accountability of the processor. GDPR article 5.2 states: "The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

1.3.3 PBENG-1.03.03 Personal data and special personal data

1.3.3.1 PBENG-1.03.03.01 Personal data

In the GDPR personal data refers to any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

- Directly identifiable:
  Data that by nature directly relates to a person, such as someone's name.
- Indirectly identifiable:
  Data that by its nature does not relate to a person is considered personal data if they partly determine the way in which the data subject in question is assessed or treated in society. Examples of this are the type of house or car of a person involved, because it is an indication of the income and assets of the person involved. Data that can lead to identifiability in combination with other data are also regarded as personal data.

Note that a definition of "Data Subject" can be derived from the definition of "Personal Data".

The data subject is the person to whom the personal data relates and can be identified with it. In addition, the following: the data subject is not the owner of his / her data; ownership of data is not possible in a legal sense.

1.3.3.2 PBENG-1.03.03.02 Special categories of personal data

The GDPR mentions 'Special categories of personal data'. This is data regarding:

- racial or ethnic origin,
- political opinions,
- religion or philosophical beliefs,
- trade-union membership,
- genetic data,
- data concerning health,
- data concerning sex life or sexual orientation,
- Biometric data.

Special categories of personal data are, by their very nature, more confidential than 'ordinary' personal data and processing takes place on other grounds than 'ordinary' personal data. Processing of these categories of data is prohibited unless a number of conditions are met. These conditions have significant differences with regard to the conditions for the processing of personal data in general. The criterion PBENG-U.01 Purpose limitation data processing specifies this in detail.

In the considerations of the GDPR we still come across the term 'sensitive data'; it is used as a qualification of special personal data and actually reflects the reason for the special, stricter requirements that apply to the processing of this data.

1.3.3.3 PBENG-1.03.03.03 Criminal convictions and offences and National identification number

Criminal convictions and offences are not regarded as 'special personal data'. In GDPR article 10 specific provisions have been included with regard to the processing of this data.

In the GDPR, a national identification number is not regarded as special personal data. In the “Uitvoeringswet AVG” additional conditions are set for the use of such a number, in the Netherlands the BSN (see further under PBENG-U.01 Purpose limitation of data processing). A number that is prescribed by law for the identification of a person is only used in processing for the implementation of the relevant law or for purposes specified by law.

1.3.4 PBENG-1.03.04 The ACT privacy principle

PBENG-1.03.04.T1 Privacy types
[[Afbeelding:Thema Privacy - de ACT-doelen van privacybescherming.png|thumb|left|500px|none|alt=”De ACT-doelen van privacybescherming”|link=Wikipagina]]

Different types of privacy can be distinguished. The right to protection of personal data is called informational privacy, as we already discussed in the introduction. Protecting informational privacy can be expressed in ACT goals: Protection, Quality and Transparency (in Dutch "Afscherming, Corrigeerbaarheid en Transparantie").

PBENG-1.03.04.T2 Act principals
GDPR article 5 mentions : lawfulness, fairness and transparency. Compared to the ACT principles these should be considered to be a "legal objective". ACT is on the other hand a "functional objective", also useful when implementing Privacy by Design. In the (functional) core, there are no different starting points or objectives, so we believe. In the end it is not about compliancy to the law, but about proper privacy protection. The ACT principles have the following definition:

- Protection means that personal data are protected against use for purposes other than the purposes for which they are collected.
- Quality: with regard to any processing of personal data, it is possible to adjust or destroy the personal data if the processing does not meet the requirements; for example, in case of incorrect information or if there is no longer any need to keep the information.
- Transparency: the following information is available with regard to each processing of personal data: the controllers, the categories of personal data, categories of data subjects, categories of recipients, purpose limitation, the legal basis, the storage periods, the security measures and the organizational and technical arrangements for processing of personal data.

PBENG-1.03.04.T3 ACT goals
These goals are based on the privacy legislation and also give effect to the current privacy principles, as described by the Organization for Economic Cooperation and Development (OECD) . The tables below describe the privacy principles for each ACT goal. For each privacy principle, it is indicated which criteria are leading in order to comply with the privacy principle. The supporting criteria are, as the term implies, support for the guiding criteria and therefore preconditions for an effective interpretation of the guiding criteria.

[[Invoegen 1.3.3. Leidende criteria pdfje met tabel]]

1.4 PBENG-1.04 Risks when not complying to the GDPR

Risks when not complying to the GDPR are divided in general risks and specific risks.

1.4.1 PBENG-1.04.01 General risks

PBENG-1.04.01.T1 Risks with baseline
Although we cannot give a full guarantee from this place that you comply with the GDPR if you comply with the Baseline, it can be reasonably stated that complying with the Baseline means that an organization complies sufficiently with the GDPR principles.

Failure to comply with the GDPR can have far-reaching (negative) consequences.

PBENG-1.04.01.T2 Example data subject risks
Examples of risks for the data subject:

- The ability to make anonymous use of certain services is frustrated.
- Personal data is shared or used illegally.
- Personal data are used for purposes that the data subjects are not aware of.
- Linking systems can lead to more personal data being used than necessary.
- Vulnerable groups of people are at greater risk of adverse consequences, such as exclusion, discrimination or stigmatization, if they have been the victim of improper use of their personal data.
- personal data are not or incorrectly managed, resulting in a proliferation of files with personal data resulting in increasing security risks.

PBENG-1.04.01.T3 Example organization risks
Examples of risks for the organization:

- Negative publicity and image damage.
- Coercive measures or fines imposed by the authorities due to non-compliance with the legislation.
- Claims for damages by data subjects.
- Higher costs when taking privacy measures afterwards.
- Poor data quality leads to poorer performance of the business.
- Data breaches lead to distrust.

PBENG-1.04.01.T4 Example legal risks
Examples of legal risks:

- Not respecting privacy regulations.
- Failure to comply with sectoral regulations.
- Not respecting human rights.

1.4.2 PBENG-1.04.02 Specific risks

PBENG-1.04.02.T1 Specific deductible risks
Furthermore, any requirement set by the privacy legislation entails a specific risk if this is not met. In the Baseline the legal requirements have been translated into concrete standards and per standard it is indicated which (non-legal) risks entail non-compliance with the standard.

1.5 PBENG-1.05 Baseline format

The requirements for the implementation of the privacy legislation are presented in the form of a standards framework. This standards framework is based on the SIVA method. The requirements are structured on the basis of a template in which the elements “who”, “what” and “why” are addressed. In principle, an answer is given to the question: "who does what and why?".

*** Tabelletje invoegen

A conformity indicator is a (sub) standard that must be met in order to meet the criterion (the main standard). Conformity indicators in the text of the main standard take the form of a keyword that identifies the sub standard. You can say that every underlined keyword is defined and elaborated in the form of measures. For each conformity indicator, one or more measures (/ 01, / 02, etc.) are formulated, on the basis of which a statement is possible on the relevant conformity indicator. In many cases, the explanatory notes to the framework provide further explanation of the measures.

2. PBENG-B Policy domain

This chapter contains guidelines for the general policy regarding privacy. With this policy, the organization provides both its own departments and other parties with clarity about the framework within which the processing of personal data takes place. This policy also describes the conditions that processes and systems must meet and how this policy is checked for compliance.

PBENG-B.T1 Objective
The objective of the policy domain is to ensure that there are sufficient prerequisites and conditions at strategic level to process the personal data responsibly and that the right support is provided to achieve the agreed objectives.

PBENG-B.T2 Risk
The absence of a policy issued by the management creates the risk that insufficient control will be given to the processing of personal data. Usually this will have a negative impact on realizing organizational objectives (and meeting the requirements of the GDPR)

2.1 PBENG-B.01 Privacy policy

The Privacy Policy provides clarity and guidance to the establishment of privacy at the organisational and strategic level.

PBENG-B.01.T1 Content
The privacy policy indicates how - by taking measures - the applicable laws and regulations are complied with. Because the laws and regulations are external factors, periodic review is needed to determine whether the policy is still in compliance. It is therefore not sufficient to draw up a single policy once and never adjust it. Internal factors, such as insufficient policy effectiveness and altered mission or vision, can also be decisive in order to achieve policy adjustments. By setting up the policy process cyclically, it is achieved that the policy is tailored to developments and implementation.

PBENG-B.01.T2 Process
The development of the organisation to an organisation that is demonstrably compliant with laws and regulations (alternatively: 'Complies' with laws and regulations), requires a cyclical process. This implies that there is a feedback mechanism whereby - by understanding the implementation - the policy can be adjusted and corrected. The Privacy Baseline is set up as a cyclic process (Policy, Execution and Control). Agreements on how this cyclic process is designed is part of the policy.

PBENG-B.01.T3 Definitions

PBENG-B.01.T3.01 Criteria

The organization has developed and established privacy policy and procedures that define the way in which personal data are processed and the legal principles are met (see GDPR article 5 paragraph 1).

PBENG-B.01.T3.02 Objective

"Privacy Policy" is intended to provide an organizational and strategic level of clarity about the provisioning choices of privacy and to ensure that data processing takes place in a lawful manner.

PBENG-B.01.T3.03 Risk

The lack of a privacy policy causes the organization to have no clarity as to exactly what is expected, thus allowing personal data to be processed unlawfully (including collecting, editing, understanding, etc.).

PBENG-B.01.T3.04 Referral

GDPR: Article 5, 24, 40

Uitvoeringswet AVG: Article 2, 4, 78, 157

2.1.1 PBENG-B.01.01 Privacy policy

2.1.1.1 PBENG-B.01.01.01 Clear responsibility

The policy provides clarity on how the controller arranges his responsibility for compliancy to the principles and legal bases and how this compliance can be demonstrated ('accountability') (see GDPR article 5 paragraph 2).

2.1.1.2 PBENG-B.01.01.02 Created through cyclic process

The privacy policy was created through a cyclical process that meets a standardized pattern containing the elements: preparing, developing, approving, communicating, executing, implementing and evaluating.

PBENG-B.01.01.02.01 Explanation (1)

The development of the policy is cyclical, so that the policy can be adjusted and corrected. Known examples of cyclic processes are Plan-Do-Check-Act (PDCA) of Observe-Orient-Do-Act (OODA).

PBENG-B.01.01.02.02 Explanation (2)

Establishing the policy through a cyclical process mainly means that the effectiveness of the policy is measured. If the measures resulting from the policy prove insufficient to contribute to the objectives of the policy, both the measures taken and the policy itself are examined for gaps. This way possible additions and corrections are identified, which are included after validation. With that the policy and / or the underlying implementation has been adjusted.

2.1.1.3 PBENG-B.01.01.03 Established by top management

The top management of the organization has laid down, ratified and communicated the privacy policy within the organization, including the vision on privacy protection and guidelines for the lawfully, properly and transparently processing - in accordance with the law - of personal data.

PBENG-B.01.01.03.01 Explanation (1)
By establishing the privacy policy by the top management, the privacy policy and the responsibilities at strategic and execution level are safeguarded.

PBENG-B.01.01.03.02 Explanation (2)
Any processing of personal data should be lawful and fair. It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed.

The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed. Natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing.

PBENG-B.01.01.03.03 Explanation (3)
The specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data. The personal data should be adequate, relevant and limited to what is necessary for the purposes for which they are processed.

2.1.1.4 PBENG-B.01.01.04 Adopting laws and regulations

The organization has established and recorded which laws and regulations apply.

PBENG-B.01.01.04.01 Explanation (1)
The organization makes an analysis of whether they can take the appropriate measures required by the applicable legislation and regulations.

2.1.1.5 PBENG-B.01.01.05 Sector-specific legislation

The policy stipulates and confirms how the requirements of the sector-specific legislation are met.

PBENG-B.01.01.05.01 Explanation (1)
In the policy, it has been established and confirmed in which way sector-specific legislation is implemented. Various sector-specific laws set further rules on data processing in specific sectors, for instance "de -Dutch- Telecommunicatiewet" and "wet Brp". In case of overlap, the special rules of the sector-specific rules overrule the general rules of the GDPR. If nothing is stipulated in sector-specific legislation, the general rules of the GDPR apply.

2.1.1.6 PBENG-B.01.01.06 Code of conduct

The policy stipulates if a code of conduct is used in which the implementation of the GDPR is further specified for the organization or branch, and with what frequency this code of conduct and compliance are checked and evaluated by the responsible and - if appointed - the Data Protection Officer (DPO) (see GDPR articles 25 and 64 paragraph 2).

PBENG-B.01.01.06.01 Explanation (1)
An organization can choose to draw up a Code of conduct (see GDPR article 40). In this Code of Conduct the requirements of the GDPR for a specific branch or organization are elaborated into concrete measures to be taken to comply with the GDPR. This Code of Conduct must meet requirements (when writing this version of the Privacy Baseline, no other requirements were known regarding codes of conduct). These requirements are drafted before the arrival of the GDPR:

a) Each provision has an explanation why it has been included;
b) If the provision is an elaboration of the law, it is indicated why the law has been translated in that specific way;
c) The applicant for the Code of conduct is an adequate representative of the sector concerned and the sector concerned is sufficiently accurate described in the Code of conduct
d) The Code of conduct is more concrete than the GDPR;
e) The Code of conduct is a correct elaboration of the GDPR, or: other legal provisions for the processing of personal data;
f) If a provision of the Code of conduct consists of a part or a paraphrasing of a statutory provision, then this deviation is motivated;
g) The AP or (if appointed) the Data Protection Officer can be asked to check the Code of conduct for correctness.

PBENG-B.01.01.06.02 Explanation (2)
If a Code of Conduct provides for dispute resolution about compliance, the AP may issue the statement only if there are safeguards for the independence of the dispute resolution.

2.1.2 PBENG-B.01.02 To implement the legal principles

2.1.2.1 PBENG-B.01.02.01 Description Privacy by Design

It has been described how it is ensured that managers have demonstrably taken measures in advance by applying Privacy by Design in accordance with PBENG-B.03, Risk management, Privacy by Design and the DPIA.

2.1.2.2 PBENG-B.01.02.02 Description purpose

It has been described how it is ensured that personal data, in accordance with PBENG-U.01, is collected for specified, explicit and legitimate purposes and that the data are not processed in a manner that is incompatible with those purposes.

2.1.2.3 PBENG-B.01.02.03 Description minimal data processing

It has been described how it is ensured that, in accordance with PBENG-U.01, the processing is adequate, relevant and limited to "minimal data processing"; to what is necessary for the purposes for which the data are processed.

2.1.2.4 PBENG-B.01.02.04 Description accuracy

It has been described how it is ensured that, in accordance with PBENG-U.03, the personal data are accurate and, where necessary, kept up to date and where every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

2.1.2.5 PBENG-B.01.02.05 Description pseudonymizing

It has been described how it is ensured that, in accordance with PBENG-U.04, appropriate technical or organisational measures, such as pseudonymisation of personal data, are taken in such a way that appropriate security of processing and personal data is guaranteed, and that they are protected against, among other things, unauthorized or unlawful processing and against accidental loss, destruction or damage.

2.1.2.6 PBENG-B.01.02.06 Description transparency

It has been described how it is ensured that, in accordance with PBENG-U.05 and PBENG-C.02, the personal data are processed in a way that is transparent to the public and the data subject and allows the data subject to exercise his rights. Specific attention is paid to the protection of children.

2.1.2.7 PBENG-B.01.02.07 Description storage period

It has been described how it is ensured that, in accordance with PBENG-U.06, the personal data are stored for no longer than the data for which the personal data are processed is necessary and in what form the personal data should be stored, so that after this period the data subjects no longer can be identified.

2.1.2.8 PBENG-B.01.02.08 Description of transfer

It has been described how it is ensured that, in accordance with PBENG-U.07, personal data are only transferred when sufficient guarantees are given, so that it can be demonstrated that the GDPR is also met with the transfer of personal data and what must be documented in a data processing agreement and a cooperation agreement.

2.1.2.9 PBENG-B.01.02.09 Description of demonstrability in proper management

It has been described how it is ensured that, in accordance with PBENG-C.01, the controller can show that during and after the processing, the processing related to the data subject is fair and how this can be done using a register (PBENG-U.02) and can be demonstrated in a dossier.

2.1.2.10 PBENG-B.01.02.10 Data leak procedure

It has been described how it is ensured that, in accordance with PBENG-C.03, the data subjects and the Authority are informed of a personal data breach if this infringement is likely to present a risk to the rights and freedoms of natural persons.

2.2 PBENG-B.02 Organizational embedding

The protection of natural persons in relation to the processing of personal data is not the task of one person. A multitude of people within an organization are involved to meet the requirements of the laws and regulations.

PBENG-B.02.T1 Definitions

PBENG-B.02.T1.01 Criteria

The division of tasks and responsibilities, the resources required and the reports have been defined and determined by the organization.

PBENG-B.02.T1.02 Objective

The objective of the division of tasks and responsibilities, the resources required, and the reports is to guarantee the proper remediation of the demands of the privacy policy and the GDPR

PBENG-B.02.T1.03 Risk

The lack of a good and transparent division of tasks and the resources and reporting lines required for this is not always clear as to those involved, which prevents meeting the requirements of the AVG, the sector-specific legislation and the privacy policy is .

PBENG-B.02.T1.04 Referral

GDPR: Article 5, 37, 38, 39

Uitvoeringswet AVG: -

2.2.1 PBENG-B.02.01 Division of Tasks and Responsibilities

2.2.1.1 PBENG-B.02.01.01 Clear accountable

The controller for data processing is the person who has established the purpose and means of data processing: it is clear at all times who this person is.

2.2.1.2 PBENG-B.02.01.02 Data Protection Officer

The controller and the processor shall designate (or have access to) a data protection officer in any case where:

- it concerns a public authority or body
  the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
- it concerns regular monitoring on a large scale
  the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
- it concerns special categories of data, personal data relating to criminal convictions and offences:
  the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10.

In other cases the controller or processor or associations and other bodies representing categories of controllers or processors may or, where required by Union or Member State law shall, designate a data protection officer.

PBENG-B.02.01.02.01 Explanation (1)
The Authority keeps a public register of Data Protection Officers (DPO).

PBENG-B.02.01.02.02 Explanation (2)
Requirements to the DPO

a) Accessibility
   A group of undertakings can appoint one DPO, provided the DPO is easy to contact from any location. Where the controller or processor is a public authority or government body, one DPO may be designated for the different public authorities and/or government bodies, taking into account their organizational structure and size.
b) For one or more organizations
   The DPO can act for associations and other bodies representing categories of controllers or processors.
c) Professional qualities
   The DPO shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the following tasks:

   - to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to the GDPR and other statutory data protection provisions;
   - to monitor compliance with the GDPR, with other statutory data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
   - to provide advice where requested as regards the DPIA and monitor its performance;
   - to cooperate with the Authority;
   - act as the contact point for the Authority on issues relating to processing, including the prior consultation for the purpose of the DPIA (see PBENG-B.03) and to consult, where appropriate, with regard to any other matter.

- The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

d) Legal protection
The DPO may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract.
e) Publication
The controller or the processor shall publish the contact details of the DPO and communicate them to the Authority.

2.2.1.3 PBENG-B.02.01.03 Tasks and agreements documented

All processing by a processor shall be governed by a contract or other legal act, that sets the tasks and responsibilities to guarantee the lawfulness of the data processing.

PBENG-B.02.01.03.01 Explanation (1)
Every appointment of a processor is laid down in a written agreement, in which the concrete agreements are anchored on how the requirements of the GDPR are met.

PBENG-B.02.01.03.02 Explanation (2)
From 1 January 2016, agreements on the obligation to report data breaches must be included in the Data Processing Agreement.

2.2.1.4 PBENG-B.02.01.04 TVB-matrix

The tasks, responsibilities and authorizations are clearly documented in a matrix in which the mutual relationships between the various managers and processors have also been made transparent.

PBENG-B.02.01.04.01 Explanation (1)
The controller and the processor shall ensure that the DPO can perform its tasks:

a) Involved properly and in a timely manner
The DPO is involved properly and in a timely manner, in all issues which relate to the protection of personal data.
b) Providing access
The DPO has the resources necessary to carry out his or her tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.
c) Does not receive any instructions
The DPO does not receive any instructions regarding the exercise of those tasks. He or she shall not be dismissed or penalized by the controller or the processor for performing his tasks. The data protection officer shall directly report to the highest management level of the controller or the processor.
d) Contact options
Data subjects may contact the DPO with regard to all issues related to processing of their personal data and to the exercise of their rights under the GDPR.
e) Confidentiality
The DPO shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with applicable legislation.
f) Other tasks
The DPO may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests.

2.2.2 PBENG-B.02.02 Resources needed

2.2.2.1 PBENG-B.02.02.01 Necessary resources

Linked to the privacy policy, the organization provides sufficient and demonstrable means for its implementation.

PBENG-B.02.02.01.01 Explanation (1)
Linked to the privacy policy, the organization provides sufficient and demonstrable means to comply with the privacy policy; among which:

- the resources for internal awareness and target group-oriented employee training on privacy-resistant working;
- the means for facilitating transparency for those involved (such as access);
- the (technical) possibility to correct personal data;
- the (technical) possibility to anonymize or delete personal data;
- the means for informing (the public);
- the means for adequate and independent supervision, for example through the allocation of a DPO.

2.2.3 PBENG-B.02.03 Report Resources

2.2.3.1 PBENG-B.02.03.01 Reporting and accountability lines

The reporting and accountability lines between the responsible parties, processors and - if appointed - the Data Protection Officer have been established and recorded.

2.3 PBENG-B.03 Risk management, Privacy by Design and the DPIA

Risk management is a continuous process that identifies and assesses the privacy risks and monitors the appropriate treatment thereof. Privacy risk management focuses on managing privacy risks during the processing of personal data (which includes collecting, storing and transferring of personal data). By privacy risk management, the organization's privacy risks are aligned with the privacy policy when developing, organizing and deploying data processing. So compliance with laws and regulations is guaranteed and the interests of data subjects are protected.

PBENG-B.03.T1 Definitions

PBENG-B.03.T1.01 Criteria

The controller is responsible for the evaluation of a data protection impact assessment, the implementation of appropriate measures and the demonstration of the appropriateness of these measures.

PBENG-B.03.T1.02 Objective

Assessing the privacy risks (the probability and their potential size / impact) is necessary to determine how, by taking measures, can be reduced to limits that the organization considers acceptable.

PBENG-B.03.T1.03 Risk

Privacy risks are not identified or not identified in time, which prevents the processing of personal data to comply with the GDPR and imposes major risks of security breaches; this can result in damage to natural persons whose personal data are being processed unlawfully.

PBENG-B.03.T1.04 Referral

GDPR: Article 24, 25, 35, 36, 42

Uitvoeringswet AVG: -

2.3.1 PBENG-B.03.01 Assessing the privacy risks

PBENG-B.03.01.T1 Assessment earliest possible
A Data Protection Impact Assessment (DPIA) should be conducted at the earliest possible stage, but prior to the processing of personal data. This way, the measures to protect personal data can be made part of the design. This ensures that the protection of personal data will comply with the obligations of the GDPR regarding appropriate technical and organizational measures and prevents unlawful data processing. Cost reduction can also be the result of an early assessment. Implementing security principle from the start is easier and cheaper than applying them afterwards. In addition, compensation can be avoided because adequate measures have been taken to prevent foreseeable risks from actually occurring.

PBENG-B.03.01.T2 Assessment range
One assessment can cover a range of comparable processing operations that involve equally high risks.

PBENG-B.03.01.T3 Assessment content
The assessment shall contain at least:

a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
c) an assessment of the risks mentioned above; and
d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

2.3.1.1 PBENG-B.03.01.01 DPIA

Where a type of processing (in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing), is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (see GDPR article 35 paragraph 1).

PBENG-B.03.01.01.01 Explanation (1)
A DPIA in relation to high risk is particularly required in the following cases and / or at the following risks (see GDPR article 35 paragraph 3):

a) a systematic and comprehensive assessment of personal aspects of natural persons, which is based on automated processing, including profiling and on which decisions are based on which the natural person has legal consequences, or which affect the natural person in a similar way;
b) large-scale processing of special categories of personal data (PBENG-U.01/ PBENG-U.04 or GDPR article 9, paragraph 1) or of personal data relating to criminal convictions and offences (PBENG-U.04/ PBENG-U.05) or GDPR article 10), or:
c) systematic and large-scale monitoring of publicly accessible areas.

PBENG-B.03.01.01.02 Explanation (2)
This should apply in particular to large-scale processing operations intended for the processing of a significant amount of personal data at regional, national or supranational level, where a large number of data subjects may be affected and, for example, due to their sensitive nature, may be at high risk. Where, in accordance with the level of technological knowledge achieved, a new technology is widely used, as well as for other processing operations that pose a high risk to the rights and / or freedoms of the data subjects, in particular when data subjects, as a result of those processing operations, makes it more difficult to exercise their rights.

PBENG-B.03.01.01.03 Explanation (3)
A DPIA should also be conducted when personal data are processed with a view to taking decisions on specific natural persons after a systematic and comprehensive assessment of personal aspects of natural persons based on the profiling of these data or after processing special categories of personal data, biometric data or data relating to criminal convictions and offenses or related security measures.

PBENG-B.03.01.01.04 Explanation (4)
A DPIA is also necessary for the large-scale monitoring of publicly accessible areas, particularly when using optical electronic equipment or for all other processing operations when the AP considers that they are likely to pose a significant risk to the rights and freedoms of data subjects, particularly as data subjects as a result of these processing cannot exercise a right or cannot invoke a service or an agreement or because these processing operations are systematically carried out on a large scale.

PBENG-B.03.01.01.05 Explanation (5)
The processing of personal data may not be regarded as a large-scale processing when it concerns the processing of personal data of patients or clients by an individual doctor, another healthcare professional or by a lawyer. In these cases, a DPIA may not be required.

2.3.1.2 PBENG-B.03.01.02 DPIA advice from DPO

The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.

2.3.1.3 PBENG-B.03.01.03 Evaluation of DPIA after changes

Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations (see GDPR article 35 paragraph 11).

2.3.1.4 PBENG-B.03.01.04 Consult AP

The controller shall consult the AP prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk (see GDPR article 36).

PBENG-B.03.01.04.01 Explanation (1)
When consulting the AP, the controller shall provide the supervisory authority with (see GDPR article 36 paragraph 3):

a) where applicable, the respective responsibilities of the controller, joint controllers and processors involved in the processing, in particular for processing within a group of undertakings;
b) the purposes and means of the intended processing;
c) the measures and safeguards provided to protect the rights and freedoms of data subjects pursuant to this Regulation;
d) where applicable, the contact details of the data protection officer;
e) the data protection impact assessment; and
f) any other information requested by the supervisory authority.

2.3.2 PBENG-B.03.02 Appropriate measures

PBENG-B.03.02.T1 Suitable for probability

The measures are appropriate for the likelihood and severity for the rights and freedoms of natural persons. Taking into account (see GDPR article 24 paragraph 1):

- the nature;
- the scope;
- the context, and:
- purposes of the processing.

PBENG-B.03.02.T2 Suitable for severity
When determining what is appropriate, account is taken of the likelihood and severity of the risks, in particular where the processing (see GDPR recital 75) can lead to:

- discrimination,
- identity theft or fraud,
- financial loss,
- damage to the reputation,
- loss of confidentiality of personal data protected by professional secrecy,
- unauthorised reversal of pseudonymisation, or
- any other significant economic or social disadvantage;

or where

- data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data;
- personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade-union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures;
- personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles;
- personal data of vulnerable natural persons, in particular of children, are processed;
- processing involves a large amount of personal data and affects a large number of data subjects.

2.3.2.1 PBENG-B.03.02.01 Measure type

Measures contain technical and organisational measures

2.3.2.2 PBENG-B.03.02.02 Measure for development

Appropriate measures have been implemented at the time of the determination of the means for the processing (Privacy by Design) and at the time of the processing itself (Privacy by Default) (see GDPR article 25).

PBENG-B.03.02.02.01 Explanation (1)
This involves looking at the processing means and the processing.

PBENG-B.03.02.02.02 Explanation (2)
See also the (future) list of the AP for which this does and does not apply. Exceptions to this (see GDPR article 35 paragraph 10) are processing pursuant to a statutory obligation or for the fulfilment of the general interest (see PBENG-U.01).

PBENG-B.03.02.02.03 Explanation (3)
Privacy by Design and by Default actually means (see "Uitvoeringswet AVG Mvt", paragraph 5.2.1) that from the outset the controller takes into account privacy considerations when drafting new policy and designing new processing of personal data.

PBENG-B.03.02.02.04 Explanation (4)
The Privacy by Design and Privacy by Default obligation applies to:

- the amount of personal data collected,
- the extent to which they are processed,
- the period for which they are stored, and:
- the accessibility thereof.

In particular, these measures ensure that personal data are in principle not made available to an unlimited number of natural persons without human intervention. Think for example of:

- pseudonymizing (see also PBENG-U.04), and:
- minimal data processing (only processing what is required).

2.3.2.3 PBENG-B.03.02.03 Measures maintained by DPIA

The measures are permanently appropriate by conducting data protection impact assessments.

2.3.2.4 PBENG-B.03.02.04 Use DPIA results for awareness

The results of the DPIA are used to make the organization (better) aware of the importance privacy protection.

2.3.3 PBENG-B.03.03 Prove

2.3.3.1 PBENG-B.03.03.01 DPIA delivers DPIA report

Of all data processing activities on which a DPIA has been carried out and a DPIA report is available, existing risks and which measures must be taken, are known.

PBENG-B.03.03.01.01 Explanation (1)
The risk management report is not only directive at implementation level, but also at organizational level.

PBENG-B.03.03.01.02 Explanation (2)
If the report contains an overview, where privacy risks are the greatest (risk = probability x impact), then this is supportive to prioritizing the processing operations whose protection and privacy must be brought to level. Incidentally, 'risk = chance x impact' is a theoretical definition; in practice it will often be 'the probability that an incident occurs or the chance of occurrence of an activity on which the risk is based in relation to the potential impact of this incident'.

2.3.3.2 PBENG-B.03.03.02 Process description DPIA

There is a process description for executing DPIA and monitoring the results.

PBENG-B.03.03.02.01 Explanation (1)
Risk management supports the entire process from signalling to eliminating the identified risks and is structured as a cyclical process.

2.3.3.3 PBENG-B.03.03.03 Demonstrable risk management

The risk management approach is demonstrably applied, for example because an action plan demonstrably follows the recommendations / improvement proposals from the DPIA.

PBENG-B.03.03.03.01 Explanation (1)
For demonstrating the appropriateness of the measures, the approved code of conduct (see GDPR article 24 paragraph 3) can be used.

PBENG-B.03.03.03.02 Explanation (2)
For demonstrating the appropriateness of the measures, the approved certification (see GDPR article 43) can be used.

2.3.3.4 PBENG-B.03.03.04 Standard DPIA model

A standard DPIA model is used; this model meets the requirements set in the GDPR.

2.3.3.5 PBENG-B.03.03.05 Privacy by Design and DPIA part of risk management

Privacy by Design and the DPIA and are part of a standard approach to risk management.

3. PBENG-C Control domain

This chapter contains guidelines for the specific management aspects of data processing; this implies, among other things, that adequate technical and organizational measures must be set up to shape the management processes.

3.1 PBENG-C.01 Internal supervision

Within the organization, the lawfulness of data processing is monitored. A data processing is lawful if it complies with the requirements set by the GDPR, sector-specific legislation and/or a (possible) Code of Conduct

PBENG-C.01.T1 Definitions

PBENG-C.01.T1.01 Criteria

Evaluation of the data processing takes place by or on behalf of the controller and demonstrates the legality.

PBENG-C.01.T1.02 Objective

The purpose of 'Internal supervision' is to guarantee the lawful, proper and transparent processing of personal data, to guarantee compliance with the GDPR and other laws and regulations relating to data protection, and to guarantee and demonstrate compliance with the policy of the controller or the processor regarding the protection of personal data.

PBENG-C.01.T1.03 Risk

If the processing of personal data does not comply with the GDPR, then the risks are twofold: the data subject is exposed to personal privacy risks and the controller is confronted with political-administrative and/or legal measures, loss of confidence and damage to its image as a result of communicative or enforcing measures of data subjects, third parties and / or the supervisory authorities.

PBENG-C.01.T1.04 Referral

GDPR: Article 5

Uitvoeringswet AVG: -

3.1.1 PBENG-C.01.01 Evaluate

3.1.1.1 PBENG-C.01.01.01 Compliancy assessments

Controller and - if appointed - the Data Protection Officer checks whether data processing meets the legal obligations. To this end, compliancy assessments are periodically performed and the results recorded.

PBENG-C.01.01.01.01 Explanation (1)
If the controller is aware of a violation of the privacy obligations and he fails to take the necessary measures to terminate this violation, he is approachable and must therefore take the necessary measures in time. The 'necessary measures' consist of corrective measures that make it possible to terminate the privacy violation within an appropriate period of time.

PBENG-C.01.01.01.02 Explanation (2)
If the DPO has encountered irregularities, he reports this to the person responsible or the organization for which he has been appointed and gives advice on the correct implementation of the privacy obligations.

3.1.1.2 PBENG-C.01.01.02 Report on measure to end GDPR violation

If it turns out that the requirements of the GDPR are not met, the controller will report on the measures to be taken to terminate the privacy violation. The evaluation reports are made available to the management.

3.1.1.3 PBENG-C.01.01.03 Planning compliancy assessment

There is a planning of activities in the context of assessing compliancy.

3.1.2 PBENG-C.01.02 Legality demonstrated

3.1.2.1 PBENG-C.01.02.01 Demonstrate purpose

It has been demonstrated that, in accordance with PBENG-U.01, the personal data is collected for specified, explicit and legitimate purposes and not processed in a way that is incompatible with those purposes (purpose limitation).

3.1.2.2 PBENG-C.01.02.02 Demonstrate data minimisation

It has been demonstrated that, in accordance with PBENG-U.01, the processing is adequate, relevant and limited to what is necessary for the purposes for which it is processed (minimum data processing).

3.1.2.3 PBENG-C.01.02.03 Demonstrate legality

It has been demonstrated that, in accordance with PBENG-U.01, the processing with regard to the data subject is lawful (legality).

3.1.2.4 PBENG-C.01.02.04 Demonstrate agreements for transfers

When demonstrating legality (PBENG-C.01.02.03) agreements for the transfers (PBENG-U.07) are used.

3.1.2.5 PBENG-C.01.02.05 Demonstrate integrity and confidentiality

It has been demonstrated that, in accordance with PBENG-U.04, appropriate technical and organizational measures are processed so that adequate security is ensured and that they are protected, inter alia, against unauthorized or unlawful processing and against unintentional loss, destruction or damage (integrity and confidentiality).

3.1.2.6 PBENG-C.01.02.06 Demonstrate correctness

It has been demonstrated that, in accordance with PBENG-U.03, the personal data are accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (accuracy)

3.1.2.7 PBENG-C.01.02.07 Demonstrate proper processing

It has been demonstrated that, in accordance with PBENG-B.03, the manner of processing with regard to data subject is fair (fairness).

3.1.2.8 PBENG-C.01.02.08 Demonstrate transparency

It has been demonstrated that, in accordance with PBENG-U.05 and PBENG-C.02, the personal data are processed in a manner that is transparent to the data subject (transparency).

3.1.2.9 PBENG-C.01.02.09 Demonstrate compliancy

The controller shall demonstrate compliancy by means of a file/dossier (whether or not kept by a Data Protection Officer) (see GDPR article 5 paragraph 2).

PBENG-C.01.02.09.01 Explanation (1)
The outcome of the compliance process can also be used for publication on the results achieved in ensuring the privacy of the customers.

3.1.2.10 PBENG-C.01.02.10 Demonstrate register

The register in accordance with PBENG-U.02 is used to prove a compliant and complete file.

3.2 PBENG-C.02 Access to data processing for data subjects

Every data subject involved has (within limits of reasonableness) the right to know whether, by whom, for what and in what way his personal data is processed. The controller must be able to offer this transparency. This transparency is necessary to enable the data subject or his/her legal representative - if necessary - without any disproportionate costs and/or effort to have data corrected or to address the controller (in court) in the event of the unlawfulness of a data processing in order to ensure that this unlawfulness is terminated.

Prior to the processing of the personal data, data subjects are informed about the processing in accordance with PBENG-U.05, and provisions have been made within the operations with which the data subject can keep control over his data, in accordance with PBENG-U.03.

PBENG-C.02.T1 Definitions

PBENG-C.02.T1.01 Criteria

The data controller provides the data subject with information about the processing of personal data and does so in a timely manner and in an appropriate form so that the data subject can exercise his rights (see GDPR article 12), unless there is a specific exception.

PBENG-C.02.T1.02 Objective

The purpose of 'Access to data processing for the data subject' is to provide transparency on data processing where necessary, so that the data subject can exercise his rights and thus be able to hold the controller accountable for the unlawfulness of data processing, so that this unlawfulness is terminated.

PBENG-C.02.T1.03 Risk

The organization is not transparent, as a result of which there is no insight into the legitimacy of organizations, as a result of which trust in an organization is lost.

PBENG-C.02.T1.04 Referral

GDPR: Article 11, 12, 15, 86

Uitvoeringswet AVG: -

3.2.1 PBENG-C.02.01 Information about the processing of personal data

3.2.1.1 PBENG-C.02.01.01 Data processing exclusion

The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed,

PBENG-C.02.01.01.01 Explanation (1)
There may be a need for information about the logic underlying the automated processing of the personal data if, for example, special computer software allows a manner of processing that for the data subject is not entirely clear at first glance. This announcement does not have to go so far that the Copyright and / or Intellectual Property Law that protects the software or the trade secret is violated.

3.2.1.2 PBENG-C.02.01.02 Access to personal data

Access to the personal data shall contain the following information: (see GDPR article 15):

a) the purposes of the processing;
b) the categories of personal data concerned;
c) the recipients or categories of recipients to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
f) the right to lodge a complaint with a supervisory authority;
g) when the personal data are not collected from the data subject, any available information as to their source;
h) the existence of automated decision-making, including profiling, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
i) where personal data are transferred to a third country or to an international organisation and on data subject request information about the appropriate safeguards pursuant.
j) a copy of the personal data undergoing processing on request of data subject

3.2.1.3 PBENG-C.02.01.03 Access conditions

The right to have access shall not adversely affect the rights and freedoms of others (see GDPR article 15 paragraph 4).

PBENG-C.02.01.03.01 Explanation (1)
The public shall have access to personal data in official documents which are in the possession of a public authority, a public body or a private body for the performance of a general interest task, such data may be published by the authority or body concerned in accordance with the legal right applicable to the public authority or body in order to bring the right of public access to official documents into line with the right to protection of personal data under the GDPR.

3.2.2 PBENG-C.02.02 Timely

3.2.2.1 PBENG-C.02.02.01 Access without delay

Information shall be provided without undue delay and in any event within one month of receipt of the request (see GDPR article 12 paragraph 3 and 4) unless:

- the complexity and number of the requests makes extension necessary, and;
- information is provided within two further months, and;
- the data subject is informed of any such extension within one month of receipt of the request.

PBENG-C.02.02.01.01 Explanation (1)
If the data subject submits his request electronically, the information will be provided electronically, if possible, unless the data subject requests otherwise.

3.2.2.2 PBENG-C.02.02.02 Information about denial

If the controller does not take action on the request of the data subject,

- the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and;
- data subject is informed on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.

3.2.3 PBENG-C.02.03 Appropriate form

3.2.3.1 PBENG-C.02.03.01 Use of clear and plain language

Any communication shall, in particular for any information addressed specifically to a child, shall be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language (see GDPR article 12 paragraph 1). A combination with standardised icons can be made in order to give a meaningful overview (see GDPR article 12 paragraph 7).

3.2.3.2 PBENG-C.02.03.02 Information in writing

The information shall be provided in writing, or by other means, including, where appropriate, by electronic means.

PBENG-C.02.03.02.01 Explanation (1)
If the data subject requests additional copies, the controller can charge a reasonable fee on the basis of the administrative costs. If the data subject submits his request electronically and does not request another arrangement, the information is provided in a customary electronic form.

3.2.3.3 PBENG-C.02.03.03 Oral information provisioning

When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

3.2.3.4 PBENG-C.02.03.04 Cost of data access

Information provisioning and any communication shall be provided free of charge, unless requests from a data subject are manifestly unfounded or excessive, in particular because of their (demonstrable) repetitive character, the controller may either:

a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested, or;
b) refuse to act on the request.

3.2.3.5 PBENG-C.02.03.05 Identification data subject

A controller processes personal data for the identification of a data subject for the exercise of the rights of data subject. This data will no longer be maintained, acquired or processed when the purpose of data processing no longer exists (conform PBENG-U.01) (see GDPR article 11). If the controller can demonstrate that it is not in a position to identify the data subject, the controller shall inform the data subject accordingly, if possible.

3.2.4 PBENG-C.02.04 Specific exception

3.2.4.1 PBENG-C.02.04.01 Access exception

Controller does not provide information when data processing purpose is based on legislation where specific exceptions apply (see GDPR article 23).

PBENG-C.02.04.01.01 Explanation (1)
The following specific restrictions apply (see GPDR article 23):

a) national security;
b) defence;
c) public security;
d) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;
e) other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation a matters, public health and social security;
f) the protection of judicial independence and judicial proceedings;
g) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;
h) a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a), (b), (c), (d), (e) and (g);
i) the protection of the data subject or the rights and freedoms of others;
j) the enforcement of civil law claims.

PBENG-C.02.04.01.02 Explanation (2)
The specific grounds for exception are referred to in the GDPR as "restrictions" (of a number of articles in the GDPR).

3.3 PBENG-C.03 Notification of a personal data breach

Providing insight into a data breach and its possible consequences may limit (negative) consequences for those involved. 'Personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. The obligation to report data breaches is dealt with in articles 33 and 34 of the GDPR (see also GDPR recital 85).

PBENG-C.03.T1 Definitions

PBENG-C.03.T1.01 Criteria

The controller reports a data breach to the AP within the specified period, documents the infringement, and informs the data subject, unless an exception applies.

PBENG-C.03.T1.02 Objective

The purpose of the "Obligation to report Data breaches " is to limit and, where possible, prevent negative consequences of a data breach.

PBENG-C.03.T1.03 Risk

Negative consequences affecting the personal privacy of data subject.

PBENG-C.03.T1.04 Referral

GDPR: Article 33, 34

Uitvoeringswet AVG: -

3.3.1 PBENG-C.03.01 Communication of a personal data breach

The GDPR concerns two different reporting obligations: there is a duty to report to the AP and a duty to report to the data subject, on whose personal data a data breach has occurred.

3.3.1.1 PBENG-C.03.01.01 Data breach notification to AP

A notification of a personal data breach shall be sent to the AP in accordance to article 55, unless exceptions apply (see PBENG-C.03.04.01).

3.3.1.2 PBENG-C.03.01.02 Data breach AP notification content

The notification to the AP shall at least (see GDPR article 33a paragraph 3):

a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned;
b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
c) describe the likely consequences of the personal data breach;
d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

3.3.1.3 PBENG-C.03.01.03 Data breach notification to data subject

A notification of a personal data breach shall be sent to the data subject unless exceptions apply (see PBENG-C.03.04.02).

3.3.1.4 PBENG-C.03.01.04 Data breach data subject notification content

In the notification to the data subject the nature of the personal data breach is described, with shall at least (see GDPR article 33 paragraph 3 under b, c and 3):

a) the name and contact details of the data protection officer or other contact point where more information can be obtained;
b) the likely consequences of the personal data breach;
c) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

3.3.1.5 PBENG-C.03.01.05 Language in data breach notification

The communication to the data subject shall describe in clear and plain language the nature of the personal data breach.

3.3.2 PBENG-C.03.02 Deadline

Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

3.3.2.1 PBENG-C.03.02.01 Notify controller without undue delay

The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

3.3.2.2 PBENG-C.03.02.02 Notify AP without undue delay

The controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the competent supervisory authority personal data breach.

3.3.2.3 PBENG-C.03.02.03 Notify AP with delay explanation

Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

3.3.2.4 PBENG-C.03.02.04 Notify data subject without undue delay

The data subject shall be notified without undue delay.

3.3.3 PBENG-C.03.03 Document any personal data breaches

3.3.3.1 PBENG-C.03.03.01 Data breach registration

The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken.

PBENG-C.03.03.01.01 Explanation (1)
The documentation contains the necessary data for all data breaches, including those that have not been reported.

3.3.3.2 PBENG-C.03.03.02 Content register (I)

That documentation shall enable the supervisory authority to verify compliance with this Article.

PBENG-C.03.03.02.01 Explanation (1)
If requested, more documentation must be available that is directly related to the reporting of an infringement itself. It must be possible to check whether all appropriate technical and organizational measures have been taken to establish whether a personal data breach has taken place and to inform the AP and the data subject without delay (see GDPR recital 87).

PBENG-C.03.03.02.02 Explanation (2)
Even when deciding not to report an infringement, this assessment and the decision must be documented so it can be checked by the AP.

3.3.3.3 PBENG-C.03.03.03 Content register (II)

The documents shall contain the facts relating to the personal data breach, its effects and the remedial action taken.

PBENG-C.03.03.03.01 Explanation (1)
The documentation is up-to-date and accurate and can be submitted immediately upon request. The documentation itself contains no personal data.

PBENG-C.03.03.03.02 Explanation (2)
When documenting, the registration of processing activities in accordance with PBENG-U.02 is used. The advice is to keep the documentation of data breaches within this registration. This prevents double storage and double management of information about the data processing.

3.3.3.4 PBENG-C.03.03.04 Content register (III)

The fact that the notification was made without undue delay should be established taking into account in particular the nature and gravity of the personal data breach and its consequences and adverse effects for the data subject (see GDPR recital 87).

3.3.4 PBENG-C.03.04 Exception

3.3.4.1 PBENG-C.03.04.01 Communication AP exceptions

Controller is not obligated to notify the supervisory authority of the personal data breach if

- the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons, or
- When notification would affect a vital interest, or
- controller is responsible for the provision of publicly available electronic communication services in public communication networks (see GDPR article 95)
- organization is a financial institution as mentioned in "de Wet op het financieel toezicht" (see GDPR article 34).

3.3.4.2 PBENG-C.03.04.02 Communication data subject exceptions

The communication to the data subject shall not be required if :

- the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons, or
- the controller has implemented appropriate technical and organisational protection measures, and that those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;
- the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;
- it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner,
- data processing purpose is based on legislation where restrictions apply (see GDPR article 23), or
- processing of personal data is done by a natural person in the course of a purely personal or household activity and thus with no connection to a professional or commercial activity (see GDPR recital 18)

PBENG-C.03.04.02.01 Explanation (1)
With the exception if the Telecommunications Act or the Financial Supervision Act applies, a double reporting obligation is prevented.

PBENG-C.03.04.02.02 Explanation (2)
The following specific restrictions apply (see GPDR article 23):

a) national security;
b) defence;
c) public security;
d) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;
e) other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation a matters, public health and social security;
f) the protection of judicial independence and judicial proceedings;
g) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;
h) a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a), (b), (c), (d), (e) and (g);
i) the protection of the data subject or the rights and freedoms of others;
j) the enforcement of civil law claims.

PBENG-C.03.04.02.03 Explanation (3)
In particular, any legislative measure shall contain specific provisions at least, where relevant, as to:

a) the purposes of the processing or categories of processing;
b) the categories of personal data;
c) the scope of the restrictions introduced;
d) the safeguards to prevent abuse or unlawful access or transfer;
e) the specification of the controller or categories of controllers;
f) the storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing;
g) the risks to the rights and freedoms of data subjects; and
h) the right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction.

PBENG-C.03.04.02.04 Explanation (4)
The GDPR does apply to controllers or processors who provide the means for the processing of personal data for such personal or household activities.

PBENG-C.03.04.02.05 Explanation (5)
Personal or household activities could include correspondence and the holding of addresses, or social networking and online activity undertaken within the context of such activities (see GDPR recital 18).

4. PBENG-U Execution domain

This chapter contains the requirements for the execution of data processing. The policy developed and endorsed at higher management level is the guiding principle for the specific aspects of data processing.

PBENG-U.T1 Objective
Personal data is processed in the execution domain. The controller must create/build data processing under the conditions and boundaries (prerequisite) defined in the policy area. Persons whose personal data are processed (data subjects) must be able to be certain that data processing is conducted according to laws and regulations.

PBENG-U.T2 Risk
If guidelines for the specific aspects of data processing are missing, there is a risk that insufficient direction is given to these specific aspects of the processing of personal data. This creates uncertainty in the technical and organizational structure of the data processing.

4.1 PBENG-U.01 Data Processing Purpose

The basic principle of purpose limitation is that data are processed and collected for a specific, explicit and legitimate purposes.

'Specific and explicit' means that no data may be collected without a precise purpose description. The purpose must be determined before the collection is started.

'Specific' means that this description must be so clear, that it offers a framework during the collection process for testing whether the data is necessary for that purpose or not. The purpose may also not be formulated in the course of the collection process.

'Explicit' means that the controller should have defined the purpose of data collection.

PBENG-U.01.T1 Definitions

PBENG-U.01.T1.01 Criteria

The controller has described all personal data collections and personal data processing in a timely, specific and explicit manner, which includes:

- ✕ the purpose, and:
- ✕ the legal basis for:

a) additional processing that is compatible with the original
b) the automated decision-making;
c) special personal data;
d) personal data relating to criminal convictions and offences;
e) national identification number;
f) Personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

PBENG-U.01.T1.02 Objective

The purpose of the 'Data Processing Purpose' is to ensure that personal data is collected and processed (further) for legitimate purposes only.

PBENG-U.01.T1.03 Risk

The unauthorized and unlawful collection and (further) processing of personal data.

PBENG-U.01.T1.04 Referral

GDPR: Article 5, 6, 9, 19, 22, 23

Uitvoeringswet AVG: Article 22, 23, 24 ,25, 26 ,27, 28, 29, 30, 31

4.1.1 PBENG-U.01.01 Specific and explicitly defined in a timely manner

4.1.1.1 PBENG-U.01.01.01 Predefined purpose

The specified and explicit purpose for personal data processing is documented prior to the start and is not determined or changed during data processing (see GDPR article 5 paragraph 1 and recital 50)

4.1.1.2 PBENG-U.01.01.02 Legitimate personal data

The legitimate purposes of all personal data and the purposes for data collection and processing are specific, explicit and legitimate (see GDPR article 5 paragraph 1b)

4.1.1.3 PBENG-U.01.01.03 Specified Purpose

The purpose is documented (explicitly) so that it provides a framework for testing whether the data is necessary for the purpose and if further processing is compatible with the original purpose (see GDPR article 6 paragraph 4).

4.1.1.4 PBENG-U.01.01.04 Smart purpose

The purpose is described explicitly, not too vague or too broad but specific, measurable, assignable, realistic and time-related.

PBENG-U.01.01.04.01 Explanation (1)
The collection and processing of personal data 'solely because it may be useful in the future', is not sufficiently precise and therefore unlawful.

PBENG-U.01.01.04.02 Explanation (2)
Data may also be collected and processed for multiple purposes; these purposes do not necessarily have to be related to each other (see GDPR article 83 paragraph 1). Each purpose must separately be determined timely, must be legitimate and described explicitly and specified.

PBENG-U.01.01.04.03 Explanation (3)
A sufficiently SMART description means (see Handleiding voor verwerkers van persoonsgegevens, handleiding van de Wbp, Ministerie van Justitie, 2002, p. 20.)

a) Specific: the purpose is unambiguous
b) Measurable: there are measurable / observable conditions through which purpose can be achieved
c) Assignable: the purpose is acceptable for the target group and / or management and someone takes his responsibility for the correct realization of this purpose
d) Realistic: the purpose is feasible
e) Time-related: it is determined when (in time) the purpose must be reached.

4.1.2 PBENG-U.01.02 Purpose

Processing should be lawful where it is necessary in the context of a contract or the intention to enter into a contract (see GDPR recital 44) and should comply to the demand of legitimate purposes.

4.1.2.1 PBENG-U.01.02.01 Data minimisation

Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation).

4.1.2.2 PBENG-U.01.02.02 Only lawful processing

Processing shall be lawful only if and to the extent that at least one of the following applies (GPDR article 6, paragraph 1):

a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
c) processing is necessary for compliance with a legal obligation to which the controller is subject;
d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.
g) The basis for the processing shall be laid down by Union law; or ember State law to which the controller is subject (see GDPR article 6 paragraph 3).

PBENG-U.01.02.02.01 Explanation (1)
For the private sector, parts a, b, d and f are usually a basis for the processing of personal data. Section c can also be a basis for the processing of personal data in the private sector, when there is a legal obligation for a private party (see GDPR recital 46).

PBENG-U.01.02.02.02 Explanation (2)
For the government, processing on the basis of a statutory obligation (part c) and processing in the interest of carrying out a general interest task (section e) is relevant. These two legal bases for the government must be established (see GDPR article 6 paragraph 3) under the statutory law applicable to the controller.

Condition for lawful processing in the context of a legal obligation is that the processing is necessary to comply with the legal obligation. The statutory obligation to provide personal data is usually very precisely documented in sector-specific regulations. However, this is not necessarily the case. It is also conceivable that processing of personal data finds a basis in a more broadly formulated duty of care. In that case, the controller has a greater responsibility for assessing the necessity of the processing in the light of compliance with the legal obligation. In this respect, the legal framework, as it applied under the Directive and the Wbp, does not change (see GDPR recital 46).

PBENG-U.01.02.02.03 Explanation (3)
With regard to the legal basis 'performance of a task of general interest or of a task in the exercise of public authority' (hereinafter also: public task) the purpose of the processing must be necessary for the fulfilment of that task. By its nature, the public task is dynamic and changeable over time. The boundaries of the public task are not always clear in advance. However, the public task itself will always have to be apparent from the sector-specific regulations that apply to the controller. It is not necessary that the sector-specific regulations also explicitly state that data may be processed for the fulfilment of the statutory task. The legal basis for the public task (see GDPR article 6 paragraph 1) also provides a purpose for the processing of personal data. The purpose of the data processing is by its nature bound to the exercise of this public task and the space for data processing finds its limits here. The public-law task itself will have to appear from the legal provisions relevant to the controller (see GDPR recital 46).

PBENG-U.01.02.02.04 Explanation (4)
Neither the public task nor the processing of data needs to be exhaustively regulated in a law in the formal sense. It is sufficient that the outlines are known from the law. This insight is also in line with the EVRM's basic limitation principle, whereby the limitation of private life (see GDPR article 8 paragraph 2) must be foreseeable by law. The concept of 'foreseeable by law' is understood here as a material concept of law, which is not limited to laws in the formal sense (see GDPR recital 41). The core concern is that it must be clear to the individual that his personal data are processed in relation to a specific public task. This can also, as is now assumed in some cases, follow from a set of legal rules that together indicate a public task. The concept of a public task must therefore be widely read, partly in the light of the considerations at the GDPR but this public task must be sufficiently clear from national law. GDPR article 6 paragraph 1e is not an independent legal basis for data processing, in view of the third paragraph of this provision.

PBENG-U.01.02.02.05 Explanation (5)
If the legitimacy of the purpose of the processing is determined and if the processing relates to the public interest according to point e): "shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller". That legal basis may contain specific provisions to adapt the application of rules of the GDPR, inter alia: the general conditions governing:

- the lawfulness of processing by the controller
- the types of data which are subject to the processing
- the data subjects concerned
- the entities to, and the purposes for which, the personal data may be disclosed;
- the purpose limitation
- the storage periods
- the processing operations and processing procedures, including measures to ensure lawful and fair processing such as those for other specific processing situations as provided for in Chapter IX of the GDPR.

The Dutch law shall meet an objective of public interest and be proportionate to the legitimate aim pursued (GDPR article 6).

PBENG-U.01.02.02.06 Explanation (6)
In view of the material similarity between the GDPR and the Wbp, it can be assumed that the existing legislation and regulations that give substance to the public task with regard to the legal bases for processing data as a rule comply with the GDPR. However, the wording in statutory provisions in sectoral regulations, where it refers to the Wbp, will have to be adapted (see "Uitvoeringswet AVG Mvt", section 4.4.2).

PBENG-U.01.02.02.07 Explanation (7)
In section f, it is in the government's interest that this section does not apply to government bodies in the exercise of their duties. Public authorities will not be able to use the 'legitimate interest' basis in carrying out their tasks but will have to be able to indicate for this use that the processing is necessary for the fulfilment of a general interest task or a task within the framework of the exercise of the public authority entrusted to the controller. This does not apply insofar as the government agency performs 'typical business transactions' in which personal data are processed, such as the processing of personal data that is necessary for the security of government buildings. For actions that fall outside the exercise of the statutory task, a basis may be adopted in the legitimate interest of the organization. The government does not essentially differ from a private party in this (see GDPR recital 47).

4.1.2.3 PBENG-U.01.02.03 Transparent processing

Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject (see GDPR article 5), (The GDPR does not apply to the personal data of deceased persons. (see GDPR recital 27)). For that reason shall :

a) personal data collection be transparent (see PBENG-U.02 and PBENG-U.05).
b) personal data be accurate and rectified if necessary (see PBENG-U.03).
c) personal data be appropriate protected (see PBENG-U.04).
d) personal data kept in a form for no longer that is necessary for the identification of data subjects (see PBENG-U.06).

4.1.3 PBENG-U.01.03 Further processing

PBENG-U.01.03.T1 Further processing purpose
'Further processing" in the GDPR refers to all processing of personal data for a purpose other than that for which the personal data were originally collected. This may be processing by one and the same controller but may also be the basis for providing data to another controller.

PBENG-U.01.03.T2 Verify purpose further processing
In order to verify whether a purpose of further processing is compatible with the purpose for which the personal data were initially collected, the controller should, after having complied with all the requirements on legality of the original processing, take into account:

- a possible link between those purposes and the purposes of the intended further processing;
- the framework in which the data were collected; in particular the reasonable expectations of the data subjects on the basis of their relationship with the controller with regard to their further use;
- the nature of the personal data;
- the consequences of the intended further processing for those involved, and:
- appropriate safeguards for both the original and intended further processing.

PBENG-U.01.03.T3 Purpose archiving
Further processing for purposes of archiving in the public interest, scientific or historical research or statistical purposes is not considered incompatible with the original purposes (purpose limitation);

PBENG-U.01.03.T4 Purpose commerce
Further processing for purely commercial objectives, such as targeted advertising, cannot be based on this. This is only possible with the explicit consent of data subject.

4.1.3.1 PBENG-U.01.03.01 Further purposes

Processing for a purpose other than that for which the personal data have been collected, is only possible if:

1. processing for another purpose is compatible with the purpose for which the personal data are initially collected, and the controller takes into account (see GDPR article 6 paragraph 4):
    a. any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;
    b. the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;
    c. the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;
    d. the possible consequences of the intended further processing for data subjects;
    e. the existence of appropriate safeguards, which may include encryption or pseudonymizing.

    Or:
2. when further processing is based on consent;
    Or when:
3. when further processing is based on legislation on which specific exceptions apply.

PBENG-U.01.03.01.01 Explanation (1)
The controller may further process data for another purpose provided that the other purpose is not incompatible with the original purpose for which the data was collected (see GDPR article 5 paragraph 1b). The controller itself must determine whether the other purpose is compatible with the original purpose.

Based on the GDPR, further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes remains possible undiminished. GDPR article 5 paragraph 1b stipulates that further processing for those purposes is not considered incompatible with the original purposes. A precondition for further processing is that the controller provides appropriate safeguards for the protection of the personal data of the data subjects. Possible provisions the controller can take in this context, can for example be the pseudonymization of the personal data in question.

PBENG-U.01.03.01.02 Explanation (2)
Option 2 for further processing is based on the consent of the data subject, even if it is not compatible with the purpose of the original processing of personal data. The acceptability of further processing based on consent is in a way a matter of course. After all, the permission expresses the fact that data subject does not consider the infringement of privacy that takes place during the processing of personal data as objectionable. The permission must be given explicitly and freely (see GDPR articles 7 and 8). The controller does not have to test the compatibility requirement in case of consent.

PBENG-U.01.03.01.03 Explanation (3)
Option 3 for further processing is based on the laws and regulations that form a necessary and proportionate measure in a democratic society to guarantee the intended objectives. In the Netherlands this has been reflected in article 39 of the "Uitvoeringswet AVG". In that case further processing does not have to be compatible with the original purpose for which the data were collected. The controller therefore does not have to test the compatibility requirement (see GDPR article 6, second part of paragraph 4). Further processing by the controller is then based on the Member State provision (i.e. a specific legal provision). As stated above, further processing for a non-compatible purpose should be applied with restraint. An important limitation is therefore that the national law basis for further processing for a non-compatible purpose in a democratic society must form a necessary and proportionate measure to guarantee the objectives listed in GDPR article 23 paragraph 1. These are objectives of general interest, which will be discussed in more detail below. It is first for the legislator to determine whether these interests are at stake and, if so, whether they are sufficiently justified in the specific case for allowing non-compatible use.

PBENG-U.01.03.01.04 Explanation (4)
If the further processing is carried out based on option 3, because the controller is legally obliged to do so or if the processing is necessary for the fulfilment of a task of general interest or for a task in the exercise of the public authority, the processing must have a basis in legal law. The GDPR does not prescribe that specific legislation is required for each individual processing. Sufficient legislation can be used as the basis for several processing operations based on a legal obligation resting on the controller or processing required for the fulfilment of a general interest task, or for a task within the framework of the exercise of public authority. It must also be Dutch (or EU state) law that determines the purpose of the processing. Furthermore, that right could give a more detailed description of the general terms and conditions of the GDPR to which the processing of personal data must comply in order to be lawful and of specifications to determine for determining the controller, the type of processed personal data, the data subjects, the entities to which the personal data may be released, the purpose limitation, the storage period and other measures to ensure lawful and proper processing. It is also necessary to establish the legal right whether the controller who is charged with a task of general interest or with a task in the exercise of public authority, a public authority or another public law person or, if justified, for reasons of general interest, including health purposes such as public health, social protection and the management of healthcare services, by private law, such as a professional association, should be (see GDPR recital 45).

PBENG-U.01.03.01.05 Explanation (5)
The processing of personal data should also be regarded to be lawful where it is necessary to protect an interest which is essential for the life of the data subject or that of another natural person. Processing of personal data based on the vital interest of another natural person should in principle take place only where the processing cannot be manifestly based on another legal basis. Some types of processing may serve both important grounds of public interest and the vital interests of the data subject as for instance when processing is necessary for humanitarian purposes, including for monitoring epidemics and their spread or in situations of humanitarian emergencies, in particular in situations of natural and man-made disasters (see GDPR recital 46).

PBENG-U.01.03.01.06 Explanation (6)
The following specific restrictions apply (see GPDR article 23):

a) national security;
b) defence;
c) public security;
d) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;
e) other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation a matters, public health and social security;
f) the protection of judicial independence and judicial proceedings;
g) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;
h) a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a), (b), (c), (d), (e) and (g);
i) the protection of the data subject or the rights and freedoms of others;
j) the enforcement of civil law claims.

4.1.3.2 PBENG-U.01.03.02 Inform data subject about further processing

Where the controller intends to process the personal data for a purpose other than that for which they were collected, the controller should provide the data subject prior to that further processing with information on that other purpose and other necessary information (see PBENG-U.05). Where the origin of the personal data cannot be provided to the data subject because various sources have been used, general information should be provided (see GDPR Recital 61).

4.1.4 PBENG-U.01.04 Special categories of personal data

4.1.4.1 PBENG-U.01.04.01 No processing of personal data revealing racial or ethnic origin

Processing of personal data revealing racial or ethnic origin, shall be prohibited, unless

- ☒ conditions of PBENG-U.01.04.09 are met, or:
- ☒ processing is done (see "Uitvoeringswet AVG" article 22):

a) with the purpose to identify data subject and only if it is unavoidable for this purpose;
b) with the purpose of conferring a privileged position to specific ethnic or cultural minority groups in order to eliminate or reduce actual disadvantages related to race or ethnical origin, but only if
    1. it is necessary for that purpose;
    2. the collected data only relates to the data subject's country of birth, parents or grandparents, or any other criteria stated by law, so objective determination of membership to in sub b stated minority group is possible; and:
    3. data subject has not objected in writing.

4.1.4.2 PBENG-U.01.04.02 No processing of personal data revealing political opinions

Processing of personal data revealing political opinions, shall be prohibited, unless

- ☒ conditions of PBENG-U.01.04.09 are met, or:
- ☒ the processing takes place to comply to the requirements that can reasonably imposed with regarding to political opinions in connection with the performance of functions in administrative bodies and advisory bodies (see "Uitvoeringswet AVG" article 30).

PBENG-U.01.04.02.01 Explanation (1)
Where in the course of electoral activities, the operation of the democratic system in a Member State requires that political parties compile personal data on people's political opinions, the processing of such data may be permitted for reasons of public interest, provided that appropriate safeguards are established (see GDPR recital 56).

4.1.4.3 PBENG-U.01.04.03 No processing of personal data revealing religious or philosophical beliefs

Processing of personal data revealing religious or philosophical beliefs, shall be prohibited, unless

- conditions of PBENG-U.01.04.09 are met, or:
- data processing is done by institutions that need that information for the mental care of data subject, and data subject has not objected to processing in writing (see "Uitvoeringswet AVG" art. 29). No personal data shall be transferred without data subjects consent.

PBENG-U.01.04.03.01 Explanation (1)
Moreover, the processing of personal data by official authorities for the purpose of achieving the aims, laid down in constitutional law or international public law, of officially recognised religious associations, is carried out on grounds of public interest (see GDPR recital 55).

4.1.4.4 PBENG-U.01.04.04 No processing of personal data revealing trade union membership

Processing of personal data revealing trade union membership shall be prohibited, unless conditions of PBENG-U.01.04.09 are met.

4.1.4.5 PBENG-U.01.04.05 No processing of genetic data

Processing of genetic data shall be prohibited, unless

- conditions of PBENG-U.01.04.09 are met (see "Uitvoeringswet AVG" article 24), or:
- a major medical interest prevails, or:
- the processing is necessary for scientific research or statistics and data subject has given his explicit consent.

PBENG-U.01.04.05.01 Explanation (1)
Genetic data should be defined as personal data relating to the inherited or acquired genetic characteristics of a natural person which result from the analysis of a biological sample from the natural person in question, in particular chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis, or from the analysis of another element enabling equivalent information to be obtained (see GDPR recital 34).

4.1.4.6 PBENG-U.01.04.06 No processing of biometric data

Processing of biometric data for the purpose of uniquely identifying a natural person shall be prohibited, unless

- conditions of PBENG-U.01.04.09 are met, or:
- the purpose of processing is to identify the data subject and only is it is necessary and proportional for representing the legitimate interests of the controller or a third party (see "Uitvoeringswet AVG" article 26)

(Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health).

PBENG-U.01.04.06.01 Explanation (1)
Biometric data means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data (GDPR article 4 paragraph 14).

PBENG-U.01.04.06.02 Explanation (2)
The processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person (GDPR recital 51).

4.1.4.7 PBENG-U.01.04.07 No processing of data concerning health

Processing of biometric data concerning health is prohibited, unless

- conditions of PBENG-U.01.04.09 are met, or:
- it is necessary for general public health, such as protection against serious transboundary health risks or insuring high standards of quality and safety of healthcare, medicines or medical devices. Then data will only be processed by those who are obliged by virtue of office, profession or statutory provision, or bound by a confidentiality agreement. If a controller processes data on a personal basis and not on the basis of his office, profession or statutory provision, he is obligated to keep data confidential (unless legislation or duty obliges him to process data to others who are authorized to process that data).

PBENG-U.01.04.07.01 Explanation (1)
Data concerning health are personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status (GDPR article 4 paragraph 15).

These data concerning health should include all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject. This includes information about the natural person collected in the course of the registration for, or the provision of, health care services as referred to in Directive 2011/24/EU of the European Parliament and of the Council to that natural person; a number, symbol or particular assigned to a natural person to uniquely identify the natural person for health purposes; information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples; and any information on, for example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test (see GDPR recital 35).

PBENG-U.01.04.07.02 Explanation (2)
Special categories of personal data which merit higher protection should be processed for health-related purposes only where necessary to achieve those purposes for the benefit of natural persons and society as a whole. This applies particularly to:

- the management of health or social care services and systems, including processing by the management and central national health authorities of such data for the purpose of quality control, management information and the general national and local supervision of:
  - the healthcare system, or
  - o social care system

  and
- Ensuring continuity of:
  - healthcare, or
  - social care and cross-border healthcare, or
  - health security, monitoring and alert purposes, or
  - for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, based on Union or Member State law which has to meet an objective of public interest, or
  - for studies conducted in the public interest in the area of public health.

Therefore, the GDPR should provide for harmonized conditions for the processing of special categories of personal data concerning health, in respect of specific needs, in particular where the processing of such data is carried out for certain health-related purposes by persons subject to a legal obligation of professional secrecy. Union or Member State law should provide for specific and suitable measures so as to protect the fundamental rights and the personal data of natural persons. Member States should be allowed to maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health. However, this should not hamper the free flow of personal data within the Union when those conditions apply to cross-border processing of such data (see GDPR recital 53).

PBENG-U.01.04.07.03 Explanation (3)
The processing of special categories of personal data may be necessary for reasons of public interest in the areas of public health without consent of the data subject. Such processing should be subject to suitable and specific measures so as to protect the rights and freedoms of natural persons. In that context, 'public health' should be interpreted as defined in Regulation (EC) No 1338/2008 of the European Parliament and of the Council, namely all elements related to health, namely health status, including morbidity and disability, the determinants having an effect on that health status, health care needs, resources allocated to health care, the provision of, and universal access to, health care as well as health care expenditure and financing, and the causes of mortality. Such processing of data concerning health for reasons of public interest should not result in personal data being processed for other purposes by third parties such as employers or insurance and banking companies.

4.1.4.8 PBENG-U.01.04.08 No processing of data concerning sex

Processing of personal data concerning a natural person's sex life or sexual orientation shall be prohibited, unless conditions of PBENG-U.01.04.09 are met.

4.1.4.9 PBENG-U.01.04.09 Condition for processing excluded data

If any of the in PBENG-U.01.04.01 - PBENG-U.01.04.08 processing occurs, one of the following conditions apply (Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health):

a) the data subject has given explicit consent to the data processing
b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law (see also PBENG-U.01.04.10);
c) processing is necessary to protect the vital interests of the data subject;
d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade-union aim;
e) processing relates to personal data which are manifestly made public by the data subject;;
f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject (see also PBENG-U.01.04.10);
h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment on the basis of Union or Member State law under conditions of paragraph 4 (see also PBENG-U.01.04.10);
i) de processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy, or:
j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

4.1.4.10 PBENG-U.01.04.10 Exception condition for processing excluded data

Conditions b, g and h of PBENG-U.01.04.09 do not apply if data processing is performed by (see "Uitvoeringswet AVG" article 23):

a) social workers, institutions or facilities for health care or social services insofar as this is necessary for the proper treatment or care of data subject, or necessary for managing the institution or professional practice concerned;
b) insurance companies as referred to in Section 1: 1 of the "Wet of financieel toezicht" and financial service providers that mediate in insurance as referred to in Section 1: 1 of this Act, insofar as this is necessary for:
    1. the assessment of the risk to be insured by the insurer and data subject has not objected, or:
    2. the implementation of the insurance agreement;
c) schools when it is necessary for the special supervision of pupils or the making of special provisions in connection with their state of health;
d) a probation institution, a special probation officer, the child protection board or the certified institution referred to in Article 1.1 of the "Jeugdwet" and the legal entity referred to in Article 256 first paragraph or Article 302 second paragraph of Book 1 of the Dutch Civil Code, insofar as is necessary for the performance of the tasks assigned to them by law;
e) Our Minister insofar as this is necessary in connection with the enforcement of custodial sentences or custodial measures;
f) administrative bodies, pension funds, employers or institutions that work for them in so far as this is necessary for:
    1. proper implementation of statutory regulations, pension schemes or collective agreements that provide for claims that are dependent on the health status of data subject, or:
    2. the reintegration or supervision of employees or benefit recipients in connection with illness or incapacity for work.

4.1.4.11 PBENG-U.01.04.11 Exceptions due to substantial interest

The prohibition to process special personal data is not applicable from the general interest (point g) if (see "Uitvoeringswet AVG" article 28):

a) this is necessary in order to comply with an international law obligation;
b) the data are processed by the Authority or an ombudsman as referred to in Section 9:17 of the General Administrative Law Act and this is necessary in view of an overriding public interest, for the performance of the tasks assigned to them by law and in the execution of these tasks and is provided in such a way that the privacy of the data subject is not disproportionately harmed, or:
c) it is necessary in the interest of an overriding public interest, that adequate safeguards are provided for the protection of privacy and that the Authority has granted an exemption. The Authority may impose restrictions and requirements when granting an exemption. This ensures proportionality with the objective pursued, respects the essential content of the right to the protection of personal data and takes appropriate and specific measures to protect the fundamental rights and fundamental interests of the data subject.

4.1.5 PBENG-U.01.05 Criminal convictions and criminal offenses

PBENG-U.01.05.T1 Verify directive
Investigative authorities should first verify whether Directive (EU) 2016/680 of 27 April 2016 is applicable to the protection of natural persons in connection with the processing of personal data by competent authorities for the purposes of prevention, investigation, detection and investigation. the prosecution of criminal offenses or the execution of penalties and the free movement of such data.

PBENG-U.01.05.T2 Verify specific legal act
The protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security and the free movement of such data, is the subject of a specific Union legal act. This Regulation should not, therefore, apply to processing activities for those purposes. However, personal data processed by public authorities under this Regulation should, when used for those purposes, be governed by a more specific Union legal act, namely Directive (EU) 2016/680 of the European Parliament and of the Council. Member States may entrust competent authorities within the meaning of Directive (EU) 2016/680 with tasks which are not necessarily carried out for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and prevention of threats to public security, so that the processing of personal data for those other purposes, in so far as it is within the scope of Union law, falls within the scope of this Regulation (see GDPR Recital 19).

PBENG-U.01.05.T3 Legitimate purpose
Indicating possible criminal acts or threats to public security by the controller and transmitting the relevant personal data in individual cases or in several cases relating to the same criminal act or threats to public security to a competent authority should be regarded as being in the legitimate interest pursued by the controller. However, such transmission in the legitimate interest of the controller or further processing of personal data should be prohibited if the processing is not compatible with a legal, professional or other binding obligation of secrecy (see GDPR Recital 50).

4.1.5.1 PBENG-U.01.05.01 Exception on data relating to criminal convictions

Processing of personal data relating to criminal convictions and offences (including a prohibition imposed by the court in connection with unlawful or obstructive behaviour) or related security measures is only possible when (see "Uitvoeringswet AVG" article 31):

a) if the processing is carried out by bodies charged with the application of criminal law by law, as well as by controllers who have obtained them pursuant to the Police Data Act or the Judicial and Criminal Data Act;
b) if the controller has to process this data for their own benefit:
    1. to assess a request by data subject to make a decision about him or to provide him with a performance, or:
    2. for the protection of his interests insofar as it concerns criminal offenses which are or are expected to be committed on the basis of facts and circumstances against him or against persons who are in his service;
c) if these are processed for third parties:
    1. by controllers who act pursuant to a license pursuant to the Private Security Organizations and Investigation Offices Act;
    2. by a controller who is also a legal entity and is affiliated to the same group as referred to in Section 2: 24b of the Dutch Civil Code, or:
    3. by a controller who has obtained permission from the Authority for this.

4.1.5.2 PBENG-U.01.05.02 Processors of data relating to criminal convictions

Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority (see GDPR article 10).

4.1.5.3 PBENG-U.01.05.03 Processing personnel data

The processing of the data on personnel employed by the controller is carried out in accordance with rules established in accordance with the procedure referred to in the "Wet op de ondernemingsraden" (see "Uitvoeringswet AVG" article 31 paragraph 2).

4.1.5.4 PBENG-U.01.05.04 Processing personnel data exception

The prohibition to process personal data does not apply when it is necessary in addition to the processing of criminal data for the purposes for which this data is processed (see "Uitvoeringswet AVG" article 31 paragraph 3).

4.1.5.5 PBENG-U.01.05.05 Exception processing of criminal data controllers

Processing of personal data relating to criminal convictions and offences or related security measures is permitted, if this is done by and on behalf of public-law partnerships of controllers or groups of controllers, if the processing is necessary for the execution of the task of these controllers or groups of controllers and when appropriate safeguards for the rights and freedoms of data subjects are provided (see "Uitvoeringswet AVG" article 31 paragraph 4).

4.1.6 PBENG-U.01.06 National identification number

4.1.6.1 PBENG-U.01.06.01 Burgerservicenummer

Determining a number that is prescribed by law for the identification of a person is only used for the implementation of the relevant law or for purposes specified by law:

a) Government bodies can use the citizen service number (BSN) when processing personal data in the context of carrying out their public task, without further regulations being required.
b) The citizen service number (BSN) as unique personal number complies with article 10 of the "Wet algemene bepalingen burgerservicenummer (Wabb)".
c) For institutions that cannot appeal to Wabb art. 10 the use should be prescribed in sectoral legislation. For example, for the healthcare sector, the "Wet gebruik burgerservicenummer in de Zorg" applies and banks must use the BSN for exchange of information with the Tax Authorities. In addition, other identifying numbers are in use, for example the education number, which corresponds to the citizen service number, unless the participant does not have a citizen service number.

PBENG-U.01.06.01.01 Explanation (1)
Article 87 of the GDPR provides a basis for setting specific conditions under Member State law for the processing of the national identification number. Article 38 of the "Uitvoeringswet AVG" regulates the use of statutory numbers.

Article 46 of the "Uitvoeringswet AVG" regulates that a number that is prescribed by law for the identification of a person is only used in the processing of personal data for the implementation of the relevant law or for purposes specified by law. The article describes the use of an "algemene maatregel van bestuur" on which other laws can be interpreted in such numbers.

For the government, the use of a unique personal number, the "BurgerServiceNummer" (BSN), is regulated in Wabb art. 10. Government bodies may use the BSN in the processing of personal data in the context of carrying out their public duties without further regulations being required. For institutions that cannot appeal to Wabb art. 10 the use should be prescribed in sectoral legislation. For example, for the healthcare sector, the Act on the use of a BSN in healthcare applies and banks must use the BSN for exchange of information with the Tax Authorities. In addition, other identifying numbers are in use, for example the education number, which corresponds to the BSN, unless the participant does not have a BSN. Neither in the provision as included in the Wbp nor in sector-specific regulations are changes foreseen for the BSN (see "Uitvoeringswet AVG Mvt", paragraph 4.10).

4.1.7 PBENG-U.01.07 Automated decision making

PBENG-U.01.07.T1 Term decision
The term 'decision' in the sense of the GDPR must be read more broadly than the decision-making from the "Awb"; private parties also fall under the scope of this provision when they make use of automated decision-making.

PBENG-U.01.07.T2 Negative characteristics
The negative characteristics of a certain group may not be thrown against an individual. The individual does not have to have these characteristics at all.

PBENG-U.01.07.T3 Specific protection children
Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child. The consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child (see GDPR recital 38).

4.1.7.1 PBENG-U.01.07.01 Automated individual decision-making

The data subject shall have the right not to be subject to a decision, unless the decision:

a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;
b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
c) is based on the data subject's explicit consent.

4.1.7.2 PBENG-U.01.07.02 Automated individual decision-making exception (I)

In the cases referred to in points (a) and (c) of PBENG-U.01.07.01, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

4.1.7.3 PBENG-U.01.07.03 Automated individual decision-making exception (II)

Decisions referred in points (a) and (c) of PBENG-U.01.07.01 shall not be based on special categories of personal data, unless point (a) or (g) of PBENG-U.01.04.01 apply and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

4.1.8 PBENG-U.01.08 Scientific or historical research or statistical purposes or archiving purposes in the public interest

PBENG-U.01.08.T1 Processing reference
Processing personal data for scientific or historical research or with a statistical objective are addressed at several locations in the GDPR.

PBENG-U.01.08.T2 Processing not incompatible
First, further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes. Also, personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes and is subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (see GDPR article 5 paragraph 1b and 1e). These provisions work directly in the Dutch legal system and do not require transposition into Dutch law.

PBENG-U.01.08.T3 Research options
For the processing of special personal data for scientific or historical research or statistical purposes, two options are available. In the first place, processing is possible after explicit consent of the data object. With regard to processing data for scientific research, explicit permission from the data subjects has its own specific meaning. It is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research. Data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose. (GDPR Recital 33)

PBENG-U.01.08.T4 Processing in public interest
Processing is also possible if processing serves a public interest, processing must be necessary for scientific or historical research or statistical purposes and, finally, guarantees must be provided in the course of implementation to ensure that the privacy of the data subject is not disproportionately damaged (see GDPR article 27).

PBENG-U.01.08.T5 Comply to conditions
Furthermore, the processing must of course also comply with the other applicable conditions set by the GDPR and by this law.

4.1.8.1 PBENG-U.01.08.01 Scientific research/statistics

Where (special categories of) personal data are processed for scientific or historical research purposes or archiving purposes in the public interest (see article 9 paragraph 2j and see "Uitvoeringswet AVG" article 27):

a) The research serves a public interest;
b) the provision of such information proves impossible or would involve a disproportionate effort;
c) asking for explicit consent proves impossible or would involve a disproportionate effort, and:
d) suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

4.1.8.2 PBENG-U.01.08.02 Scientific research/archiving

Processing of personal data for the purpose of scientific research or archiving takes place only if appropriate technical and organizational measures have been taken to protect the rights and freedoms of the data subject:

- ensuring the purpose limitation (see GDPR article 5 paragraph 1b) (e.g. by pseudonymisation) and:
- data subject can no longer be identified (see GDPR article 5 paragraph 1e).

4.2 PBENG-U.02 Register of processing activities

In order to demonstrate compliance with this Regulation, the controller or processor should maintain records of processing activities under its responsibility (see GDPR recital 82).

This can be recorded via data management within an organization. The records show how the various organizational units support the business processes and which security measures have been taken (in outline) for the processing operations and data subjects. The register makes supervision of the processing activities possible.

PBENG-U.02.T1 Definitions

PBENG-U.02.T1.01 Criteria

The controller and the processor have recorded their data on data processing in a register, whereby the register provides an up-to-date and coherent image of the data processing, processes and technical systems involved in the collection, processing and transfer of personal data.

PBENG-U.02.T1.02 Objective

The purpose of a 'Register of processing activities' is to provide insight into the processing and data flows within the organization and in the parties that handle the processing of personal data on behalf of the organization.

PBENG-U.02.T1.03 Risk

Not having an overview of processing results in an incomplete image of the processed categories of personal data and measures taken for the relevant processing, processes and technical systems.

PBENG-U.02.T1.04 Referentie

GDPR: Article 30

Uitvoeringswet AVG:

4.2.1 PBENG-U.02.01 Register

PBENG-U.02.01.T1 Centralized unit

Keeping the register of data processing can be done by a centralized unit. This improves the possibilities to give an up-to-date and coherent picture. This is usually done by the Data Management component.

4.2.1.1 PBENG-U.02.01.01 Register of controllers

Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility, unless there is an exception (PBENG-U.02.01.06).

4.2.1.2 qPBENG-U.02.01.02 Content of register of controllers

That record of the processing activities of the controller shall contain all the following information (see GDPR article 30 paragraph 1):

1. the name and contact details of
    a. the controller and, where applicable, the joint controller,
    b. where appropriate
        i. the controller's representative and
        ii. the data protection officer;
2. The purposes of the processing;
3. a description of the categories of data subjects;
4. of the categories of personal data;
5. the categories of recipients to whom the personal data have been or will be disclosed;
6. in case of transfers to a third country or an international organisation:
    a. the transfer of personal data
    b. the identification of that third country or international organisation;
    c. the documentation of appropriate safeguards;
7. where possible, the envisaged time limits for erasure of the different categories of data;
8. where possible, a general description of the technical and organisational security measures.

4.2.1.3 PBENG-U.02.01.03 Register of processors

Each controller and, where applicable, the controller's representative, shall maintain a record categories of processing activities under its responsibility, unless there is an exception (PBENG-U.02.01.06).

4.2.1.4 PBENG-U.02.01.04 Content of Register of processors

That record of the processors with categories of processing activities shall contain all the following information (see GDPR article 30 paragraph 1):

1. the name and contact details of
    a. the processors,
    b. where appropriate of every controller for who processer process data:
        i. the controller's representative or
        ii. the processor and the data protection officer;
2. of the categories of processing activities that are performed for controller;
3. in case of transfers to a third country or an international organisation:
    a. the transfer of personal data
    b. the identification of that third country or international organisation;
    c. the documentation of appropriate safeguards;
4. where possible, a general description of the technical and organisational security measures.

4.2.1.5 PBENG-U.02.01.05 Electronic register

The records shall be in writing, including in electronic form.

4.2.1.6 PBENG-U.02.01.06 Exception on register obligation

The obligations to keep a register shall not apply if,

1. an enterprise or an organisation employing fewer than 250 persons
2. the processing it carries out is not likely to result in a risk to the rights and freedoms of data subjects,
3. the processing is occasional, and:
4. the processing does not include special categories of data or personal data relating to criminal convictions and offences.

4.2.2 PBENG-U.02.02 Current and coherent image

4.2.2.1 PBENG-U.02.02.01 Cohesive registers

The registers of the controller and the processor provide one coherent image.

PBENG-U.02.02.01.01 Explanation (1)
The mutual coherence and dependencies between all interlocking components involved in the processing of the personal data have been named and described.

4.2.2.2 PBENG-U.02.02.02 Request AP

At the request of the AP, an up-to-date picture is given by means of the registers.

4.2.2.3 PBENG-U.02.02.03 Content cohesive registers

The mutual coherence (data flows) and dependencies between:

1. the business processes;
2. organizations and organizational components;
3. the processing;
4. the locations where personal data is stored;
5. the data exchanges (inside and outside the organization);
6. the systems have been named and described.

PBENG-U.02.02.03.01 Explanation (1)
There may be a need for information about the underlying logic of the automated processing of the personal data if, for example, special computer software allows a manner of processing that the data subject is not entirely clear at first glance. This does not have to go so far that the Copyright and / or Intellectual Property Law that protects the software or the trade secret is violated.

4.2.2.4 PBENG-U.02.02.04 Result DPIA as part of register

When changes to existing and new processing operations occur, the results from the data protection impact assessment (DPIA) are included in the register of data processing activities.

PBENG-U.02.02.04.01 Explanation (1)
The description of mutual dependencies provides insight into the context of a processing and, in the event of changes to a processing process, provides insight into the consequences for other processing operations and vice versa.

PBENG-U.02.02.04.02 Explanation (2)
As a result of changes in the context, the threat assessment, changes at the organizational level, changes in the state of the art or changes in processing, changes in the processing itself or the guarantees for the safe processing. The register must be maintained with the relevant information to provide insight into the compliance status and the assessment of the extent to which the safeguards are appropriate for the processing.

4.3 PBENG-U.03 Quality management

Quality management ensures that the processing, correctness and accuracy of personal data is monitored and that, in case of incorrectness or inaccuracy of data or in case of unwanted processing, it is possible to rectify, complete, delete personal data or limit its processing or revoke consent to data processing.

PBENG-U.03.T1 Definitions
PBENG-U.03.T1.01 Criteria
The controller has set up quality management to be able to monitor the correctness and accuracy of personal data. Processing is arranged in a way that the personal data can be corrected, discontinued or transferred. If this happens at the request

PBENG-U.03.T1.02 Objective
Quality management must ensure that data processing is correct and in accordance with the wishes the data subjects.

PBENG-U.03.T1.03 Risk
If the data is incorrectly and inaccurately entered or is corrupted, incorrect conclusions could be drawn about the data subject with negative consequences as a result or lead to undesirable processing of personal data according to the data subject.

PBENG-U.03.T1.04 Referral
GDPR: Article 7 part 3, 11 part 2, 12, 16, 17, 18, 19, 20, 21, 22, 23

Uitvoeringswet AVG:

4.3.1 PBENG-U.03.01 Correctness and accuracy

4.3.1.1 PBENG-U.03.01.01 Measures correctness and accuracy

The controller has taken the necessary measures to ensure the accuracy and accuracy of personal data.

PBENG-U.03.01.01.01 Explanation (1)
The controller will take the necessary measures to ensure the correctness and accuracy of personal data. The 'necessary measures' are those measures that can reasonably be expected from the controller. What can reasonably be expected depends on the type of data, the state of the technology and the costs associated with the measures. Ensuring the correctness and accuracy of the personal data is therefore a best-effort obligation for the controller and not a result obligation. The measures taken have been shown to have been examined and assessed to ensure that these measures are adequate. Examples of necessary measures are:

a) to set up the (technical) possibility to be able to correct;
b) determining and confirming when and by whom periodic checks are carried out on the correctness, accuracy, topicality, completeness and correct use of the data and by whom the personal data - if necessary - are corrected;
c) identifying and restricting persons and departments that have access to the personal data, while also gaining certainty about the way in which the accuracy of data on access is guaranteed and that the data are not used for purposes other than the required objective;
d) identifying and restricting parties to whom personal data may be provided, while at the same time obtaining certainty about the way in which the accuracy of the data is guaranteed when it is provided, and that the data are not used for purposes other than the required objective;
e) identifying the consequences of the incorrect use of personal data and / or how these consequences can be overcome;
f) when appointing a processor:

- to demonstrate that it has been investigated and assessed that the relevant processor offers sufficient quality in view of the nature of the work and the associated privacy risks;
- the obligations of secrecy are guaranteed by establishing this and recording it in the processor agreement.

Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either:

a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or
b) refuse to act on the request.

The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request (see GDPR article 12 paragraph 5).

4.3.1.2 PBENG-U.03.01.02 Periodic checks measures

The controller conducts periodic checks on the proper operation of the measures and reports to senior management.

4.3.2 PBENG-U.03.02 Revised, suspended or transferred

4.3.2.1 PBENG-U.03.02.01 Rectification of personal data

At the data subject's request, inaccurate personal data will be rectified (see GDPR article 16 paragraph 1).

PBENG-U.03.02.01.01 Explanation (1)
The right to correction can be restricted by means of statutory provisions that apply to the controller or the processor (see GDPR article 23 paragraph 1).

4.3.2.2 PBENG-U.03.02.02 Completion of personal data

At the data subject's request incomplete personal data shall be completed (taking into account the purposes of the processing), including by means of the provision of a supplementary statement by data subject (see GDPR article 16 paragraph 1).

4.3.2.3 PBENG-U.03.02.03 Erasure of personal data

At the data subject's request personal data concerning him or her shall be erased where one of the following grounds applies (see GDPR article 17 paragraph 1):

a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
b) the data subject withdraws consent on which the processing is based, and where there is no other legal ground for the processing;
c) the data subject objects to the processing and there are no overriding legitimate grounds for the processing;
d) the personal data have been unlawfully processed;
e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
f) the personal data of children younger than 16 have been collected in relation to the offer of information society services.

PBENG-U.03.02.03.01 Explanation (1)
The right to erasure ("right to be forgotten") does not apply to the extent that processing is necessary:

a) for exercising the right of freedom of expression and information;
b) for compliance with a legal obligation which requires processing to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
c) for reasons of public interest in the area of public health;
d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with, so far as the right is likely to render impossible or seriously impair the achievement of the objectives of that processing;
e) for the establishment, exercise or defence of legal claims (see GDPR article 17 paragraph 3).

PBENG-U.03.02.03.02 Explanation (2)
The right to erasure is not applicable if the processing is necessary:

a) for exercising the right of freedom of expression and information;
b) for compliance with a statutory processing obligation resting on the controller or for carrying out a task of public interest or exercising the public authority granted to the controller;;
c) for reasons of public interest in the area of public health;
d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with, so far as the right is likely to render impossible or seriously impair the achievement of the objectives of that processing;
e) for the establishment, exercise or defence of legal claims.

4.3.2.4 PBENG-U.03.02.04 Processing ceased in case of objection

When data subject objects, the controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims (see GDPR article 21 paragraph 1).

4.3.2.5 PBENG-U.03.02.05 Erasure also at third parties

Where the controller has made the personal data public and is obliged to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data (see GDPR article 17 paragraph 2).

4.3.2.6 PBENG-U.03.02.06 Restriction of processing

At data subject's request controller shall restrict the processing where one of the following applies:

a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;
b) the processing is unlawful, and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;
d) the data subject has objected to processing pending the verification whether the legitimate grounds of the controller override those of the data subject.

PBENG-U.03.02.06.01 Explanation (1)
The right to limit the processing applies if the processing (including profiling) takes place for (GDPR article 21 paragraph 1):

a) the performance of a task carried out in the public interest;
b) the performance of a task carried out in the exercise of official authority;
c) for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child;
d) direct marketing, or:
e) scientific or historical research purposes or statistical purposes, unless processing is necessary for the performance of a task carried out in the public interest.

4.3.2.7 PBENG-U.03.02.07 Right to obtain personal data/data portability other controller

The data subject has the right to receive the personal data concerning him or her in a structured, commonly used and machine-readable format and has the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where processing:

a) is based on consent or
b) is based on a contract to which the data subject is involved, or the processing is carried out by automated means;

But is not granted if:
a) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
b) is adversely affects the rights and freedoms of others.

4.3.2.8 PBENG-U.03.02.08 Change controller

The data subject is able to have the personal data transmitted directly from one controller to another, where technically feasible and PBENG-U.03.02.07 applies.

4.3.3 PBENG-U.03.03 Informed

4.3.3.1 PBENG-U.03.03.01 Communicate third parties about changes

The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort (see GDPR article 19).

4.3.3.2 PBENG-U.03.03.02 Inform data subject about communication

The controller shall inform the data subject about the recipients that receive a communication if the data subject requests it (see GDPR article 19).

4.3.3.3 PBENG-U.03.03.03 Inform about rectification

The controller shall provide information on rectification of personal data to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request.

4.3.3.4 PBENG-U.03.03.04 Electronic response

Where the data subject makes the request by electronic means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject (see GDPR article 12 paragraph 3).

4.3.3.5 PBENG-U.03.03.05 Response in writing

The controller shall respond in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means (GDPR article 12 paragraph 1).

4.3.3.6 PBENG-U.03.03.06 Response when request rejection

If the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy (see GDPR article 12 paragraph 4).

4.3.3.7 PBENG-U.03.03.07 Reaction on non-identification

When the controller is able to demonstrate that it is not in a position to identify the data subject, the controller shall inform the data subject accordingly. The data subject can provide additional information enabling his or her identification (see GDPR articles 11 and 12, and GDPR recital 57).

PBENG-U.03.03.07.01 Explanation (1)
The controller can, when he has reasonable doubts concerning the identity of the natural person making the request, request the provision of additional information necessary to confirm the identity of the data subject (see GDPR article 12 paragraph 6 and recital 58, 59).

4.4 PBENG-U.04 Securing the processing of personal data

Information security is the set of preventive, detective, repressive and corrective measures, as well as procedures and processes to limit any consequences of security incidents to an acceptable (appropriate), predetermined level. The measures are based on a risk analysis and legal obligations (including the GDPR).

PBENG-U.04.T1 Definitions
PBENG-U.04.T1.01 Criteria
the controller and the processor shall implement technical and organisational measures to ensure the appropriate level of security of the data processing (see GDPR article 32).

PBENG-U.04.T1.02 Objective
The purpose of 'Securing the processing of personal data' is to protect personal data against loss, unavailability, corruption and any form of unlawful or unnecessary collection and (further) processing.

PBENG-U.04.T1.03 Risk
The unwanted publication, manipulation, abuse and unavailability of data.

PBENG-U.04.T1.04 Referral
GDPR: Article 32

Uitvoeringswet AVG: Paragraph 5.2.4

4.4.1 PBENG-U.04.01 Technical and organizational measures

4.4.1.1 PBENG-U.04.01.01 Limited access

The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law (see GDPR article 32 paragraph 4),

PBENG-U.04.01.01.01 Explanation (1)
Such measures could consist, inter alia, of minimising the processing of personal data, pseudonymising personal data as soon as possible (see GDPR recital 78). Technical measures are measures in and around information systems, such as access controls, recording usage and back-up, password protection and encryption. The security is not limited to own information systems but extends to externally placed backup and the storage and processing at and by third parties (Receiving a back-up and the storage of personal data is considered 'processing' of personal data).

PBENG-U.04.01.01.02 Explanation (2)
Physical personal data are also physically protected, such as building zoning and locks on cabinets.

4.4.1.2 PBENG-U.04.01.02 Physical security

Personal data are physically protected against theft and unauthorized access:

1. If personal data exist physically, they are also physically protected.
2. The method of collecting data is not privacy-sensitive.

4.4.1.3 PBENG-U.04.01.03 Organizational security

Personal data are protected organisationally by means of measures for the set up of the organization, which are included in an information security plan.

PBENG-U.04.01.03.01 Explanation (1)
The controller has taken adequate organizational measures to secure the data and can demonstrate this. Organizational measures are measures for organizing the organization and for processing personal data, such as allocation and division of responsibilities, authorities, instructions, training courses, emergency plans and confidentiality obligations. A good way to safeguard and demonstrate this is to draw up and keep a security plan up to date.

PBENG-U.04.01.03.02 Explanation (2)
The GDPR speaks instead of a security plan about binding corporate rules: "the application of the general data protection principles, in particular purpose limitation, data minimisation, limited storage periods, data quality, data protection by design and by default, legal basis for processing, processing of special categories of personal data, measures to ensure data security, and the requirements in respect of onward transfers to bodies not bound by the binding corporate rules".

PBENG-U.04.01.03.03 Explanation (3)
For privacy, no separate security plan has to be made; if additional security measures have to be taken to protect personal data, this can be included in the regular security plan. Also, the "Richtsnoeren van de AP" about securing personal data can be implemented in the regular security plan.

PBENG-U.04.01.03.04 Explanation (4)
For example, the security plan includes:

a) what technical, organizational and physical security measures have been taken
b) what standards the organization has adopted;
c) how any indications (guidelines, policy rules) of the AP about the protection of personal data have been implemented
d) how confidentiality of employees is arranged;
e) what actions the responsible processor takes in data leaks;
f) how the processor periodically demonstrates the compliance to agreements;
g) how control on compliance with the security measures has implemented;
h) how instructions and training are given on the way in which personal data needs to be protected;
i) a disaster plan;
j) the cyclical adjustment of security as part of the daily practice of the organization, so that the security measures are part of the daily practice of the organization;
k) the inclusion of the technical and organizational measures in the processor agreement, with continuous monitoring of its execution and immediate intervention if this is not met;
l) how the measures are periodically tested and adjusted if they no longer offer sufficient protection;
m) allocation and division of responsibilities and authorities with regard to the handling of personal data;
n) appointing an overall responsible within the organization for drafting, implementing and maintaining the security policy.

4.4.1.4 PBENG-U.04.01.04 PET measures

Appropriate technical and organisational measures to ensure a level of security appropriate to the risk, include inter alia (see GDPR article 32 - the information security article):

1. the pseudonymisation and encryption of personal data;
2. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
3. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
4. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

PBENG-U.04.01.04.01 Explanation (1)
Privacy Enhancing Technologies (PET) is a common collective term for a number of privacy protection techniques that can be applied. A central principle of PET is to reduce the traceability of personal data to the data subject, with anonymization of data as the heaviest form (see Borking, J., Privacyrecht is code. About the use of Privacy Enhancing Technologies, Kluwer, Den Haag, 2010. CBP Richtsnoeren voor het beveiligen van persoonsgegevens 2013, p.13): after anonymization, the data can no longer be traced back to the original data.

A similar technique is pseudonymisation. The GDPR defines pseudonymizing as (see GDPR article 4 paragraph 5): "the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person".

PBENG-U.04.01.04.02 Explanation (2)
When applying pseudonymisation, the additional data used to link the personal data to a specific data subject must be stored separately.

PBENG-U.04.01.04.03 Explanation (3)
The explicit introduction of pseudonymizing as referred to in the GDPR is not intended to exclude other data protection measures (see GDPR article 5 paragraph 5).

PBENG-U.04.01.04.04 Explanation (4)
Special aspects in this respect are:

- Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted (see GDPR recital 39).
- The controller should use all reasonable measures to verify the identity of a data subject who requests access, in particular in the context of online services and online identifiers (see GDPR recital 64).

4.4.2 PBENG-U.04.02 Appropriate level

4.4.2.1 PBENG-U.04.02.01 Appropriate protection level

The technical, organizational and physical security measures provide an adequate level of protection for all processing of personal data and this can be demonstrated. To this end, the measures are proportional and subsidiary.

PBENG-U.04.02.01.01 Explanation (1)
When determining the appropriate level, the technical possibilities and the costs of implementation in relation to the risks and the nature of the personal data to be protected, should be taken into account (see GDPR recital 83).

PBENG-U.04.02.01.02 Explanation (2)
A controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures (see GDPR article 28 paragraph 1).

PBENG-U.04.02.01.03 Explanation (3)
Not the toughest technical security has to be chosen, but the most adequate. The NEN-ISO 27001/27002 and the derived government standards (like the Baseline Informatiebeveiliging Rijksdienst (BIR) and the Baseline Informatiebeveiliging Gemeenten (BIG) are at the moment the standard for adequate security (see Zwenne, G.J. en Knol. PC., Tekst en Commentaar Telecommunicatie- en Privacyrecht, Kluwer, Deventer, 2013, p.726). Whether this is really adequate, also depends on the scope and the applicability provision. It is important to realise that the BIR and the BIG do not replace the NEN-ISO standards, but are a practical implementation guide. The full NEN-ISO standards have to be checked, always.

PBENG-U.04.02.01.04 Explanation (4)
In order to be able to determine the appropriate level of protection on the basis of the risk analysis, the next quality requirements must be met (Borking, J., Privacyrecht is code. About the use of Privacy Enhancing Technologies, Kluwer, Den Haag, 2010, p.117 en CBP, Richtsnoeren voor het beveiligen van persoonsgegevens, Den Haag, 2013, p.13):

a) Availability (the undisturbed progress of data processing): the personal data and the information derived from them must be available without obstacles in accordance with the agreements made and the legal requirements.
b) Integrity (the accuracy of the data): the personal data must be in accordance with the depicted part of the reality and nothing can be wrongly withheld or suppressed.
c) Exclusivity (the confidentiality of the data): only authorized persons have access to the personal data.
d) Verifiability (to be able to check afterwards whether the above quality requirements have been met): the extent to which it is possible to establish that the processing of personal data has been carried out in accordance with the aforementioned quality aspects.

PBENG-U.04.02.01.05 Explanation (5)
The controller may demonstrate the measures by adopting policies and implementing measures that comply with the principles of Data protection by Design and Data Protection by Default in particular (see PBENG-B.03).

PBENG-U.04.02.01.06 Explanation (6)
If greater security can be achieved at small additional costs, these must be considered 'appropriate', while costs that are disproportionate in relation to the additional security that would be obtained as a result are not required.

4.4.2.2 PBENG-U.04.02.02 Security measures based on risk analysis

The security measures are based on an analysis of the processing risk (risk analysis). In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed (see GDPR article 32 paragraph 2).

PBENG-U.04.02.02.01 Explanation (1)
The desired level of security is determined in the risk analysis. By carrying out a risk analysis, it becomes clear which measures are necessary to manage certain risks. The security measures need to be proportionate to the nature of the data. As the data, for example, have a more confidential character or the context in which they are used constitute a greater threat to privacy, stricter requirements are imposed on the security of the data. Some data are more confidential by nature (such as special personal data such as race, religion, sexual preference, biometric data and login data), other data will be kept confidential if placed in a specific context (eg data on the out-of-home placement of a minor, or about the financial situation of a person). An additional rule of thumb: the greater the collection of personal data of a specific data subject, the more risky and therefore more confidential this data can become.

PBENG-U.04.02.02.02 Explanation (2)
The levels of technical, organizational and physical measures are periodically evaluated and, if necessary, updated so that the level remains appropriate.

An Information Security Management System (ISMS) offers an organization a process approach for managing information security. ISO / IEC 27001 is the standard for this. This standard document describes the cyclic process (plan / do / check / act) for defining security objectives based on a risk assessment, taking measures and monitoring and assessing the outcomes. See for information security in healthcare: https://www.werkenmetnen7510.nl.

PBENG-U.04.02.02.03 Explanation (3)
When special personal data are involved, or unique identifying data (such as BSN numbers, fingerprints, biometric data) or data about vulnerable groups, persons or user names, passwords and other log-in data, this requires extra attention to risk analysis and possible measures. (Member States may further determine the specific conditions for the processing of a national identification number or any other identifier of general application (see GDPR article 87)).

4.4.2.3 PBENG-U.04.02.03 Demonstrate appropriate measures

Adherence to an approved code of conduct or an approved certification mechanism may be used as an element by which to demonstrate compliance with the requirements.

4.5 PBENG-U.05 Information provisioning to the data subject

Anyone, providing personal data to an organization, has the right to know for what purpose, in which way and by whom this data is processed. The organization has an obligation to provide this information. This obligation to inform also applies when personal data is received from others.

PBENG-U.05.T1 Definitions

PBENG-U.05.T1.01 Criteria

The controller shall inform the data subject timely and in a fixed and predetermined manner about each collection of personal data, so that the data subject, unless an exception applies, can give permission for the processing (see GDPR article 14).

PBENG-U.05.T1.02 Objective

The purpose of 'Information provisioning to the data subject' is to ensure that the data subject is informed on the existence of the data collection and processing (see GDPR article 12 and recital 60), so that the data subject can exercise his rights in accordance with the principles of fair and transparent processing.

PBENG-U.05.T1.03 Risk

The organization is not transparent, so the organization cannot justify that the data processing complies with the principles of proper and transparent processing, with potentially high costs as a result.

PBENG-U.05.T1.04 Referral

GDPR: Article 13, 14, 15

Uitvoeringswet AVG: Paragraph 4.2.1

4.5.1 PBENG-U.05.01 Timely

4.5.1.1 PBENG-U.05.01.01 Prior consent

The consent of data subject is obtained prior to processing, passing on to third parties and further processing (see GDPR article 14 paragraph 3). This applies to personal data that is or has been obtained via data subject or others.

PBENG-U.05.01.01.01 Explanation (1)

The data subject does not have to provide his personal data until he has received the information from the controller.

PBENG-U.05.01.01.02 Explanation (2)

Where the controller intends to further process the personal data for a purpose other than that for which the personal data were obtained, the controller shall provide the data subject prior to that further processing with information (see GDPR article 14 paragraph 4).

4.5.1.2 PBENG-U.05.01.02 Inform about data not obtained for data subject

The controller shall provide information where information is not obtained from data subject within a reasonable period after obtaining the personal data, but at the latest within one month (see GDPR article 14 paragraph 3).

PBENG-U.05.01.02.01 Explanation (1)
Where personal data have not been obtained from the data subject, one can think of the linking of data, "chain computerization" and network computerization:

- Chain computerization is data exchange between two organizations in a chain (service chain).
- Network computerization is data exchange or joint control of data without a regular monitoring (chain) of actors.

PBENG-U.05.01.02.02 Explanation (2)
Transfer of personal data between parties in countries within the EU (including within the Netherlands) is covered by the general concept of processing. The 'communicator' of the data (the provider) remains responsible for the proper use of the personal data by others. Other / additional requirements apply to transfers to persons / organizations in countries outside the EU; for more information about the transfer of personal data (see PBENG-U.07).

PBENG-U.05.01.02.03 Explanation (3)
The GDPR includes the duty for the data provider (so not only for the recipient) to actively inform the data subject about the transfer of his / her personal data before the transfer takes place (see GDPR article 14, paragraph 1).

4.5.2 PBENG-U.05.02 Information

4.5.2.1 PBENG-U.05.02.01 Clear and plain language

The request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language (see GDPR article 7 paragraph 2).

PBENG-U.05.02.01.01 Explanation (1)
The information must be in clear and plain language for the 'ordinary citizen'.

PBENG-U.05.02.01.02 Explanation (2)
The information must be provided in a way that data subject actually has it. This can be done in many ways; both orally, in writing, digitally, etc. It is up to the controller to be able to prove that the information was actually provided to the data subject, so written communication is preferable.

4.5.2.2 PBENG-U.05.02.02 Information provided to data subject (I)

Where personal data relating to a data subject are collected from the data subject, the data subject shall receive the following information (see GDPR article 13):

a) the identity and the contact details of the controller;
b) the contact details of the data protection officer, where applicable;
c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;
e) the recipients or categories of recipients of the personal data, if any;
f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available;
g) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
h) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
i) where the processing is based consent, the existence of the right to withdraw consent at any time;
j) the right to lodge a complaint with a supervisory authority;
k) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract
l) as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;
m) the existence of automated decision-making, including profiling, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject
n) information on further processing, when purpose of further processing is other than for which personal data was collected.

4.5.2.3 PBENG-U.05.02.03 Information provided to data subject (II)

Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information (see GDPR article 14):

a) the identity and the contact details of the controller and, if any, of the controller's representative;
b) the contact details of the data protection officer, where applicable;
c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
d) the categories of personal data concerned;
e) the recipients or categories of recipients of the personal data, where applicable;
f) where applicable, that the controller intends to transfer personal data to a recipient in a third country or international organisation and the existence or absence of an adequacy decision by the Commission, reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available.
g) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
h) where the processing is based on a legitimate interest, the legitimate interests pursued by the controller or by a third party;
i) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to processing as well as the right to data portability;
j) where processing is based on consent, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
k) the right to lodge a complaint with a supervisory authority;
l) from which source the personal data originate, and if applicable, whether it came from publicly accessible sources;
m) the existence of automated decision-making (including profiling), including meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

4.5.3 PBENG-U.05.03 Exception

4.5.3.1 PBENG-U.05.03.01 Exception on information providing

The obligation to provide information does not apply where and insofar as:

- the data subject already has the information;
- the provision of such information proves impossible or would involve a disproportionate effort;
- the objectives of that processing is likely to render impossible or the achievement is seriously impaired (in such cases the controller shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available);
- obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interests; or
- where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy;
- when the processing is based on a statutory provision, with a specific exception;
- it is the processing of personal data that are part of archival records and that are not eligible for destruction under the “Archiefwet” and that have been transferred to an archive (see "Uitvoeringsweg AVG Mvt", explanation to article 41).

PBENG-U.05.03.01.01 Explanation (1)
The controller must be able to demonstrate that the data subject is already aware of this, if he wants to be able to invoke this exception.

PBENG-U.05.03.01.02 Explanation (2)
If the data subject possesses the information, for example because it has been handed over or sent to him, then he is aware of this, regardless of whether he takes the initiative to get the information. (see Mvt Wbp, Tweede Kamer, vergaderjaar 1997–1998, 25 892, nr.3, pp.151, 152).

PBENG-U.05.03.01.03 Explanation (3)
The following specific restrictions apply (see GPDR article 23):

a) national security;
b) defence;
c) public security;
d) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;
e) other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation a matters, public health and social security;
f) the protection of judicial independence and judicial proceedings;
g) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;
h) a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a), (b), (c), (d), (e) and (g);
i) the protection of the data subject or the rights and freedoms of others;
j) the enforcement of civil law claims.

4.5.4 PBENG-U.05.04 Consent

4.5.4.1 PBENG-U.05.04.01 Freely given consent

Consent must be given freely by data subject. When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract (see GDPR article 7 paragraph 4).

PBENG-U.05.04.01.01 Explanation (1)
The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology (see GDPR article 8 paragraph 2).

4.5.4.2 PBENG-U.05.04.02 responsibility for child's consent

Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child (see GDPR article 8).

4.6 PBENG-U.06 Storage of personal data

Personal data may not be kept longer than is necessary to achieve the purpose for which they were collected or no longer than the retention period provided for by sector-specific legislation. The retention period can be terminated by actively deleting the data or by anonymizing the personal data. In the case of anonymisation, the data can no longer be traced back to the data subjects (see GDPR recital 27: "This Regulation does not apply to the personal data of deceased persons. Member States may provide for rules regarding the processing of personal data of deceased persons.").

PBENG-U.06.T1 Definitions

PBENG-U.06.T1.01 Criteria

By taking the appropriate measures, the organization uses a retention period for personal data that is not exceeded.

PBENG-U.06.T1.02 Objective

The purpose of 'Storage of personal data' is to guarantee that personal data is stored no longer than necessary for the purpose.

PBENG-U.06.T1.03 Risk

Unnecessary stored personal data can be processed for purposes other than the original ones.

PBENG-U.06.T1.04 Referral

GDPR: Article 5 part 1e

Uitvoeringswet AVG: Article 43

4.6.1 PBENG-U.06.01 Necessary measures

4.6.1.1 PBENG-U.06.01.01 End of storage period

When the retention periods expire, the data has been deleted, destroyed or anonymised.

PBENG-U.06.01.01.01 Explanation (1)

The controller must, after each processing of personal data, ask himself whether there are still reasons to keep the personal data in question.

PBENG-U.06.01.01.02 Explanation (2)

The law states as follows: Personal data must be kept in a form that makes it possible to identify the data subjects no longer than is necessary for the purposes for which the personal data are processed. In other words: if the data subject can no longer be identified on the basis of the data, no maximum storage period under the GDPR applies to these data.

PBENG-U.06.01.01.03 Explanation (3)

There is control on the removal, destruction or anonymization. Software removal or anonymization and destruction of data-bearing hardware is preferably done by a specialized organization.

4.6.1.2 PBENG-U.06.01.02 Determine

The controller determines after each processing of personal data whether there are still reasons to keep the personal data in question.

PBENG-U.06.01.02.01 Explanation (1)
If data linked to the personal data are of importance to keep longer, the personal data must be anonymised in such a way that it is then no longer possible to make this anonymised data traceable again. (see "Handleiding voor verwerkers van persoonsgegevens, handleiding van de Wbp", Ministerie van Justitie, 2002, p.126).

PBENG-U.06.01.02.02 Explanation (2)
If the personal data are recorded on a 'read only' data medium in which no changes can be made but data can be copied, such as a CD-ROM or DVD, measures have been taken so that the data can no longer be used in any way, neither recognized, used or otherwise processed. The data subject is also informed of the impossibility of removal or anonymization (Handleiding voor verwerkers van persoonsgegevens, handleiding van de Wbp, Ministerie van Justitie, 2002, p.37).

4.6.2 PBENG-U.06.02 Storage period

4.6.2.1 PBENG-U.06.02.01 Storage period for personal data

The retention period of all personal data has been determined and confirmed.

PBENG-U.06.02.01.01 Explanation (1)
Sometimes a purpose requires that personal data is retained, for example someone's e-mail address must be kept in order to prevent the person from receiving mailings.

4.6.2.2 PBENG-U.06.02.02 Maximum storage period

The retention period is the maximum period during which the personal data are stored in order to achieve purpose the processing or no longer than the period laid down in sector-specific legislation (see GDPR article 5 paragraph 1).

PBENG-U.06.02.02.01 Explanation (1)
In some (sector-specific) legislation, a retention period is specified for certain personal data. An example of this is the storage of medical data: in the Dutch Civil Code the period for this has been set at 15 years (see article 7: 454 paragraph 3 Dutch Civil Code). Also think about data about financial transactions.

4.6.2.3 PBENG-U.06.02.03 Legal storage period

If a storage period for specific personal data is specified in sector-specific legislation, then that retention period applies.

4.6.2.4 PBENG-U.06.02.04 Safeguards for longer storage

Personal data may be stored for longer periods (see GDPR article 5 paragraph 1, e) insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with article 89 (1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation').

PBENG-U.06.02.04.01 Explanation (1)
Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. They will ensure that personal data can no longer attributed to data subjects.

PBENG-U.06.02.04.02 Explanation (2)
The measures may include pseudonymisation, so that intended original purpose processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, can still be achieved.

4.7 PBENG-U.07 Transfer of personal data

Transfer may take place to processor(s) and to other controller(s). A processor performs the processing on behalf of a controller (see GDPR article 28 paragraph 1 and GDPR article 28 paragraph 10: If a processor infringes the GDPR, that processor is considered to be the controller). Where there are multiple controllers, they jointly determine the objectives and means for the processing and are joint controllers (see GDPR article 27 paragraph 1).

The transfer distinguishes between transfer within the EU, where the GDPR applies, and transfer to outside the EU. If transfer takes place outside the EU, the GDPR speaks of transfer to third countries and international organizations.

PBENG-U.07.T1 Definitions

PBENG-U.07.T1.01 Criteria

In case of transfer to another controller, the mutual responsibilities are clear and there are sufficient guarantees for the transfer to a processor.

When transferring outside the EU:

- ☒ is there a representative, and:
- ☒ there are no grounds for exception

And:

- ☒ an adequacy decision by European Commission is in order, or
- ☒ there are appropriate safeguards (see GDPR article 27, paragraph 1), or
- ☒ an exception applies for a specific situation.

PBENG-U.07.T1.02 Objective

The purpose of the requirements for 'Transfer of personal data' is to ensure that personal data are passed on in a legitimate manner, that they are used correctly and that the responsibility for this legality and correctness remains tuned.

PBENG-U.07.T1.03 Risk

If an organization does not meet this criterion, it is not clear to the organization what exactly is expected when passing on personal data, so that there is a chance that personal data will be passed on unlawfully and will be processed unlawfully and there is a lack of responsibility and control.

PBENG-U.07.T1.04 Referral

GDPR: Article 26, 27, 28, 29, 44, 45, 46, 47, 48, 49, 96

Uitvoeringswet AVG: -

4.7.1 PBENG-U.07.01 Respective responsibilities

4.7.1.1 PBENG-U.07.01.01 Responsibilities for transferring personal data

Where data is transferred to another controller:

a) their respective responsibilities are determined for compliance with the obligations under the GDPR, in particular as regards (see GDPR article 26 paragraph 1):
    1. the exercising of the rights of the data subject (PBENG-C.02), and
    2. informing data subject on receiving data (PBENG-U.05)
b) the respective responsibilities of the controllers are made available to data subjects (see GDPR article 26 paragraph 3).

PBENG-U.07.01.01.01 Explanation (1)
The responsibilities of the controllers can also be laid down in the legislation and regulations.

PBENG-U.07.01.01.02 Explanation (2)
A contact point can be designated for exercising the rights by data subjects. The data subject can also exercise his rights under the GDPR up to and against any controller (see GDPR article 26 paragraph 3).

PBENG-U.07.01.01.03 Explanation (3)
Examples of such arrangements can be found at:

https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/internationaal-gegevensverkeer/doorgifte-binnen-en-buiten-de-eu#welke-modelcontracten-zijn-er-voor-doorgifte-naar-een-derde-land-5524

4.7.2 PBENG-U.07.02 Sufficient guarantees

Adherence of a processor to an approved code of conduct or an approved certification mechanism may be used as an element by which to demonstrate sufficient guarantees. Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor shall be imposed on that other processor.

4.7.2.1 PBENG-U.07.02.01 Data processing agreement

Processing by a processor shall be governed by a contract or other legal act under Union or Member State law (see GDPR article 28, paragraph 2), that sets out:

a) the subject-matter and duration of the processing,
b) the nature and purpose of the processing for which personal data is transferred, including
    1. the personal data that is transferred
    2. how data minimisation is applied;
c) the type of personal data, including
    1. personal data classification;
d) categories of data subjects
e) the obligations and rights of the controller.

4.7.2.2 PBENG-U.07.02.02 Provisions processor agreement

The contract or other legal act with the processor shall stipulate that processor:

a) processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data;
b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
c) takes all measures required pursuant to PBENG-U.04, including:
    1. which employees of the processor need access to the personal data;
    2. which procedure is followed in case of a data breach; in which countries personal data are stored;
d) respects the conditions for engaging another processor;
e) has made appropriate technical and organisational measures, for exercising the data subject's rights, including
    1. how the data subject is informed about the outsourcing of the personal data to the processor;
    2. the contact that the processor may have with data subjects;
f) assists the controller in ensuring compliance with the obligations pursuant to ensuring the security of the processing
g) deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, at the choice of the controller pursuant PBENG-U.06;
h) makes available to the controller all information necessary to demonstrate compliance and contribute to audits, including inspections,
i) the processor informs the controller immediately if, in his opinion, an instruction violates the GDPR or other data protection laws and regulations.

4.7.2.3 PBENG-U.07.02.03 Data process agreement in writing

The contract or the legal act shall be provided in writing, or by other means, including, where appropriate, by electronic means.

4.7.3 PBENG-U.07.03 Representative

4.7.3.1 PBENG-U.07.03.01 Processor outside EU

If a controller or processor is not established in the Union, the controller or the processor shall designate in writing a representative in the Union, unless:

1. processing which is occasional, does not include, on a large scale, processing of special categories of data, or
2. processing of personal data relating to criminal convictions and offences and is unlikely to result in a risk to the rights and freedoms of natural persons, or
3. processor is a public authority or body.

PBENG-U.07.03.01.01 Explanation (1)
When determining the probability, consideration is given to the nature, the context, the scope and the processing purposes.

PBENG-U.07.03.01.02 Explanation (2)
The representative shall reside in one of the Member States where data subject are whose personal data are processed related to the offering of goods or services or whose conduct is observed.

PBENG-U.07.03.01.03 Explanation (3)
The representative is authorized by the controller or the processor to be approached besides or in his place.

PBENG-U.07.03.01.04 Explanation (4)
The appointment of a representative does not affect the ability of making claims against the controller or the processor.

4.7.3.2 PBENG-U.07.03.02 Safeguards measures by processor

Processing by a processor takes place only if a controller has sufficient guarantees about the application of appropriate technical and organizational measures, (see PBENG-B.03), by the processor.

4.7.3.3 PBENG-U.07.03.03 Prior data processing agreement

Prior to, a processor delegating processing activities to another processor, a specific or general written permission has to be given by the controller (see GDPR article 28 paragraph 1).

PBENG-U.07.03.03.01 Explanation (1)
In the case of general written consent, the processor shall inform the controller of any planned changes regarding the addition or replacement of other processors, giving the controller the opportunity to object to these changes.

4.7.4 PBENG-U.07.04 Exception ground

4.7.4.1 PBENG-U.07.04.01 Stop processing on judgement

Processing will not take place if there exists any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this regulation (see GDPR article 48).

PBENG-U.07.04.01.01 Explanation (1)
The term 'transfer to non-EU countries' refers to the communication of personal data to a person or organization that resides outside the jurisdiction of one of the countries of the Union. It involves:

a) the processing of personal data within a group context, if parts of a group are located inside and outside the EU; binding company regulations then apply.
b) the provision to third parties outside the EU;
c) making the data available to third parties outside the EU
d) the collection of data by countries outside the EU

4.7.4.2 PBENG-U.07.04.02 Limitation by law and regulations

The transfer may be restricted if the laws, regulations or provisions expressly set limits for important public data transfers to the transfer of specific categories of personal data to a third country or an international organization.

4.7.5 PBENG-U.07.05 Adequacy decision

4.7.5.1 PBENG-U.07.05.01 Condition processing outside EU (I)

A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection (see GDPR article 45).

PBENG-U.07.05.01.01 Explanation (1)
No specific permission is required for such a transfer

PBENG-U.07.05.01.02 Explanation (2)
Canada: parts of the country covered by the Canadian Personal Information Protection and Electronic Documents Act offer an appropriate level of protection. But beware: Québec, among others, is not included here, as a result of which the data may not be passed on to an organization in Québec unless there is one of the other grounds for lawful transfer to countries outside the EU.

PBENG-U.07.05.01.03 Explanation (3)
In the United States of America, only US-based organizations that have conformed to the EU-US Privacy Shield Convention have an appropriate level of protection. They must also have registered in the EU-US Privacy Shield register with the Federal Trade Commission and have also actively taken the necessary measures (The state of affairs surrounding the non-controversial Privacy Shield is more complicated than expressed here and also in motion. Pay attention, in this context, for example, to the Article 29 working group).

PBENG-U.07.05.01.04 Explanation (4)
The European Economic Area includes the countries of the EU, Norway, Liechtenstein and Iceland. Personal data may therefore be transferred to these countries.

4.7.6 PBENG-U.07.06 Appropriate guarantees

4.7.6.1 PBENG-U.07.06.01 Condition processing outside EU (II)

If no adequacy decision has been taken by the European Commission, appropriate safeguards are required so there (see GDPR article 46):

a) is legally binding and enforceable instrument between public authorities or bodies;
b) are binding company regulations that are approved by the AP (see PBENG-U.07.06.02);
c) are standard data protection provisions, laid down in the examination procedure referred to by the European Commission (see GDPR article 93 paragraph 2);
d) are standard data protection provisions approved by the AP, laid down in the examination procedure referred to by the European Commission (see GDPR article 93 paragraph 2);
e) is an approved code of conduct, together with binding and enforceable commitments by the controller or processor in the third country to apply the appropriate safeguards, including safeguards for the rights of data subjects;
f) is an approved certification mechanism, together with binding and enforceable commitments by the controller or processor in the third country, to apply the appropriate safeguards, including for the rights of the data subjects, or:
g) appropriate safeguards by the AP, with:

- contractual clauses between the controllers or the processor and the controller, the processor or the recipient of the personal data in the third country or international organization, or:
- provisions included in administrative arrangements between government bodies or bodies, including enforceable and effective rights of data subjects

PBENG-U.07.06.01.01 Explanation (1)
When guarantees can be provided, no specific permission from an AP is required for processing.

4.7.6.2 PBENG-U.07.06.02 Condition processing outside EU (III)

If binding company regulations (PBENG-U.07.05.01 point b) are used to provide appropriate guarantees, then:

a) are legally binding on, applicable to and enforced by all relevant members of the group, or the grouping of companies jointly carrying out an economic activity, including their employees;
b) data subjects may explicitly grant enforceable rights with regard to the processing of their personal data, and:
c) the elements summarized here have been documented (see for full view GDPR article 47 paragraph 1):
    1. the structure and contact details;
    2. the data transfers or set of transfers;
    3. their legally binding nature, both internally and externally;
    4. the application of the general data protection principles;
    5. the rights of data subjects;
    6. the acceptance by the controller or processor of all liability;
    7. how the information on the binding corporate rules is provided;
    8. the tasks of any data protection officer or any other person or entity in charge of the monitoring compliance with:
    9. the binding corporate rules within the group of undertakings, or group of enterprises engaged in a joint economic activity,
        a. training, and
        b. complaint-handling;
        c. the complaint procedures;
    10. the mechanisms within the group of undertakings, or group of enterprises engaged in a joint economic activity for ensuring the verification of compliance with the binding corporate rules;
    11. the mechanisms for reporting and recording changes to the rules and reporting those changes to the supervisory authority;
    12. the cooperation mechanism with the supervisory authority;
    13. the mechanisms for reporting to the competent supervisory authority any legal requirements, and:
    14. the appropriate data protection training to personnel having permanent or regular access to personal data.

4.7.6.3 PBENG-U.07.06.03 Unauthorized processing

If data processing should not have taken place, the controller had to terminate the data transfer and inform the AP and the data subjects (see GDPR article 49).

4.7.7 PBENG-U.07.07 Deviation for a specific situation

4.7.7.1 PBENG-U.07.07.01 Condition processing outside EU (IV)

Transfer of personal data can take place only on one of the following conditions:

a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request, unless this is done by a governmental authority for the purpose of a public authority;
c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person, unless this is done by a governmental authority for the purpose of a public authority;
d) the transfer is necessary for important reasons of public interest, that is recognized by the laws and regulations;
e) the transfer is necessary for the establishment, exercise or defence of legal claims;
f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;
g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down in Union or Member State law for consultation are fulfilled in the particular case;
h) the transfer is made to third countries or international organisations which were concluded by Member States prior to May 24, 2016, and which are in accordance with Union law applicable prior to that day, shall remain in force until amended, replaced or revoked (see GDPR article 96).


MEXON
TECHNOLOGY