Rijksoverheid

Model data protection impact assessment (PIA)

Quick and dirty translation by Utrecht University 2019

no rights can be derived from this file

Model privacy impact assessment (PIA)

Contact: Ministerie van BZK, directie Constitutionele Zaken en Wetgeving
Ministerie van VenJ, directie Wetgeving en Juridische Zaken

Versie: September 2017

Index

Introduction

This Document contains three components. The first component gives a general introduction on the instrument that is the Privacy Impact Assessment (PIA) and describes the process of carrying out a PIA. The second part encloses the model of carrying out a PIA, subsisting of 17 points. The third part provides an explanation on each of the 17 points of the model, detailed after a PIA of intended regulations and the data processing intended by the state (after: state processing).

This model is being used by the state.[1]Organisations can add to this model with elements that are specific to their organisation. By adding such elements, the instrument can be better tailored to the respectable organisational branch, which would make this instrument more usable.

[1] The notion of the state in this model will mean in any event: the state of the Kingdom of the Netherlands (core departments, agencies, supervision- and execution organisations). This definition does not include: independent governing bodies, defence, police, judiciary and decentralized governments. Some of these sectors, however, do make use of this Model Privacy Impact Assessment.

Part I - Process Framework

1 What is a PIA?

A PIA is an instrument to measure and assess the effects of intended regulations or projects that involve the processing of personal data. This instrument serves to map out the effects for data subjects in a standardized and structured manner, based on which measures can be taken to prevent or reduce these effects.

This model privacy impact assessment replaces the test model Privacy Impact Assessment Rijksdienst 2013.[2] This model is based on the new European regulation, the General Data Protection Regulation (GDPR),[3] the Directive Data Protection Investigation and Prosecution[4] (Directive) and national legislation. The guidelines of European privacy authorities are also involved in this model.[5] The model is aimed at the development of policy and regulation upon which processing of personal data are based as well as at the processing of personal data by or commissioned by the state. The model is meant for application on all policy areas and legal domains. This model PIA is included in the Integraal Afwegingskader beleid en regelgeving (IAK) en the Handboek portfoliomanagement Rijk.

The goal of a PIA is to take the protection of personal data into consideration when constructing policy. The instrument is a means to improve compliance of the privacy regulations.[6]
A PIA is *not* an instrument to determine whether an intended data processing is in line with the privacy regulations. The results of a PIA should, however, be kept in mind when determining appropriate measures that are to be taken to prove compliance with privacy legislation regarding the processing of personal data.

A PIA can relate to a single kind of data processing. A PIA can also see to a series of similar types of data processing that pose similar risks.[7] A PIA does not have to be limited to a single process, product or controller, for example when governmental bodies jointly decide to set up an application or processing environment.[8]

A completed PIA must contain the following:

A. a description of the characteristics of the data processing: a description of the intended processing and goals of processing;
B. an assessment concerning the lawfulness of the data processing: an assessment of the legal basis, the need, proportionality and compatibility of the intended processing in relation to the goals of processing;
C. a description and assessment of the involved risks for the data subjects: an assessment concerning the consequences and risks of the intended processing for the rights and freedoms of the data subjects; and
D. a description of intended measures: the intended measures to combat these consequences and risks of the intended data processing.[9]

[2] *Kamerstukken II* 2012/13, 26 643, nr. 282, herdruk 1.

[3] Regulation (EU) 679/2016 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (Algemene Verordening Gegevensbescherming) (PbEU 2016, L 119/1).

[4] Directive (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad.

[5] The 4 April Directive, WP 248.

[6] Consideration 84 GDPR.

[7] Article 35 (1), GDPR.

[8] Consideration 92 GDPR.

[9] Article 35 (7), GDPR and article 27 (2), Directive.

2 Why carry out a PIA?

By carrying out a PA, the protection of personal data becomes a structurally integrated part of the considerations and decision making of intended policy, regulation and (IT-)projects within the state. This improves the quality of the decision making.

In the first place, a PIA is directive. By following the model, relevant privacy risks that were not previously recognized can be brought to light. If that is the case, it is necessary to take these aspects into consideration. A PIA helps to identify and manage risks and to avoid unnecessary costs (in the sense that the problem does not have to be solved at a later stage).

A PIA is also correcting. During the process of carrying out a PIA, it can appear that it is necessary to reconsider previous choices, and subsequently choose for another (less impacting) solution to achieve the goal. It can thus appear that decisions made in an earlier stage can, in hindsight, not be sufficiently justifiable given the privacy risks involved. Given this directive and corrective character of a PIA, its execution can be a dynamic process, among which intended (policy) solutions or system designs can gradually be straightened out, aiming to reduce privacy risks for the data subjects.

The carrying out of a PIA can increase confidence in the intended measure, both within and outside of the organisation. The collecting of information to answer questions helps staff members and managers with the decision making and the accountability they carry. Carrying out a PIA stimulates the awareness of privacy.

3 In which cases is a PIA mandatory?

A PIA must be carried out:

1. with the development of policy and regulation related to the processing of personal data or from which data processing can result;
2. with intended processing of personal data which is likely to result in a high risk to the rights and freedoms of the data subjects. [10]

A PIA is, therefore, not always mandatory in the second situation for intended governmental processing, but only when the processing involves a high risk. The GDPR is directive in such cases.

A PIA for intended processing is in any event mandatory in the following cases:

a. a systematic and extensive evaluation of personal aspects which is based on automated processing, and on which decisions are based which produce legal effects or which similarly affect the data subjects significantly;
b. processing on a large scale of special categories of personal data or data relating to criminal convictions and offences on a grand scale;
c. systematic monitoring of a publicly accessible area on a large scale;
d. when the Autoriteit persoonsgegevens (the Dutch national supervisory authority) has established that a PIA is mandatory.[11]

[10] Article 35 (1), GDPR and article 27 (1), Directive.

[11] Article 35 (3) (4), GDPR and article 28 (3), Directive.

The European Privacy authorities have, in addition, put together criteria by which can be judged whether processing is likely to result in a high risk.[12] This is the case when there is processing involving:

1. evaluation or scoring of data subjects, including profiling and predicting;
2. automated-decision making with legal or similar significant effect;
3. systematic observation, monitoring or control;
4. the processing of special, criminal or otherwise sensitive personal data;
5. data processing on a large scale, considering the number of data subjects concerned, the volume of personal data, the duration and geographic extent of the processing activity;
6. datasets that have been matched or combined;
7. data considering vulnerable data subjects that, given the situation, may be unable to consent to, or oppose, the processing of their data, such as employees, children, the mentally ill, asylum seekers, the elderly and patients;
8. the use of new technologies;
9. data transfer across borders outside the European Union;
10. preventing data subjects from exercising a right or using a service or a contract.

The more criteria are met by the intended processing, the more likely it is to present a high risk to the rights and freedoms of data subjects. The authorities consider, as a rule of thumb, that processing operations meeting at least two of these criteria require a PIA.

If an intended data processing touches upon big political and social issues, a PIA will be desirable in any event.

A PIA is *not* mandatory in the following cases: [13]

a. the data processing is necessary for compliance with a legal obligation or for the performance of a task carried out in the public interest, and concerning the determining of the legal basis, a PIA has already been carried out.
b. When the Autoriteit persoonsgegevens has declared that a PIA does not have to be carried out.

According to the Autoriteit persoonsgegevens, there is also no need to carry out a PIA when the data processing is unlikely to result in a high privacy risk, or when the processing bears strong similarities to another data processing for which a PIA has already been carried out. Despite not being mandatory in the situation described under a, it can still be desirable to carry out a PIA, if in the execution further elaboration is being given on issues that on the current level of the regulation are not assessed, such as the choice for a certain IT-system and certain security measures.

If, contrary to the GDPR, no PIA has been carried out, or if a PIA has been carried out in an incorrect way, the Autoriteit persoonsgegevens can impose an administrative fine up to 10 million euros.[14]

Please contact the data protection officer with any questions regarding whether carrying out a PIA is desirable or mandatory.

4 How does a PIA compare to other instruments?

A PIA is being used alongside, and if necessary in coordination with, other instruments for the development of regulations and data processing by the government. Thus, a PIA does not replace any of the existing instruments.

[12] Guidelines from 4 April 2017, WP 248, p. 7-12.

[13] Article 35 (5) and (10) GDPR.

[14] Article 83 (4) (a) GDPR.

When concerned with intended policy and regulation, one may think of the instruments from the IAK, such as:

- the business impact assessment (BET);
- the feasibility and enforceability test; and
- review of proposed regulations against higher law, including constitutional law.

When it comes to governmental processing, one may think of the following normative frameworks:

- het Voorschrift Informatiebeveiliging Rijksdienst 2007 (VIR 2007);
- het Besluit voorschrift informatiebeveiliging rijksdienst – bijzondere informatie 2013 (VIRBI 2013); and
- de Baseline Informatiebeveiliging Rijksdienst 2012 (BIR 2012).

When it comes to informational security, the VIR 2007 states that for an information system measures must be taken based on a risk assessment, aimed at securing the information within the system adequately. The mentioned risk assessment would ideally be made in a risk analysis, in which the impact of the informational security loss regarding the business process (also referred to as: *business impact analysis* (BIA)) is determined.

In both the VIR 2007 and GDPR as well as the Directive, it is being stated that the controller has equipped a plan and control cycle to secure that the security always remains adequate regarding the current state of technology. [15] It is of importance to consider the requirements of privacy and informational security in conjunction. To comply with the applicable legislation, the responsible must view all relevant aspects as to ensure that the measures that are to be taken are adequate in the organisation considering the level of technology. For reasons of efficiency, it can be considered to carry out a BIA and a PIA simultaneously, as well as to determine the measures that are to be taken.

5 Who is responsible for carrying out a PIA?

Policy and regulation
The minister responsible for the policy and the possible regulation that results from it, is formally responsible for carrying out a PIA. In practice, this responsibility lies with the policy directorate.

Governmental processing
The controller is responsible for carrying out a PIA. Formally, the concerning minister is the respective controller for the data processing by a branch of governmental services. In practice, the competency to decide whether, and in what way personal data will be processed will be mandated, for example to a director-general or a director. The mandated official will then be responsible for carrying out a PIA.

In the event that multiple ministers are responsible for the processing of data, they must make sure amongst themselves that a PIA will be carried out.[16] In such a situation, it is reasonable that the minister who has taken the initiative regarding the development of the project (for example the manager for state-wide purchasing), also takes the initiative when it comes to drawing up the PIA.

If a part of government or an organisation outside of the government is the processor within the meaning of the GDPR – the entity that processes personal data on behalf of the controller– then that part or that organization is not responsible for the PIA. The processor is, however, obligated to assist the controller when requested. The involvement of the processor is often required to carry out the PIA.

[15] Article 25 GDPR and article 20 Directive.

[16] Conform article 26 GDPR and article 21 Directive.

6 When during the process must I carry out a PIA?

A PIA shall be carried out at an early stage of the policy development. At that stage, it is possible to be open minded about the effects of the policy and there is still ample opportunity to revise the baseline of the proposal without big negative consequences.
This also prevents later, costly adaptations in processes, redesigns of systems or even a complete halt to a project. This way, one would also be compliant with the obligation from the GDPR to keep data protection in mind while designing the project (*privacy by design*).[17]

A PIA can be carried out and/or updated multiple times and on multiple occasions.
When a proposal involving the processing of personal data changes, a (new) PIA should be carried out. In such an event, the changes should be judged in conjunction with the existing processing. If the data processing (for example when more personal data are being processed than previously) or its effects change, the PIA should be updated. The European privacy authority advices the good practice of evaluating a PIA every three years (see also point 9).

Policy and regulation
The PIA must, in any case, be carried out before any (internet) consultancy takes place. That way, the outcome of the PIA can be discussed through consultancy.

Governmental processing
The PIA must, in any event, precede the intended processing. In that way, the results of the PIA can be taken into consideration during the decision-making process regarding the intended processing.

7 How do I carry out a PIA?

The carrying out of a PIA covers the following steps.

1. Collect all relevant information about the intended regulation or the project that involves the processing of personal data.

2. Discus the points of the model, preferably in a group setting in which several relevant expertises are taking part. The involvement of multiple persons of different backgrounds and expertises on the area that is relevant to the intended policy – such as regulations, informational security and IT – results in a better PIA. When carrying out a PIA, a privacy expert should in any case be involved. Apart from employees working on the project concerned, it can also be desirable to involve an external party (not linked to the project) into the consideration. The ideal size and diversity of the group is dependent upon the nature and size of the intended data processing.

3. Write down the conclusions in a report.

4. Consult, where appropriate, the data subjects, organisations that represent them or other relevant parties.[18] For example branch organizations or interest organizations. Involving stakeholders enables the executors of the PIA to map out any concerns that might rise, as well as to be transparent about the personal data that will be processed and the reasons for that. If the personal data of staff is being processed, the department or company council should be involved.[19]

[17] Article 25 (1), GDPR and article 20 (1), Directive.
[18] Article 35 (9), GDPR.
[19] Article 27 (1) (k and l), Wet op de ondernemingsraden and het Besluit medezeggenschap Defensie 2008.

Record into the report what those who have been consulted have advised and what has been done with this advice. If no consultation has taken place, justify this decision in the report.

If the PIA is related to a proposed regulation, consultation of the stakeholders can coincide with existing consultation obligations. Conform the standard procedure for regulation, the advice about the proposal shall be collected at official advisory colleges and through internet consultation.

5. Submit the PIA-report to the data protection officer for advice. Include in the report what the data protection officer has advised and what has been done with this advice. The GDPR requires that advice is taken from the data protection officer.[20] The Directive simply points out the possibility but does not make it a requirement.[21] It can be wise to involve the data protection officer at an earlier stage of the PIA-process.

6. If the data processing is a part of the development of a new IT-system, the Chief Information Officer must be involved. The CIO tests the project plan on clarity concerning the processing of data and examines the reasoning regarding the desirability of carrying out a PIA. If a PIA is desirable, it will also be tested whether its execution has taken place and whether the measures have been included in the project. That is why the PIA should be made available to the CIO. If the PIA is being carried out in the context of policy development by which the development of IT-systems is being provided, the control measures should also be considered as described in the handbook portfoliomanagement Rijk voor projecten met een grote ICT-component.

7. When it turns out, from the PIA, that the processing by the government carries a high risk and the controller fails in taking measures that bring these risks back to an acceptable level, the Autoriteit persoonsgegevens must be consulted before the intended processing takes place.[22] If the PIA relates to regulation, the proposal must always be sent to the Autoriteit persoonsgegevens for consultation.[23]
Insofar as the intended processing falls within the scope of the Directive, the Autoriteit persoonsgegevens may draw up a list of types of processing that always require prior consultation.[24]

   According to the European privacy authority, the risk is unacceptably high if the data subject is being confronted with significant or irreversible consequences that he possibly cannot overcome or when the chance of this is considerably high.

   A period of eight weeks applies to the written advice from the Autoriteit Persoonsgegevens regarding the intended processing. This period can be extended by six weeks if the complexity of the intended processing warrants this.[25] Include in the report what the Autoriteit Persoonsgegevens has advised and what has been done with this advice.

8. Send the definitive PIA-report to all stakeholders concerned with the drafting of the PIA, unless rules concerning confidentiality or secrecy do not allow this.

[20] Article 35 (2), GDPR. See also Directives of 13 December 2016 (last edited on 5 April 2017), WP 243, p. 17.

[21] Article 34 (30), Directive.

[22] Article 36 (1), GDPR and article 28 (1), Directive.

[23] Article 36 (4), GDPR and article 28 (2), Directive.

[24] Article 28 (3), Directive.

[25] Article 36 (2), GDPR.

8 How do I justify the results of a PIA?

The results of a PIA are justified through a report according to the model in part II.

Policy and regulation

With regulation, the PIA-results are mentioned in the explanatory statement or note.[26] In those, a summary is given of the main considerations and choices in the PIA.
this paragraph may be added to the standard considerations regarding the compatibility with constitutional law and privacy legislation. Although a completely standardized accountability statement cannot be given, a template of this statement could be the following:

> *“Given the nature of this proposal, a data protection impact assessment was carried out in the policy development phase. Through this assessment, the necessity of the intended processing of personal data has been investigated and the consequences and risks of the data protection measure(s) / system have been mapped out in a structured way. Particular attention has been paid to the principles of transparency, data minimisation, purpose limitation, the requirement of good security and the rights of those involved. [Description of specific aspects and the balancing of interests made in this particular case]"*

In addition to the policy on the active publication of the execution and effects test, the results of the PIA must also be published – if it is referenced in the explanation of the proposal – on the publicly accessible wetgevingskalender. [27]

Government processing

The controller must maintain a register of data processing activities that take place under his responsibility.[28] The results of the PIA can be recorded in this register. In the context of transparency and an increase of support, it can be desirable to (partially) publish the results of the PIA, considering the frame of consideration given by the Wet openbaarheid van bestuur. For example, vulnerabilities in an IT-system do not have to be published.

[26] Indication 212 (a), designation for regulation.

[27] *Kamerstukken II* 2016/17, 33 009, nr. 39.

[28] Article 30 GDPR.

9 What must I do after the PIA is established?

After establishing the PIA, the controller must consider the results of the PIA when working on further developments of the intended regulation or project proposal.[29]

The controller assesses, if necessary, whether the processing will be executed corresponding to the PIA. He does that in any event when there is a change in the risk of the processing.[30] Risks may change because of changes in the parts of the processing (data, means, threats etc.), changes in context (goals, facilities etc.) or changes in the organisation or society.

Furthermore, the European privacy authorities recommend, as a good practice, to carry out a PIA once more every three years. The Autoriteit persoonsgegevens calls this a continuous process. The controller must keep monitoring whether the data processing changes and whether the PIA should therefore be updated.

[29] Consideration 84 GDPR.

[30] Article 35 (11), GDPR.

Part II - Model

A. Description characteristics data processing

Describe in a structured manner the intended data processing, the goals of the processing and the interests of the data processing.

1. Proposal

Generally, describe the proposal for which this PIA will be made and the context within which this takes place.

2. Personal data

List all categories of personal data that will be processed. Furthermore, list per category of personal data which data subjects are concerned. Divide these personal data amongst the following types: regular, special, criminal and legally identifying.

3. Data processing

Display all intended data processing.

4. Processing goals

Describe the goals of the intended processing.

5. Concerned parties

Name which organisations are concerned with which data processing. Divide these organisations per type of data processing in the following roles: controller, processor, provider and recipient. Also name which officials within these organisations will have access to what personal data.

6. Interests concerning data processing

Describe all interests which the controller and others have with the intended data processing.

7. Processing locations

Name in which countries the intended data processing will take place.

8. Techniques and methods of the data processing

Describe in which way and with the use of what (technical) means and methods the personal data will be processed. Indicate whether there is (semi-) automated decision making, profiling or big data processing involved and, if so, describe of which it consists.

9. Legal and policy framework

Name the applicable legislation, other than the GDPR and the Directive, and the policy with possible consequences for the intended data processing.

10. Retention periods

Determine and motivate the retention periods of the personal data considering the processing goals.

B. Assessment lawfulness of data processing

Assess the legal basis, necessity and purpose limitation of the intended data processing and the rights of the data subject.

11. Legal basis

Determine on which legal basis the data processing will take place.

12. Special personal data

If special or criminal personal data are being processed, assess whether one of the legal exceptions on the prohibition of processing applies. When processing legal identification numbers, determine whether this is allowed.

13. Purpose limitation

If the personal data are being processed for a purpose other than those for which the personal data were initially collected, assess whether this further processing is compatible with the purposes for which the personal data were initially collected.

14. Necessity and proportionality

Assess whether the intended data processing is necessary for the realization of the purposes of the processing. Consider in this regard in every case proportionality and subsidiarity.

a. Proportionality: is the invasion of privacy and the protection of personal data of the data subjects proportional to the processing purposes?

b. Subsidiarity: can the purposes of the processing not be achieved in another, to the data subjects less harmful way? State the considered alternatives.

15. Rights of the data subjects

Indicate how the data subjects can effectively make use of their rights. If the rights of the data subjects are infringed upon, determine on which legal basis that is allowed.

C. Describing and assessing risks for the data subjects

Describe and assess the risks of the intended data processing for the rights and freedoms of the data subjects. Consider the nature, scope, context and purposes of the intended data processing.

16. Risks

Describe and assess the risks of the intended data processing for the rights and freedoms of the data subjects. Elaborate in any case on:

a. which negative consequences the data processing can have for the rights and freedoms of the data subjects;

b. the origins of these consequences;

c. the likelihood (chance) that these consequences will occur;

d. the severity (impact) of these consequences for the data subjects if these occur.

D. Describing intended measures

Describe the intended measures to combat the previously described risks of the intended data processing for the freedoms and rights of the data subjects.

17. Measures

Assess which technical, organisational and legal measures can reasonably be taken to prevent or reduce the previously described risks. Describe which measure will combat which risk and which the risk will remain after implementing the measure. If the measure does not completely cover the risk, argue why the remaining risk is acceptable.

Part III - Explanation

This part of the PIA model provides an explanation on the model of part II. In this explanation, the relevant provisions of the privacy legislation will be elaborated upon. This explanation is not intended to server as a manual on privacy law.

Where relevant, in this explanation a distinction will be made between a PIA for intended regulation and a PIA for intended governmental processing. Regulation concerns: Acts of Parliament, algemene maatregelen van bestuur and ministeriële regelingen. Processing by the government concerns the processing of personal data by or commissioned by a part of the government. The object of a PIA may be: one or more products, services, processes or systems.

The model consists of 17 points spread over four parts. Part A is about the facts of the intended data processing. The legal assessment and facts are discussed in part B. Part C concerns the risks for the rights and freedoms of data subjects and part D is about intended measures to combat those risks. This outline derives from privacy regulations.[31] Carrying out a PIA is a dynamic process. One may imagine that after the assessment as described in part B, and after mapping out the risks in part C, measures may be proposed involving a modification of the intended data processing as described in part A, thus starting the process anew.

The answers to the 17 points in this model may be more or less detailed depending on the nature and scope of the intended regulation or processing by the government. In all cases, however, is it necessary to check all points of the model and to separately record all the considerations per point.

A. Describing characteristics of the data processing

The first step of a PIA is described under point A: a summary of all the relevant facts regarding the intended data processing. Some relevant facts might not be clear, and this may affect this assessment.

1. Proposal

Generally, describe the proposal for which this PIA will be made and the context within which this takes place.

To perform a PIA, it must be clear what topic or object it concerns. Through a short and concise description of the proposal for which the PIA is carried out, differing opinions regarding the 17 points can be avoided. For the sake of clarity, it can be useful to explicitly state what the PIA is *not* about.

Regarding **concept regulation**, one may seek for a connection with the explanatory statement when writing this description of the proposal, insofar as the processing of personal data are mentioned.

Regarding **governmental processing**, the data processing may be described generally in a summary. If that is available, a connection can be made with the project proposal or a description of the architecture.

[31] Article 35 (7), GDPR and article 27 (2), Directive.

2. Personal data

List all categories of personal data that will be processed. Furthermore, list per category of personal data which data subjects are concerned. Divide these personal data amongst the following types: regular, special, criminal and legally identifying.

Firstly, describe all categories of the personal data that are to be processed. The definition of personal data is: any information relating to an identified or identifiable natural person.[32] Natural person means a human. Information regarding deceased persons, legal entities, animals and objects falls, in principle, outside of the definition of personal data.[33] However, this information does qualify as personal data if the information also has bearing on a living person.

To determine whether someone is identifiable, account should be taken of all the means reasonably likely to be used to identify the person.[34]

Pseudonymized (also: encrypted) data are also considered personal data.[35] Pseudonymisation is understood as: 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 (keys), provided that such additional information is kept separately and is subject to measures to ensure that the personal data are not attributed to an identified or identifiable natural person.[36]

Anonymous and anonymized data are *not* personal data. In this context, anonymous and anonymized are used to indicate that the person to which the data relates is not or no longer identifiable.[37] The anonymizing of personal data is, however, considered a type of processing of personal data.

Examples of personal data are: name, prefix, address, phone number, e-mail address, age, date and place of birth, gender, place of residence, nationality, IP-address, MAC-address, KvK-number, vehicle identification number, profit (under certain conditions, such as in case of a one-man business), bank account number and account balance, IQ, job position, education, income and wealth data, solvency, personal preferences, wage scale, reports of performance interviews and (mis)behaviour. Metadata - information about information - can also be deemed personal data if one can deduce the identity of the data subject from this data. Examples of metadata are: which browser or phone someone uses, when a file was drafted or last edited as well as the written language. Information regarding location qualifies as personal data if traceable to a person. One may think of the possibility of combining data with other information accessible in public registers and monitoring the locations of vehicles.

Types

Subsequently, determine the nature of the categories of personal data that are to be processed. The GDPR distinguishes three types of personal data - regular, special and criminal - and sets different requirements for lawfully processing each type. The rationale behind this is that the more sensitive the nature of the data, the bigger the effects will be for the data subjects.

[32] Article 4 GDPR and Article 3 Directive.

[33] Consideration 27 GDPR.

[34] Consideration 26 GDPR and consideration 21 Directive.

[35] Consideration 26 Directive.

[36] Article 4 (5), GDPR and article 3 (5), Directive.

[37] Consideration 26 GDPR and consideration 21 Directive.

Special personal data

Below is an exhaustive list of categories of special personal data:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- genetic data;
- biometric data for the purpose of uniquely identifying a natural person;
- data concerning health;
- data concerning a natural person's sex life or sexual orientation.[38]

Examples of special personal data are: the address file of a church magazine, data processed via a pharmacist application, data regarding employees' illness and absenteeism, member list of a political party, relationship status on social media. Attention: sometimes imagery like photography or films can be special personal data, such as when ethnic origin or medical status can be derived from the imagery.

Genetic data

Genetic data are personal data relating to the inherited or acquired genetic characteristics of a person which provide unique information about his physiology or health and which result, in particular, from an analysis of a biological sample from the person in question.[39] Such as chromosomes, DNA or RNA and inheritable diseases.

Biometric data

Biometric data are personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a person, which allow or confirm the unique identification of that person.[40] Examples are: finger prints, iris pattern, facial profile, keystroke analysis, walking pattern, voice and sleeping pattern. Photographs are only considered biometrical data when processed through a specific technical means allowing the unique identification or authentication of a person.[41]

Data concerning health

Data concerning health are personal data related to the physical or mental health of a person.[42] Examples are: weight, heartbeat, handicaps, risk of falling ill or provided health services.

Criminal personal data

Personal data relating to criminal convictions and offences or related security measures (after: criminal personal data) are a separate type of personal data.[43] It includes both convictions as well as suspicions of offences. Examples of this are: an official report, decision to dismiss, criminal record, interrogation and a request for subsidized legal assistance in a criminal case.

[38] Article 9 (1), GDPR and article 10 Directive.

[39] Article 4(13), GDPR and article 3 (12), Directive.

[40] Article 4 (14), GDPR and article 3 (13), Directive.

[41] Consideration 51 GDPR.

[42] Article 4 (15), GDPR and article 3 (14), Directive.

[43] Article 10 GDPR.

Legal identification numbers

Identification numbers of a person that are prescribed by law, may only be processed for purposes determined by law. The thought behind this is that personal numbers highly facilitate the connection of different files regarding the same person, and thereby pose an additional threat to the data subject's privacy. Consider the following: a civil number (BSN), BIG-number (for professions in individual health care), A-number, education number, criminal justice number and licence plate number. This merely concerns person identification numbers that are prescribed by law.

Other personal data

All other personal data that do not qualify as special or criminal are regarded as regular personal data in this model. 'Regular', however, does not imply that there is no high privacy risk involved for the data subject. Certain personal data can carry a high privacy risk due to the context in which they are used. Examples of this are:

- data concerning the financial situation of the data subject;
- data concerning infringements of legal obligations, administrative and/or disciplinary measures or sanctions;
- (other) data that can result in stigmatization or exclusion of the data subject;
- data that is related to vulnerable groups;
- user names, passwords and other login credentials;
- data that can be abused for (identity) fraud;
- communication- and location data.[44]

Data subjects

Finally, list all categories of data subjects of whom personal data will be processed. Some examples are: employees, consumers, clients, patients, business contacts, visitors, users or citizens of a municipality. The scope and category of data subjects may influence the effects of the proposal. Certain data subjects are more vulnerable than others. Vulnerability is used to indicate that the negative effects of the (potentially unlawful) data processing can be bigger for some data subjects compared to others. Some examples are: minors, the mentally disabled, people who are being stalked or are staying in a women's shelter, employees of intelligence services, whistle-blowers or informers for the police and the justice department. Data subjects enjoy certain rights, deriving from privacy legislation, such as the right of access and the right to rectification.

The GDPR offers specific protection to children, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data.[45] This specific protection applies, in particular, 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. For example, the processing of data of a child below the age of 16 is only lawful if the parents or legal guardian has consented to this.[46] The age of the data subject also influences the way in which he must be informed.

[44] *Stcrt.* 2013, nr. 5174, p. 14.

[45] Consideration 38 GDPR.

[46] Article 8 (1), GDPR.

In the context of the Directive, the distinction can be made between:

a. persons against whom there are grounded suspicions regarding the committing of a criminal act or the intention to commit one;
b. persons who have been convicted for a criminal act;
c. victims of a criminal act, or persons against whom certain facts can raise suspicion that they might become the victim of a criminal act; and
d. other persons that have been involved with a criminal act, such as (potential) witnesses, persons who possess otherwise useful information for persecution or persons who are in contact or maintain ties with one of the persons meant under a and b.

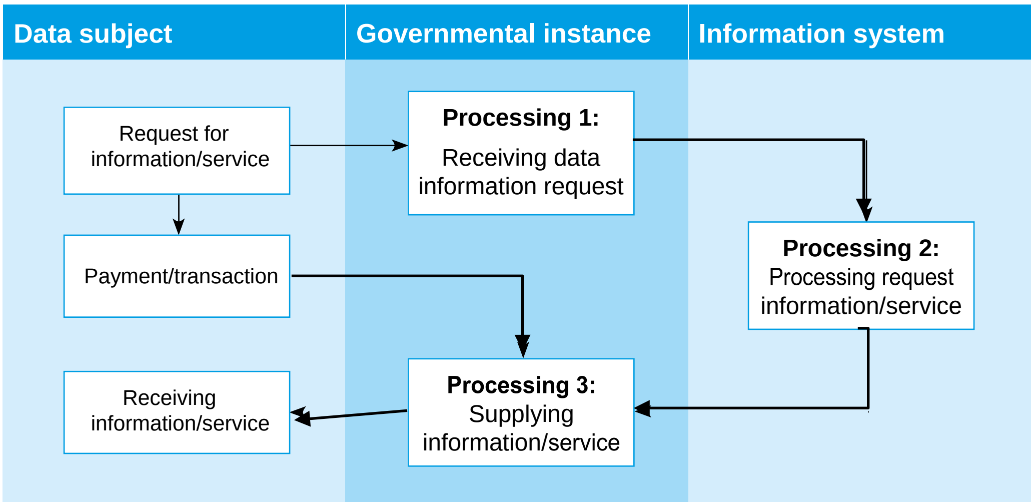
For **concept regulation**, it can be desirable to record the categories of personal data that are to be processed in the regulation. When the processing falls within the scope of the Directive, it is mandatory to list the categories of the personal data that are to be processed in the regulation.[47]

3. Data processing

List all intended data processing.

To assess the lawfulness of the intended data processing, it is necessary to visualize all types of data processing. Under processing, the following is to be understood: any operation or set of operations which is performed on personal data or on sets of personal data.[48] Some examples are: the collecting, recording, organising, structuring, storing, adaptating or alterating, retrieving, consulting, using, disclosing by transmission, disseminating or otherwise making available, alignment or combination, restricting, erasing or destruction of personal data. In other words, this concept encompasses the entirety of the process, from the moment of collection until the moment of destruction.

If possible, it is recommended to visualize the data processing, for example through an *input-process-output* model, *flowchart* or *workflow*.


Data subject
Governmental instance
Information system
Request for information/service
Processing 1:
Receiving data information request
Processing 2:
Processing request information/service
Payment/transaction
Processing 3:
Supplying information/service
Receiving information/service

[47] Article 8 (1), Directive.

[48] Article 4 (2), GDPR and article 3 (2), Directive.

4. Processing purposes

Describe the purposes of the intended data processing.

One of the principles of privacy regulation is that personal data may only be collected for well defined, explicitly described and justified purposes.[49] The determination of the processing purposes is a necessary requirement in order to assess whether the intended data processing can be lawful (point B) and to assess which measures have to be taken to reduce the risks, or even prevent these (point C and D). Therefore, it is important to describe the data processing purposes as specific as possible per type of processing.

Some examples of processing purposes are: security of buildings and objects, handling human resources, tracking down criminal acts, direct marketing, collecting claims, delivering orders, identification and authentication and handling disputes. Also consider possibly secondary purposes of the data processing, such as: scientific, statistical or historical research, maintaining an archive, declarations, reporting, improving services or development of policy. The purposes of processing must be specific according to the concrete data processing, while the general purpose serves as an umbrella overarching the several sub goals, such as:

- e-mail address: necessary to communicate with the data subject;
- IP address: necessary to verify that the system can only be contacted from determined locations;
- address data: necessary to send a decision to the data subject;
- financial data: necessary to determine whether the concerned party has the right to an allowance;
- criminal data: necessary to carry out a screening.

When personal data are not directly collected from the data subjects (in other words: the data are received from another source such as another person or organization, or an existing datafile), it is necessary to trace the purposes for which the data was initially collected. One of the principles of the privacy regulation is that data cannot be used for purposes that are not unifiable with the purpose for which it was originally collected. [50] In other words: the processing of personal data for other purposes than the one for which they were initially collected, is only allowed if the processing is compatible with the purposes for which the data was originally collected (for an assessment on this, see point 13 below). Further processing refers to the use of personal data that have previously been collected for a certain purpose. For example, when an organisation provides data to another organization, while at the time of collecting that data, further disclosure was not intended.

With **concept regulation**, the purpose of the data processing should be recorded, or at the very least, mentioned in the elaboration.[51] A legal description of the purposes improves legal certainty, because this results in a completion of the scope of assessment.

With **government processing**, the controller determines the purpose of the data processing. With government processing aimed at executing legislation, it is important to stay within the purpose that had been determined. It is preferred to determine the processing purposes as much as possible at the level of the work and organisation processes.

[49] Article5 (1) (b), GDPR and article 4 (1) (b), Directive.

[50] Article 5 (1) (b), GDPR and article 4 (1) (b), Directive.

[51] Article 6 (3), GDPR and article 8 (1), Directive. See also direction 162a Aanwijzingen voor de regelgeving.

5. Involved parties

List which organisations are involved in which kinds of data processing. Divide these organisations per kind of data processing in the following roles: controller, processor, provider and recipient. Furthermore, list the officials that will have access to which kinds of personal data.

To determine the lawfulness of the intended data processing, it must be clear which organisations are (functionally) involved in which data processing and in what capacity: controller, processor, provider or recipient.

The controller is the natural person, legal entity or governmental organ, that determines the purposes and means of the data processing.[52] In other words: the one that is formally entitled to decide whether the personal data are being processed, for what purposes these are being processed and in what way they are being processed. When two or more controllers jointly determine the purposes and means of the processing, they are both controllers, and must mutually record who is responsible and accountable for what.[53]

The processor is the natural person, legal entity or governmental organ that processes personal data on behalf of the controller. [54] The processor processes personal data for the controller, which means according to his instructions and under his responsibility. The processor is an entity outside of the controller's organization. The controller and processor must record in in writing who is responsible for what.[55] To determine who the controller and the processor are in a concrete situation, one must look, apart from the formal task distribution as the parties have agreed upon amongst themselves, at the circumstances as they factually are (why is the processing taking place? Who has initiated it?). That means that a mere written record of the task distribution does not meet the requirements: it is required that the controller has factual control over the purposes and means of the data processing.

The recipient is the natural person, legal entity or governmental organ to which the personal data are disclosed. [56] The provider is the natural person, legal entity or governmental organ that provides the personal data.

In the case of **concept regulation,** it can be desirable to record the capacity of the concerned organisations, or along which criteria their capacity is appointed. If a specific regulation concerning personal data is being drafted for the purpose of a public task, the controller must be mentioned in the regulation. In some cases, it may also be desirable to legally prescribe that some personal data shall only be available for certain officials, such as the prosecutor or company doctor.

[52] Article 4 (7), GDPR and article 3 (8), Directive.

[53] Article 26 (1), GDPR and article 21 (1), Directive.

[54] Article 4 (8), GDPR and article 3 (8), Directive.

[55] Article 28 (3), GDPR and article 22 (3), Directive.

[56] Article 4 (9), GDPR and article 3 (10), Directive.

When it comes to **governmental processing**, as far as it is not legally prescribed, the (functionally) concerned organisations must, in consultation amongst themselves, decide who will process what personal data and in what capacity. Furthermore, it needs to be determined, as far as there is no legal prescription, which officials within the organisation will have access to what personal data, for example based on an authorization matrix, in relation to the purposes of the data processing. In there, there is also an option to determine the conditions under which officials have access to the personal data.

6. Interests related to data processing

Describe all interests that the controller and others have with the intended data processing.

When assessing the lawfulness of the data processing, there can also be interests (such as the advantages) related to the data processing may play a role. This interest can take the form of private interests, interests of third parties or even the general interest. It is not about the possible negative consequences for the data subjects. For example: company interests, financial interests and commercial interests, maintaining legal claims, supervision on employees for the sake of safety or management purposes, (national) security such as the prevention of fraud, abuse and network security, and health.

The interest that is involved with the data processing will have an impact in the necessity test (points 11 and 14).

7. Processing locations

List in which countries the intended processing will take place.

The locations that the intended data processing can take place can carry privacy risks and are therefore subject to stricter rules and additional measures. The location will also have an influence on the competence of the local privacy authority.[57]

To safeguard that the rules regarding the protection of personal data will not be bypassed by processing the personal data in another country, the GDPR and Directive have decided that the processing of data outside of the European Union is only allowed under certain conditions.[58] This is the case, for example, when the European Commission has declared that the country has an adequate level of protection or appropriate safeguards (an adequacy decision)[59] or if there are fitting safeguards in place to protect the data subjects.[60] Besides that, there are some specific situations in which data processing in another country is allowed, despite the absence of a fitting safety level and fitting safeguards, such as explicit consent of the data subject.[61]

Apart from the GDPR and the Directive, other rules or policy can have an impact on the locations where personal data can be processed. For example, the VIRBI2013 regarding classified government information and situations in which storage in a government data centre is appropriate.

[57] Articles 55 and 56 GDPR, and article 45 Directive.

[58] Article 44 GDPR and article 35 (1), Directive.

[59] Article 45 GDPR and article 36 Directive.

[60] Article 46 GDPR and article 37 Directive.

[61] Article 49 GDPR and article 38 Directive.

8. Technique and method of data processing

Describe in what manner and using what (technical) means and methods the personal data will be processed. List whether there is any (semi-)automated decision making, profiling or big data processing and, if so, describe what it consists of.

Making use of certain techniques and methods for processing data can lead to additional privacy concerns with it, which is why they are subject to stricter rules and require additional measures. This is the case with, amongst others, with (semi-)automated decision making, profiling and bigdata processing.

Automated decision making

Decisions exclusively based on automated processing which have legal effects or similarly significantly affect the data subject, are in principle prohibited.[62]

For processing that fall within the scope of the GDPR, that prohibition does not apply if the decision:

a. is necessary for entering into, or performance of, a contract between the data subject and the 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.[63]

For processing that falls within the scope of the Directive, this prohibition does not apply if the decision:

a. is allowed by law; and
b. provides appropriate safeguards concerning the rights and freedoms of the data subjects, at least the right to obtain human intervention. [64]

Profiling

With profiling, the following is understood: any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. [65]

Certain data, such as the results of a search query in a search engine, can in combination with each other form a risk profile. The odds of certain profiles being created, rises when multiple registers are combined. There are risks of profiling when:

- based on a combination of personal data, such as car brand and age of the data subject, the decision is made to monitor this person more;
- data left behind by website visitors are used in order to determine the website's target audience.

Regarding processing that falls within the scope of the Directive, profiling resulting in discrimination based on special personal data is prohibited.[66]

[62] Article 22 (2), GDPR and article 11 (1), Directive.

[63] Article 22 (2), GDPR.

[64] Article 11 (1), Directive.

[65] Article 4 (4), GDPR and article 3 (4), Directive.

[66] Article 11(3), Directive.

Big data
Big data is not defined in the privacy regulation but is closely related to automated decision making and profiling. Big data represents/is used to describe the phenomenon that large amounts of structured and unstructured data from different sources are being analysed, through which automatically will be searched for correlations which can result in knowledge to apply to decisions in the group or individual level.[67] At the core, big data is a search for correlation, as opposed to causality. Applying big data brings specific risks and therefore requires specific measures (point D).

New technologies
Big changes in the way that personal data are being processed and the technology that is being applied there can have an impact for the data subjects. Consider the following examples: intelligent tracking systems based on GPS, biometrics and new forms of identification.

9. Legal frame and policy

List the legislation, other than the GDPR and Directive, and the policy with possible consequences for the data processing.

Apart from the GDPR and the Directive, there can be (sector) regulation that creates, conditions or limits possibilities for data processing. Examples of such laws are: Wet algemene bepalingen burgerservicenummer, Wet gebruik burgerservicenummer in de zorg, Wet basisregistratie personen, Algemene wet inzake rijksbelastingen, Archiefwet, Telecommunicatiewet, Kadasterwet, Handelsregisterwet 2007, Kieswet, Wet bijzondere maatregelen grootsstedelijke problematiek, Wet op de geneeskundige behandelingsovereenkomst, Omgevingswet, Jeugdwet, Wet maatschappelijke ondersteuning 2015 en Participatiewet. This list is not exhaustive.

There can also be departmental or state-wide policy that conditions or limits the possibilities for intended data processing, for example regarding the storing and security of personal data.

From this assessment, it can be determined whether the intended data processing is lawful (point B) and whether there are specific measures prescribed (point D).

10. Retention periods

Determine and justify the retention periods of the personal data considering the purposes of processing.

The privacy regulation states as principle that personal data may not be kept in a that enables the identification of the data subject for longer than is necessary.[68] In other words: if the personal data are no longer needed for the realization of processing purposes, it must be destroyed or anonymized. There is one exception to this principle of storage limitation: if the personal data are being exclusively processed for the sake of archiving in the general interest, scientific or historical research or statistical purposes. This does require that appropriate measures are taken to protect the data subjects.[69]

[67] Wetenschappelijk Raad voor het Regeringsbeleid (WRR), Big data in een vrije en veilige samenleving, rapport nr. 95, p. 21.

[68] Article 5 (1) (e), GDPR and article 4 (1) (e), Directive.

[69] Article 89 GDPR and article 4 (3), Directive.

With **governmental processing**, it must be verified whether the law prescribes a retention period. If that is the case, the controller must adhere to this period. If no retention period is prescribed, the processor must determine a retention period himself or periodically test the data against the principles of storage limitation.[70] When determining this, one must keep in mind any other regulation regarding retention periods, such as the Archiefwet 1995.

Example of a retention period for personal data:

Category Personal data	**Start retention period**	**Retention period**	**Motivation for storing**	**Responsible entity for removing**
Name	The moment the data subject logs into the system for the first time.	365 days, if the user checks 'remember login credentials' 30 days.	These personal data are functional: the data makes it so that you can log into several databases with only one act.	Functional manager

B. Assessing lawfulness of the data processing

Assess, based on the fact as determined in part A whether the intended data processing is lawful.[71]
In this case, it is about assessing the legal basis, necessity and purpose limitation of the data processing. Also assess the way in which the rights of the data subjects are given substance. For this part of the PIA, special legal expertise is required.

11. Legal basis

Determine on which legal basis the data processing takes place.

One of the principles of the GDPR is that personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.[72] As an elaboration on this, data processing is only lawful if it can be based on at least one of the following six legal bases:

a. the data subject has given consent to the processing of his 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 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;

[70] Consideration 39 GDPR and consideration 26 Directive.

[71] Article 6 GDPR and article 8 Directive.

[72] Article 5 (1) (a), GDPR.

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.[73]

Whether the data processing is necessary, will be determined in point 14.

With regard to legal basis c (legal obligation) and e (public interest): these legal bases must be determined by law.[74] The legal obligation (legal basis c) does not necessarily have to consist of an explicit obligation to process personal data. It is also possible that the processing of personal data finds a basis in a more broadly formulated duty of care or legal obligation. Without processing personal data, the execution of a legal obligation must be reasonably impossible. Concerning legal basis e (public interest), this task will have to be apparent from laws that are applicable on the controller. It is not necessary, however, that the law explicitly states that processing personal data must be processed to attain the purpose of the law. If processing personal data is necessary for the performance of a public task, then the legal basis for the public task can also be regarded as the legal basis for processing personal data.

The Data Protection Investigation and Prosecution Directive for Data Processing by Qualified Authorities concerning appearing in court, the investigation or the persecution of illegal acts, including the protection against, and the prevention of dangers for public safety makes sure that data processing is only legal if this is based on the law.[75]

With regard to **concept regulation**, the controller will often be able to base the data processing on legal basis c (legal obligation). This is the case when the data processing is necessary to carry out the legal obligations and when the controller is charged with carrying out the legal obligation. Regulation can also have the effect that a governmental body can base its data processing on legal basis e (public interest). The public tasks are established by law, alongside the accompanied necessary data processing for this purpose. It is also possible that regulation prescribes that consent will be required and hereby excludes all other legal bases.

With regard to **governmental processing**, the governmental organ will have to base its data processing on one of the six legal bases. The legal basis f does not apply to data processing concerning the performance of public tasks. This basis can, however, be used for data processing in business operations, such as camera surveillance, visitor registration and access control. In many situations, the legal basis a will be unusable for governmental organs, as this legal basis requires consent to be given freely, which is not the case in such a situation.[76]

[73] Article 6 (1), GDPR.

[74] Article 6 (3), GDPR.

[75] Article 8 (1), Directive.

[76] Article 4 (11), GDPR and consideration 43 GDPR.

If the data processing is based on legal basis f (legitimate interests of the controller or a third party), the GDPR requires that the interests or fundamental rights and freedoms of the data subject override the legitimate interests of the controller or third party.

12. Special personal data

If special or criminal personal data are being processed, assess whether one of the legal exceptions to the processing prohibition is applicable. When processing a legal identification number, assess whether this is allowed.

The GDPR bans the processing of special personal data. To this processing ban, the following exceptions are applicable:

a. the data subject has given explicit consent;
b. the 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;
c. processing is necessary to protect the vital interests of the data subject or another natural person;
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;
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 or the management of health or social care systems and services;
i. processing is necessary for reasons of public interest in the area of public health;
j. processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.[77]

Further exceptions can be found in national regulation.

Furthermore, the GDPR determines that processing of criminal data is only allowed by or under the control of the government or if it is regulated by law (for a definition on criminal data, see the elaboration on point 2).[78]

The processing of national identification numbers is only allowed for carrying out a legal obligation or for purposes determined by law. Governmental bodies can use citizen service numbers while carrying out their public tasks, without the requirement of any additional regulation.[79]

The Directive prescribes that the processing of special personal data is only allowed when the processing is strictly necessary, taking into consideration appropriate safeguards for the rights and freedoms of data subjects, and:

a. is legally allowed;
b. is necessary to protect the vital interests of the data subject or another natural person; or
c. the processing concerns data that has manifestly been made public by the data subject himself.[80]

[77] Article 9 (2), GDPR.

[78] Article 10 GDPR.

[79] Article 10 Wet algemene bepalingen burgerservicenummer.

[80] Article 10 Directive.

With regard to **concept regulation**, deviation from the processing ban is possible, provided that appropriate safeguards are being offered to protect personal data and other constitutional rights of the data subject.[81]

13. Purpose limitation

If the personal data are being processed for a purpose other than those for which the personal data were initially collected, assess whether this further processing is compatible with the purposes for which the personal data were initially collected.

One of the principles in the GDPR is that personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.[82]

The GDPR states that further processing for another purpose is allowed if the further processing is based on consent given by the data subject or on a specific legal prescription, which constitutes a necessary and proportionate measure in a democratic society to safeguard an important objective of the general interest, such as national security, public safety, monetary, budget or fiscal matters.[83] Other than that, the further processing for archiving in the general interest, scientific or historical research or statistical purposes are considered compatible with the original purposes. Sometimes, this requires that appropriate measures shall be taken to protect the data subject. [84]

When concerning **concept regulation**, it must be assessed whether it is it necessary to legally allow further processing (see also point 14), for example concerning the breach of confidentiality.

Within the framework for processing for another purposes outlined above there exists space for a regulation by law based on which sets of personal data of multiple parties from multiple domains can be combined for the sake of big data analysis, by which data will be processed for a purpose described in that law, that is not the purpose for which the data was originally collected, but is compatible with it. This is without prejudice regarding the analysis that the controller must conduct which has to meet all the requirements concerning the lawfulness of processing. Such processing does require a legal basis on its own (see point 11).

When concerning **governmental processing**, the controller himself must assess whether the further processing of personal data is allowed and compatible based on:

a. any link between the purposes for which the personal data was collected and the purposes of the intended further processing;
b. the context in which the personal data were collected, in particular regarding the relationship between the data subject and the controller;
c. the nature of the personal data, in particular special or criminal personal data;
d. the possible consequences of the intended further processing for the data subject;
e. the existence of appropriate safeguards.[85]

The Directive allows further processing of personal data for purposes that fall within the scope of the Directive, not being the one for which the data was originally collected, provided that:

[81] Consideration 52 GDPR and consideration 37 Directive.

[82] Article 5 (1) (b), GDPR and article 4 (1) (b), Directive.

[83] Article 6 (4), GDPR in conjunction with article 23 (1), GDPR.

[84] Article 89 GDPR.

[85] Article 6 (4), GDPR.

a. the controller is authorized by law to use these personal data for such a purpose; and
b. the processing is necessary and is proportional to that other purpose.[86]

The further processing for other purposes is only allowed if there is a legal basis given by law. The GDPR is applicable when personal data are being used for such other purposes. [87]

14. Necessity and proportionality

Assess whether the intended processing is necessary for the realization of the processing purposes. Consider at least the proportionality and subsidiarity.

a. Proportionality: is the infringement on the privacy and protection of personal data of the data subject is proportional to the processing purposes?
b. Subsidiarity: can the purposes of the processing not be achieved in another, to the data subjects less harmful way?

Another principle of the GDPR is that all data processing shall be limited to what is necessary for the processing purposes. This principle of minimal data processing/data minimisation is further expressed by the use of the word “necessary” in article 6 GDPR and article 8 of the Directive. The GDPR and Directive require that the data processing is necessary for the realization of the purposes. Therefore, the data processing must meet the subsidiarity and proportionality requirements.

Proportionality entails that the infringement of the intended data processing must be in proportion to the purpose of this processing. When it comes to proportionality, one must weigh whether the realization of the processing purposes has such weight that, considering the infringements upon privacy, the data processing is justified (are the infringements on the rights of the data subject and the goal of the intended processing balanced?). In this proportionality test, one should assess whether or not the intended data processing is an effective means to realize the purposes of the processing, as well as whether the arguments brought forward are relevant and sufficient. Empirical research results can help in that regard.

Subsidiarity entails that there are no less invasive means to realize the processing purposes. Examples are:

- when using special or criminal personal data, can the same result be achieved by using combinations of regular personal data?
- can the processing of personal data be limited, or can the same goal be achieved with less processing?

For example: in some cases, photographs can be used for the same purpose (e.g. identification) as the processing of videos. Subsidiarity also entails that if personal data will be made public, not all personal data are automatically made public, but a selection will be made based on justified criteria. During such a consideration, the purposes, interests and facts should be brought into the picture like in part A.

15. Rights of the data subject

Indicate how the rights of the data subject will be implemented. If the rights of the data subject will be limited, determine based on which legal exception that is allowed.

[86] Article 4 (2), Directive.

[87] Article 9 (1), Directive.

Data subjects enjoy several rights based upon the privacy regulation, which also describe in what way and under which circumstances they can exercise these rights.[88] These rights are the right to information, right of access, right to rectification, right to erasure, right to restriction of processing, notification obligation regarding rectification or erasure of personal data or restriction of processing, right to data portability, right to object and the right to not be subject to a decision based solely on automated processing. There are possible exceptions to the exercising of these rights, provided that such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure to safeguard some explicitly listed important objectives of general interest.[89] Exceptions must always be based on a national law and directly allowed based on European privacy regulations.

If an exception is being made on the rights of the data subjects in **concept regulation**, it must be assessed whether this is allowed based on grounds listed in the privacy regulation and, additionally, specific statements must be recorded containing at least the following:

a. the processing purposes;
b. the categories of personal data;
c. the scope of application of the implemented restrictions;
d. the safeguards to prevent abuse or unlawful access or disclosure;
e. the specification of the controller or categories of controllers;
f. the retention periods and applicable safeguards;
g. the risks for the rights and freedoms of data subjects;
h. the right of data subjects to be informed of the restriction, unless this detracts of the purpose of the restriction.[90]

With regard to **governmental processing**, address how the rights of data subjects will be incorporated, for example the way in which the data subject will be informed and how a request to erasure or correction of data will be handled. If the controller wishes to make exceptions to the exercising of certain rights of data subjects, he must argue why that is necessary and on what basis that is allowed.

C. Describing and assessing the risks for the data subjects

Describe and assess the risks the intended data processing brings about for the rights and freedoms of the data subject. Consider the nature, scope, context and purposes of the data processing as described and assessed in part A and B. This assessment does not concern the risks for the controller.

16. Risks

Describe and assess the risks of the intended data processing for the rights and freedoms of the data subjects. Elaborate in any case on:

a. which negative consequences the data processing can have on the rights and freedoms of the data subjects;
b. the origins of these consequences;
c. the likelihood (chance) that these consequences will occur;
d. the severity (impact) of these consequences for the data subjects if these occur.

[88] Chapter III (articles 12-22) GDPR and Chapter III (articles 12-18) Directive.

[89] Article 23 GDPR, article 13 (3), 15 and 16 (4), Directive.

[90] Article 23 (2), GDPR.

According to privacy regulation, a PIA is supposed to contain the assessment of the risks for the rights and freedoms of the data subject.[91] Based on the nature, the scope of application, the context and the purposes of the data processing, the likelihood and severity of the risk for the rights and freedoms of the data subjects must be determined. Based on an objective assessment, the risk level of the data processing can be determined.[92] It is required to evaluate the origin, the nature, the specific character and the severity of that risk. [93]

It is all about a risk centred approach that can consist of the following steps:

1. identifying risks;
2. estimating/analysing risks;
3. assessing/evaluating risks.

This approach will be broadly comparable with the risk evaluation concerning informational security.[94] That is why information that has come out of this analysis can be used here. Different from this risk evaluation, which is aimed at reliability requirements for information systems, and the risks it carries for the responsible party (such as adjustment, trustworthiness, publicity, supervision and enforcement, services, reliable information), the PIA is more geared toward the risks for the data subjects.

The privacy regulation does not prescribe in what manner the risk assessment is to be carried out. It is advisable to join in on international standards, such as the International Organization of standardization (ISO), Eenduidige Normatiek Single Information Audit (ENSIA) and Organisation for Economic Co-operation and Development (OECD).

1. Identifying risks

The first step is to determine any potential privacy risks. A privacy risk is a chance of a negative effect for the rights and freedoms of the data subjects to take effect as a consequence of processing of personal data.

When thinking of rights and freedoms of the data subjects, one must primarily think of the right to privacy, but also of other fundamental rights and freedoms, such as the freedom of expression, the freedom of religion, and the prohibition of discrimination. The occurrence of the (hypothetical) situation can lead to physical, material or non-material damage for the data subject. Some examples of these situations are:

- when data processing can give rise to:
  - discrimination, stigmatization and exclusion;
  - (exposure to) identity theft or fraud;
  - financial losses;
  - reputation or relational damage;
  - loss of confidentiality of personal data protected by professional secrecy;
  - unauthorized reversal of pseudonymization;
  - or any other significant economic or social disadvantage for the natural person in question;
- when data subjects might be deprived of their rights and freedoms or are prevented from exercising control over their personal data;
- when special or criminal personal data are processed;

[91] Article 35 (7) and 7 (c), GDPR and article 27 Directive.

[92] Consideration 76 GDPR.

[93] Consideration 84 GDPR.

[94] Article 4 and article 4 (a), Besluit voorschrift informatiebeveiliging rijksdienst 2007.

- when 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;
- when personal data of vulnerable persons, such as children, is processed; or
- when processing involves a large amount of personal data and affects a large number of data subjects.[95]

2. Estimating risks

Subsequently, the listed risks must be qualified by estimating the chance that a threat will occur and the possible consequences of this for the data subjects. In other words: wat are the feared consequences and how big will the impact be on the data subjects? How will these threats manifest and how likely is it that they will? These questions are not aimed at getting black and white answers, but rather a consideration based on which a level of risk can be determined.

The impact/severity of the risks depends on the context of the processing: the nature of the personal data, the nature of the processing and the purposes for which the data is processed.

The chance that risks will manifest also depends on the means that the controller uses for the data processing, as well as the nature of the personal data. Personal data which form a key to access monetary means or with which the data subject can be blackmailed, are attractive for hackers. Some examples of this are login details for DigiD or a dating website.

The chance that the consequences for the rights and freedoms of the data subjects will occur can also be related to the (level of) security of the personal data. Consider the intentional or unintentional:

- destruction and loss (availability);
- modification (integrity);
- unauthorized access and disclosure (confidentiality);

of personal data, that can lead to damages for the data subject.[96]

When assessing risks, it can be useful to consult data subjects or their representatives.

Processing big data can lead to specific risks for the data subject. For example: an algorithm can discover a correlation that may be logical in a statistical sense, but can lead to prejudices and stereotyping, discrimination and social exclusion or otherwise impact the data subjects, such as during job interviews, taking a loan or taking out an insurance. Furthermore, there is a risk that the data subject is subject to big data decision making which he does not comprehend and cannot influence.

3. Assessing risks

Define acceptable risk values and assess whether the risks are acceptable.

D. Describing intended measures

In part D, the measures to prevent or reduce the risks recognized in part C are evaluated. Which measures can reasonably be taken is a balancing act for the controller. For this part of the PIA, when it concerns security measures, expertise on information security is important.

[95] Consideration 75 and 85 GDPR and consideration 51 Directive.

[96] Consideration 83 GDPR and consideration 60 Directive.

17. Measures

Assess which technical, organisational and legal measures reasonably can be taken to prevent or reduce the risks previously described. Describe which measure combats what risk and what the remaining risk will be after the measure is implemented. If the measure does not fully prevent the risk, argue why the remaining risk is acceptable.

When thinking of measures that can be taken, consider the following examples: extra information for the data subjects, periodical checks, more supervision, increasing risk- and privacy-awareness and data minimisation.

Measures can also be security measures. One of the principles of the GDPR is that personal data must be protected in such a manner to prevent unauthorized or unlawful processing as well as accidental loss, destruction or damage, using appropriate technical or organizational measures.[97]

The controller must take appropriate technical, organizational and security measures in order to safeguard a level of security adapted to the risk.[98] In this context, appropriate means that the security must be according to the state of the art. Appropriate also means that the measures must be proportional to the privacy risks involved. The bigger the risks, the heaver the requirements will be with regard to the security of the personal data. There is no obligation to have the toughest security at all times. It is only required for the measures to be reasonable considering the available technology and costs of implementation.[99] These measures must bring the risks back to an acceptable level. Reducing security risks to nothing is impossible. This means that there will always be a remaining risk. The controller has to describe how he decided the level of the remaining risk and why it is deemed acceptable.

An appropriate level of security supposes that there is a planning- and control cycle (plan-do-check-act) by which can be determined whether the security level remains adequate given the current state of technique and the organization.

For measures to be taken, one can adhere to security scopes and standards, best practises and approved codes of conduct and certification mechanisms.

For instance, the GDPR lists the following examples:

a. the pseudonymization and encryption of personal data;
b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing system and services;
c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.[100]

[97] Article 5 (1) and article 5 (1) (f), GDPR and article 4 (1) (f), Directive.

[98] Article 32 GDPR and article 29 Directive.

[99] Consideration 83 and 94 GDPR.

[100] Article 32 (1), GDPR.

Other than those mentioned above, one may think of the following measures, which are also meant to ensure that personal data, considering the purposes for which they are being processed, are correct and accurate[101]:

- physical measures for access security and logical access control;
- storage of data in a safe;
- project-, risk- and incident management;
- splitting data;
- data minimisation;
- back-ups;
- integrity controls;
- multifactor authentication;
- monitoring and logging;
- controlling granted authorizations;
- privacy awareness and security trainings;
- management reports about risk management;
- limiting inspection level;
- periodically carrying out an audit, hack or penetration test;
- guidelines regarding the use of IT tools, such as encrypted storage places;
- responsible disclosure policy;
- confidentiality statements;
- service level agreements (with penalty clauses);
- processing agreements;
- screening of staff and a Certificate of Conduct (VOG-verklaring).

Finally, the Directive lists the following measures:

a. control access to equipment;
b. controlling data carriers;
c. storage control;
d. user control;
e. controlling access to data;
f. controlling transmissions;
g. input control;
h. transport control; and
i. recovery options.[102]

The Directive requires the keeping of log files of certain forms of processing, as to trace back the reason, date and time of an act as well as, if possible, the identity of the person who consulted or disclosed personal data, and the identity of the recipients of that personal data.[103]

With regard to **concept regulation**: also, at this regulatory level, measures can be taken. Consider implementing a maximum retention period, limiting access to and decisions about personal data to certain officials or confidentiality clauses.

[101] Article 5 (1) (d), GDPR and article 4 (1) (d), Directive.

[102] Article 29 (2), Directive.

[103] Article 25 (1), Directive.

Big Data

When working with Big data analyses (point 8) which involves the processing of personal data, one must be mindful of the risks involved. Particular attention should be paid to the following measures.

- Make sure that experts are involved when the possibility of pattern recognition when applying big data is less likely. This to reduce the chance of wrong outcomes to a minimum.
- Make sure, with as much effort as can reasonably be expected, that the data are up to date, the datasets contain as little bias as possible and the algorithms and analysis methods are sound.
- Determine, considering the potential impact of the application, the acceptable margin of error for the application.
- Make sure that useful information about the kind of logic used in the analysis reaches the data subjects, as well as that supervision and judicial review can be given sufficient insight in the algorithms and analysis methods in use.[104]

When applying the results of big data analyses, attention should be paid to implementing the following measures.

- Ensure that there is human intervention in the process of automated decision making.[105]
- The bigger the potential negative impact for the data subject, the bigger the need for a good validation and consideration of the results.

[104] Kamerstukken II 2016/17, 26 643, nr. 426, p. 7-10.

[105] Article 22 GDPR.

Deze brochure is een uitgave van:

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Turfmarkt 147
2511 dp Den Haag
Postbus 20011
2500 ea Den Haag

September 2017 | 105172