Model
Data Protection Impact Assessment (DPIA)
Contents

Introduction ........................................................................................................................................... 3

Part 1 .................................................................................................................................................. 4
1 What is a DPIA? .................................................................................................................................. 4
2 Why carry out a DPIA? ....................................................................................................................... 4
3 In which cases is a DPIA mandatory? ............................................................................................... 5
4 How does a DPIA relate to other instruments? ................................................................................. 6
5 Who is responsible for carrying out a DPIA? ..................................................................................... 7
6 At what stage in the process do I need to carry out a DPIA? .............................................................. 7
7 How do I carry out a DPIA? .............................................................................................................. 8
8 How do I account for the outcome of a DPIA? ................................................................................... 9
9 What should I do after the DPIA has been adopted? ...................................................................... 9

Part 2 .................................................................................................................................................. 10
1. Proposal .......................................................................................................................................... 10
2. Personal Data ................................................................................................................................... 10
3. Data Processing ............................................................................................................................... 10
4. Processing Purposes ....................................................................................................................... 10
5. Parties Involved ............................................................................................................................. 10
6. Interests in Data Processing ........................................................................................................... 10
7. Processing Locations ....................................................................................................................... 10
8. Techniques and Methods of Data Processing Operations ............................................................... 10
9. Legal and Policy-related Framework ............................................................................................. 11
10. Retention Periods ........................................................................................................................ 11
11. Legal Basis ..................................................................................................................................... 11
12. Special Categories of Personal Data ............................................................................................. 11
13. Purpose Limitation ........................................................................................................................ 11
14. Necessity and Proportionality ....................................................................................................... 11
15. Rights of the Data Subjects ......................................................................................................... 11
16. Risks .............................................................................................................................................. 12
17. Measures ....................................................................................................................................... 12
Introduction

This document consists of two parts. The first part provides a general introduction to the Data Protection Impact Assessment (DPIA) instrument and describes the process of carrying out a DPIA. The second part contains the model for carrying out a DPIA, consisting of 17 points.

Part 1 describes, among other things, whether or not a DPIA is mandatory. This can be considered a pre-DPIA. The following questions can be used to determine whether a DPIA is necessary:

1. Is it a systematic and comprehensive assessment of personal aspects, based on automated processing, and on which decisions are based which produce legal effects or which affect data subjects substantially in a similar way?
2. Is there large-scale processing of special categories of personal data or of data relating to criminal convictions and punishable offenses?
3. Is there systematic and large-scale monitoring of publicly accessible areas?
4. Has the Dutch Data Protection Authority deemed a DPIA mandatory in this case?

In addition to this, the European privacy authorities have drawn up criteria on the basis of which it can be assessed whether there is a high risk. This is described in Section 3 of Part 1.
Part 1

1 What is a DPIA?
A DPIA is an instrument for the structured and standardized identification and assessment of the effects for data subjects of proposed regulations or projects involving the processing of personal data. Based on this, measures are taken to prevent or reduce these effects for the data subjects.

This university Data Protection Impact Assessment (DPIA) model is based on the new European legislation, the General Data Protection Regulation (GDPR) and the national regulations based on this regulation. In this model, the guidelines of the European privacy authorities are also involved. The model is aimed at the processing of personal data by or on behalf of (a unit of) the university.

The purpose of a DPIA is to make the protection of personal data part of the assessment process when formulating policy and developing a data processing operation. The instrument is a means to improve compliance with privacy regulations. A DPIA is not an instrument to determine whether a proposed data processing operation is in line with privacy regulations (compliance). However, the results of a DPIA should be taken into account when determining the appropriate measures to be taken in order to demonstrate compliance with privacy regulations when processing personal data.

A DPIA may cover a single type of data processing. A DPIA may also cover a range of similar operations presenting similar risks. Thus, a DPIA does not need to be limited to a single process, product, or controller, for example, when universities want to set up a joint application or processing environment.

A completed DPIA consists of:
A. a description of the proposed processing operations and the processing purposes;
B. an assessment of the legal basis, necessity, proportionality, and compatibility of the proposed processing operations in relation to the processing purposes;
C. an assessment of the impact and risks of the intended processing regarding the rights and freedoms of the data subjects; and
D. the measures proposed to deal with these consequences and risks of the proposed processing operations.

2 Why carry out a DPIA?
By carrying out a DPIA, the protection of personal data becomes part of the weighing up of interests and decision making of proposed policy, regulations, and (ICT) projects within the university in a structured manner. This increases the quality of the decision-making process.

A DPIA first and foremost serves as a guide. By following the model, relevant privacy risks that were not recognized earlier in the development can come to light. If that is the case, it is necessary to include these aspects in the preparations. In this way, a
DPIA helps to identify and control risks and avoid unnecessary costs (in the sense that problems would have to be solved at a later stage).

A DPIA is also a corrective measure. Whilst carrying out the DPIA, it may become apparent that it is necessary to reconsider previous choices and then choose another (less intrusive) solution in order to achieve an objective. It is, therefore, possible that choices made at an earlier stage cannot be adequately substantiated on closer inspection in relation to the associated privacy risks. Because of its directive and corrective nature, carrying out a DPIA can be a dynamic process, whereby proposed (policy) solutions or system designs are gradually tightened with the aim of reducing the privacy risks for the data subjects.

Carrying out a DPIA can ensure confidence in the intended measure, inside and outside the organization. Collecting the information required to answer the questions helps employees and supervisors to make decisions and to render account for them. Carrying out a DPIA stimulates privacy awareness within the university.

3 In which cases is a DPIA mandatory?
A DPIA must be performed:
1. in the development of policy and regulations relating to or resulting in the processing of personal data;
2. in the case of intended processing of personal data that is likely to present a high risk to the rights and freedoms of data subjects.

Thus, in the second situation, a DPIA is not mandatory for intended processing in all cases, but only for high-risk processing.

A DPIA of intended processing operations is required in any case in the following cases:
3. a systematic and comprehensive assessment of personal aspects, based on automated processing, and on which decisions are based which produce legal effects or which affect data subjects substantially in a similar way;
4. large-scale processing of special categories of personal data or of data relating to criminal convictions and punishable offenses;
5. systematic and large-scale monitoring of publicly accessible areas; and
6. if the Dutch Data Protection Authority considered a DPIA mandatory.

In addition to this, the European privacy authorities have drawn up criteria on the basis of which it can be assessed whether there is a high risk. This concerns processing operations involving:
1. evaluating and assessing data subjects, such as profiling and predicting;
2. automated decision making with legal effects or comparable effects;
3. systematic observation, monitoring, or verification;
4. processing of special, criminal, or other sensitive personal data;
5. large volumes of data processing, taking into account the number of data subjects, the amount of personal data, the duration, and the geographical scope of the processing;
6. linking and combining personal data;
7. vulnerable data subjects who, in view of the situation, are less able to freely give their consent or challenge the data processing, such as employees, children, the mentally disabled, asylum seekers, elderly persons, and patients;
8. making use of new technologies;
9. cross-border flows of personal data to countries outside the European Union;
10. preventing data subjects from exercising a right or invoking a service or agreement.

The more criteria the proposed processing meets, the more likely it is that the risk is high. As a rule of thumb, supervisory authorities assume that processing operations meeting two or more of the criteria require a DPIA.

In any case, a DPIA is not mandatory in the following cases:

a. The processing has its legal basis in a statutory obligation or a task carried out in the public interest, and a DPIA has already been carried out in the context of the determination of this legal basis.

b. If the Data Protection Authority has determined that a DPIA is not mandatory.

In the Data Protection Authority’s view, no DPIA needs to be carried out if the data processing is not likely to present a high level of privacy risk or if the data processing is very similar to another data processing operation that has already been subject to a DPIA. Although in the case under point a, a DPIA is not mandatory, it may still be desirable to carry it out if, in the implementation, matters are specified that have not been discussed at the regulatory level, such as the choice of a particular ICT system and certain security measures.

If, contrary to the GDPR, no DPIA has been carried out or if the DPIA has been carried out incorrectly, the Data Protection Authority may impose an administrative fine of up to 10 million euros.

For questions on whether a DPIA is mandatory or desirable, the Data Protection Officer (DPO) can be contacted.

4 How does a DPIA relate to other instruments?
A DPIA is used in addition to and, if necessary, in coordination with other aids for the development of regulations and processing. Thus, a DPIA does not replace other existing instruments.

Ideally, a risk analysis and assessment should take place in which the impact of the loss of information security on the business process is determined.
The GDPR states that the controller has set up a planning and control cycle (plan-do-check-act) to ensure that the security is always adequate for the current state of affairs regarding the technology and the organization. It is important to consider the requirements of privacy and information security in relation to each other. In order to comply with the applicable regulations, a controller will have to consider all relevant aspects integrally and thus ensure that the ultimate set of measures that need to be taken in the organization and technique is adequate. For reasons of efficiency, it could be considered to carry out a CIA\(^1\) classification at the same time as a DPIA, as well as the choice of measures to be taken that are appropriate to both the CIA classification and the DPIA.

5 Who is responsible for carrying out a DPIA?
For policy and regulations
The Executive Board is formally responsible for the implementation of the DPIA. In practice, this responsibility lies with the Secretary General or the Directors of the Divisions and Schools.

For processing operations
The controller is responsible for carrying out a DPIA. Formally, the Executive Board is the controller for data processing operations carried out by a unit of the university. In practice, the power to decide whether and in what way personal data are processed will be delegated, for example, to a Director or a head of department. The mandated officer is then responsible for carrying out a DPIA.

If several Directors are responsible for processing operations, they should jointly ensure that a DPIA is carried out. In such a situation, it would seem logical for the Director who has the lead in the development of the project to take the lead in drawing up the DPIA. If a university unit or an organization outside the university acts as a processor in the sense of the GDPR—i.e., the person who processes personal data on behalf of or on the instruction of a controller—then that unit or organization is not responsible for the DPIA. However, the processor shall be obliged to assist the controller on request. In many cases, the involvement of the processor will be necessary to carry out the DPIA.

6 At what stage in the process do I need to carry out a DPIA?
A DPIA should be carried out at an early stage of the policy development. At that stage, it will be possible to consider the effects with an open mind, and there will still be sufficient opportunity to revise the basic principles of the proposal without major adverse consequences. This also prevents later, costly changes in processes, redesign of systems, or even the termination of a project. This also meets the obligation of the privacy regulations to consider protection in the design (privacy by design).

---

\(^1\) Provision regarding Confidentiality, Integrity, and Availability of the data concerned
A DPIA can be performed and updated several times and at different times. In case of a modification of the proposal involving processing of personal data, a DPIA is carried out (again). In that case, the change shall be assessed in conjunction with the existing processing operations. In case the data processing (e.g., if more personal data are processed than before) or its effects change, the DPIA needs to be updated. The European privacy authorities consider it good practice to evaluate a DPIA every three years.

In any event, the DPIA must be carried out prior to the intended processing to the extent that the results of the DPIA can still be taken into account in the decision making regarding the intended processing.

7 How do I carry out a DPIA?
Carrying out a DPIA involves the following process steps.
1. Collect all relevant information about the proposed regulation or project proposal in which personal data are processed.

2. It is preferable to discuss the points of the model in a group that includes various relevant areas of expertise. Involvement of several people with different backgrounds and expertise—think of expertise in the policy area concerned, legislation, (information) security, and ICT—results in a better DPIA. In any event, someone with privacy expertise should be involved when carrying out a DPIA. Record the findings in writing in a report.

3. Consult, if appropriate, the persons whose personal data are processed, the organizations representing them, or other parties concerned. The involvement of stakeholders enables the people carrying out the DPIA to identify the concerns at hand and, at the same time, to be transparent about the personal data that will be processed and the reasons for this. Include in the report what the person consulted advised and what was done with this. If no consultation takes place, justify this decision in the report.

4. Submit the DPIA report to the Data Protection Officer for advice. Include in the report what the officer advised and what was done with it. The GDPR states that seeking the advice of the Data Protection Officer is obligatory.

5. If the data processing is accompanied by the construction of an ICT system, the Chief Information Officer (CIO) should be involved. The CIO checks the project plan for clarity about the processing of personal data and for arguments about the desirability of carrying out a DPIA. If a DPIA is desired, it is also assessed whether this has taken place and whether the measures have been included in the project plan. Therefore, make the DPIA available to the CIO.

6. If, from the DPIA, it appears that the processing poses a high risk and the controller fails to take measures to mitigate the (residual) risk to an acceptable
level, the Data Protection Authority should be consulted prior to the intended processing.

According to the European privacy authority, an unacceptably high (residual) risk exists when the data subject is affected with significant or irreversible consequences that he or she may not be able to overcome or the chance of this happening is considerable.

For the Data Protection Authority's written advice concerning a proposed processing operation, an eight-week period applies. This period may be extended by six weeks, depending on the complexity of the proposed processing operation. Include in the report what the advice was and what has been done with it.

7. Send the final DPIA report to all parties involved in the preparation of the DPIA unless rules on confidentiality prevent this.

8. How do I account for the outcome of a DPIA

The outcome of a DPIA shall be accounted for by means of a report in accordance with the model set out in Part II.

The controller should keep records of the processing operations carried out under his or her responsibility. The results of the DPIA may be recorded in this register.

9. What should I do after the DPIA has been adopted?

After the adoption of the DPIA, the controller should take the results of the DPIA into account when further developing the intended regulations or project proposal.

The controller shall, if necessary, assess whether the processing is carried out in accordance with the DPIA. He shall do so in any event if there is a change in the risk associated with the processing operations. Risks may change due to changes in the parts of the processing operations (data, resources, threats, etc.), changes in the context (purposes, facilities, etc.), or changes in the organization or society.

In addition, the European privacy authorities recommend as good practice to carry out a DPIA every 3 years. The Data Processing Authority calls it an ongoing process. The controller must (continue to) monitor whether the data processing changes and whether the DPIA, therefore, needs to be adjusted.
Part 2
A. Description of data processing features (use the data processing inventory diagram of the DPO for this, see appendix)

Describe, in a structured way, the intended data processing operations, the processing purposes, and the interests in the data processing operations.

1. Proposal
Describe the proposal the data protection impact assessment refers to and the context in which it will be carried out in general.

2. Personal Data
List all categories of personal data that are being processed. Indicate, for each data subject category, which of their personal data will be processed. Categorize these personal data into the following types: ordinary, special, and criminal and legal identification number.

3. Data Processing
Display all intended data processing operations.

4. Processing Purposes
Describe the purposes of the intended data processing operations.

5. Parties Involved
Identify which organizations are involved in which data processing operations. Divide these organizations into the following roles for each data processing operation: controller, processor, provider, or recipient. Mention also which officers within these organizations will have access to which personal data.

6. Interests in Data Processing
Describe any interests that the controller and others have in the intended data processing operations.

7. Processing Locations
Identify in which countries the intended data processing operations will take place.

8. Techniques and Methods of Data Processing Operations
Describe how and with which (technical) means and methods the personal data will be processed. Identify whether there is (semi) automated decision making, profiling, or big data processing and if so, describe what this consists of.
9. Legal and Policy-related Framework
   Name the legislation and regulations, with the exception of the GDPR and the Policy with possible consequences for the intended data processing.

10. Retention Periods
    Determine and justify the retention periods of the personal data on the basis of the processing purposes.

B. Assessment of lawfulness of data processing
    Assess the legal basis, necessity, and purpose of the intended data processing operations and the rights of the data subject.

11. Legal Basis
    Define the legal grounds on which the data processing operations shall be based.

12. Special Categories of Personal Data
    If special personal data are processed, assess whether one of the statutory exceptions to the ban on processing applies. When processing a legal identification number, assess whether this is permitted.

13. Purpose Limitation
    If the personal data are processed for a purpose other than that for which they were initially collected, assess whether such further processing is compatible with the purpose for which the personal data were initially collected.

14. Necessity and Proportionality
    Assess whether the intended data processing is necessary to achieve the processing purposes. In any case, take into account proportionality and subsidiarity.
    a. Proportionality: are the invasion of privacy and the protection of the personal data of the data subjects proportionate to the purposes of the processing?
    b. Subsidiarity: can the processing purposes reasonably not be achieved by any other means, which are less prejudicial to the data subjects? Indicate the alternatives considered.

15. Rights of the Data Subjects
    Specify how the rights of the data subjects are put into effect. If the data subject's rights are restricted, determine the basis on which the legal exception is allowed.

C. Description and assessment of the risks for the data subjects
    Describe and assess the risks of the intended data processing operations in relation to the rights and freedoms of data subjects. In doing so, take into
account the nature, scope, context, and purposes of the intended data processing.

16. Risks
Describe and assess the risks of the intended data processing operations in relation to the rights and freedoms of data subjects. In any case, mention:

a. the negative consequences the data processing operations may have on the rights and freedoms of the data subjects;
b. the origin of such consequences;
c. the probability (chance) that these consequences will materialize;
d. the seriousness (impact) of these consequences for the data subjects when they occur.

D. Description of measures planned
Describe the measures planned to address the above-mentioned risks of the intended data processing operations in relation to the freedoms and rights of data subjects.

17. Measures
Assess which technical, organizational, and legal measures can reasonably be taken to prevent or reduce the risks described above. Describe which measure addresses which risk and what the residual risk is after the measure has been implemented.
If the measure does not adequately cover the risk, justify why the residual risk is acceptable.