Data Protection Impact Assessment (DPIA)

Template (version 1.2) by Sieuwert van Otterloo www.ictinstitute.nl

The first part of this template should be filled in for all processing activities. With this, you explain why a DPIA should or should not be done for this activity.

Sources template
This template has been developed using the following sources:

- The GDPR itself
- The Dutch GDPR manual 'Handleiding Algemene Verordening Gegevensbescherming' by the Dutch supervisory Authority Autoriteit Persoonsgegevens and Ministry of Justice, security, and defence. Authors: Bart W. Schermer, Dominique Hagenauw, Nathalie Falot
- Guidelines for DPIA's by groep Gegevensbescherming, as last edited and published on October 4 2017
- Privacy Impact Assessment (PIA): Introductie, handreiking en vragenlijst Versie 1.2 - November 2015 published by NOREA

Organization details

Name and address of the organization:

Author DPIA:

Name and contact details DPO (if appointed):

Other involved and consulted experts:

Plan of action for the DPIA execution:
Write down here on what day with whom has been spoken, which workshops have been done when, and what parties/which people were present.

Processing activity details

Describe what personal data is involved (name, email, medical information, …)

With what purpose and in which process are these data used?

What type of data subjects do the personal data belong to? (website visitors, students, customers, …)

Is this DPIA for an existing situation, or for a new proposed situation?

Should a DPIA be done?

A DPIA is mandatory when it is on the 'DPIA-list' of a supervisory authority. In the Netherlands, the Dutch Data Protection Authority published the following list of topics for which a DPIA is mandatory:
1. Secret surveillance
2. Blacklists
3. Fight against fraud
4. Credit scores
5. Financial position
6. Genetic personal data
7. Health data
8. Partnerships
9. Camera surveillance
10. Flexible camera surveillance
11. Controlling of employees
12. Location information
13. Communication data
14. Internet of things
15. Profiling
16. Observation and influencing of behavior

17. Biometric Information

A DPIA is furthermore mandatory when a processing activity will likely have a high risk to the rights and freedoms of the involved data subjects (the people whose personal data is processed). This is certainly the case when an organization:

1. systematically and extensively evaluates personal data, such as profiling;
2. processes special categories of personal data on a large scale;
3. systematically monitors data subjects in a publicly accessible area on a large scale.

To determine whether there might be a high risk, the supervisory authorities use the following heuristics. There is a high risk to the rights and freedoms of data subjects when two or more of the following nine criteria apply:

1. evaluation of people or scoring;
2. automated decision making with legal effect or comparable substantive effect;
3. systematic monitoring;
4. special categories of personal data or other sensitive data;
5. processing of personal data on a large scale;
6. matching or merging of data sets;
7. personal data on vulnerable persons;
8. innovative use of a new technological or organizational solution;
9. restricting or blocking access to a right, service, or contract

Which criteria apply to the processing activity? Indicate for each criterium whether it applies and why (not).

Systematic description of the processing activity

Describe in more detail how the processing activity works.

How / where is the information collected? From the data subject, or other source?

Where is the data stored? Who can access it?

How is the data used? Is all collected data used?

What is the purpose of the processing? Can this goal be reached without processing the personal data?

Is consent requested from the data subject in the process? Is there the ability to sign out/opt out of the service?

What is the envisioned storage term of the data? How and when will you delete the data afterwards?

What hardware and software are used during the processing?

Which departments, suppliers, and other parties are involved as processers in this processing activity?

Is the data transferred across borders? To and from which countries?

Where are the data archived? Is this on paper or digital?

What is the expected scope of processing? (amount of data subjects involved)

Judging necessity and proportionality

Is there a clearly specified purpose? What is this goal, and why is it legitimate?

Can this goal be achieved without using the personal data? Why not, or why is the other way not used?

Is there an envisioned maximum storage term?

Are data subject informed enough and correctly? Is it clear to the data subjects what rights they have and how they can execute these?

How is the right of access guaranteed?

How is the right to rectification guaranteed?

How is the right to erasure guaranteed?

How is the right to restriction of processing guaranteed?

How is the right of data portability guaranteed?

How is the right to object guaranteed?

If automated individual decision-making is done during the processing activity, can data subjects execute their right to object to it?

Judging the privacy risks

Estimating the risks

How big do you estimate the change and impact of the following risks:

Risk	How can this risk happen?	Chance it happens within one year	Impact on data subjects
Unauthorized access – internal personnel		High because …	Low because…
Unauthorized access – external parties			
Undesirable alteration of data – internal personnel			
Undesirable alteration of data – external parties			
Disappearance / loss of data			

What is the exact impact of a personal data breach (data leak) on the involved data subjects?

- Does it have negative consequences for these individuals?
- Is there a chance of financial damage?
- Is there a chance of identity theft or fraud?

Measures

Please indicate per risk which measures you will take to protect the personal data:

Are there any additional organizational measures you will take?

Are there any additional technical measures you will take?

Is it clear who is responsible for keeping up and evaluating the taken measures after the project is over? Who is this?

Advice of the Data Protection Officer

Have you appointed a Data Protection Officer (DPO)? In that case, it is mandatory to request this person's advice on the situation. Document the DPO's advice below:

Name DPO:
Data of advice:

For the DPO to answer:

Have the processing activity and the purposes of processing been described clearly enough?

Is the processing of personal data necessary and/or proportional for the purposes?

Have the privacy risks been explored and document well enough? What risks are missing?

Advice of data subjects and representatives

Has the processing activity been discussed with data subject or representatives before doing this DPIA? What was their reaction? How is this included in the DPIA?

Prior consultation

Does the DPIA indicate that the planned measures do not completely mitigate the possible risks? Answer with a clear yes or no below, and give a motivation.

Yes / No, because …

If you answered Yes, you should request a prior consultation with your Supervisory Authority (the Autoriteit Persoonsgegevens in the Netherlands). For this, you must provide this DPIA to them.

Appendix testing questions impact NOREA

The use of this appendix is optional, and may be used to improve the assessment of privacy risks. New insights from these questions must be incorporated into the main document. We recommend answering these questions too, in order to test the data estimates above. The questions originate from the NOREA guide.

Answering Yes indicates: You have an increased risk, the impact of your project on those involved and the way in which they will react is difficult to estimate. This could lead to an increased risk of image damage, disruption of business continuity, and actions by enforcers and supervisors.

Is new technology introduced? For example intelligent transport systems, location or tracking systems based on GPS, mobile technology, face recognition in conjunction with camera surveillance.

Is there any introduction of technology that can cause questions or resistance from the public? For example, biometrics, RFID, behavioral targeting (profiling).

Is existing technology introduced in a new context? Such as camera surveillance or drug control in the workplace.

Are there any other major shifts in the way the organization works, the way in which personal data are processed and / or the technology that is used in that process? For example, merging or linking various government registrations, introducing new forms of identification or replacement of a system in which personal data is stored.

Are there (in addition to the GDPR) many laws and regulations regarding personal data that the project has to deal with? Keep in mind when answering:
1. Sectoral legislation. 2. Code of conduct. 3. General administrative measures. 4. Jurisprudence. 5. International aspects.

Are there many social stakeholders? Think of employees, customers, suppliers, interest groups, civilians, clients and regulators.
Which professional groups are involved in processing?

Are many parties involved in the implementation of the project? Keep in mind: 1. Contractors and service providers 2. Hardware and software suppliers 3. IT Service providers.

Can the goal be achieved with anonymised or pseudonymised data (while this is not being used at the moment)?

Can the data be used to map and / or assess the behavior, presence or performance of people (even if this is not the goal)? Think, for example, of geolocation, personnel tracking systems, decision support for (not) offering products or services?

Do you process special personal data, sensitive personal data, unique biometric identifiers, BSN-numbers or other data for which there is a (perceived) increased sensitivity? For example, fingerprints, DNA profiles, credit card information, financial information, inheritance aspects, work performance or data subject to confidentiality? Do you process data on vulnerable groups or people? For example, minors, mentally handicapped, prisoners, supervised persons, people whose physical safety is at risk (see Appendix F).

Do the data relate to the entirety or large parts of the population of a country?

Are the data sold to third parties?

Appendix 2 – Criteria for an acceptable Data Protection Impact Assessment

The European Working Party on Data Protection "Working Party Article 29"
(abbreviated as WP29) has published a document 'Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679.'

This contains a list of criteria that you can use to assess whether a DPIA, or a method for performing a DPIA, is sufficient to comply with the GDPR.

A systematic description of the processing is provided (Article 35(7)(a)):

- nature, scope, context and purposes of the processing are taken into account (recital 90);

- personal data, recipients and period for which the personal data will be stored are recorded;
- a functional description of the processing operation is provided;
- the assets on which personal data rely (hardware, software, networks, people, paper or paper transmission channels) are identified;
- compliance with approved codes of conduct is taken into account (Article 35(8));

Necessity and proportionality are assessed (Article 35(7)(b)):
Measures envisaged to comply with the Regulation are determined (Article 35(7)(d) and recital 90), taking into account:

- measures contributing to the proportionality and the necessity of the processing on the basis of:
  - specified, explicit and legitimate purpose(s) (Article 5(1)(b));
  - lawfulness of processing (Article 6);
  - adequate, relevant and limited to what is necessary data (Article 5(1)(c));
  - limited storage duration (Article 5(1)(e));
- measures contributing to the rights of the data subjects:
  - information provided to the data subject (Articles 12, 13 and 14);
  - right of access and to data portability (Articles 15 and 20);
  - right to rectification and to erasure (Articles 16, 17 and 19);
  - right to object and to restriction of processing (Article 18, 19 and 21);
  - relationships with processors (Article 28);
  - safeguards surrounding international transfer(s) (Chapter V);
  - prior consultation (Article 36).

Risks to the rights and freedoms of data subjects are managed (Article 35(7)(c)):

- origin, nature, particularity and severity of the risks are appreciated (cf. recital 84) or, more specifically, for each risk (illegitimate access, undesired modification, and disappearance of data) from the perspective of the data subjects:
  - risks sources are taken into account (recital 90);
  - potential impacts to the rights and freedoms of data subjects are identified in case of events including illegitimate access, undesired modification and disappearance of data;
  - threats that could lead to illegitimate access, undesired modification and disappearance of data are identified;
  - likelihood and severity are estimated (recital 90);
- measures envisaged to treat those risks are determined (Article 35(7)(d) and recital 90);

Interested parties are involved:

- the advice of the DPO is sought (Article 35(2));
- the views of data subjects or their representatives are sought, where appropriate (Article 35(9)).