Conducting a data protection impact assessment

Instructions
Data protection team, City of Helsinki

Helsinki

What is personal data and what is meant by the processing of it?

Helsinki

Data Protection Team

Personal data and processing it

- Personal data are all the data that can be used alone or in combination with other data to identify a person
- Processing of personal data means all action directed towards personal data using either automatic or manual data processing.
- Processing is collecting, saving, organising, structuring, holding, editing or changing, searching, querying, using, disclosing by transferring, distributing or otherwise making available, combining, restricting or removing and destroying of data.
- Viewing data is also considered a way of processing of data

What is a data protection impact assessment?

Helsinki

Data Protection Team

The purpose of a data protection impact assessment

- The purpose of a data protection impact assessment (henceforth impact assessment) is to identify, evaluate and manage risks connected to the processing of personal data.
- The impact assessment is regulated in the EU General Data Protection Regulation.
- The controller shall in advance, even when planning the processing, evaluate and document what kind of risks the processing of personal data creates for the people.
- When the risks have been evaluated, they must be taken into account through appropriate protective measures.

When should an impact assessment be made?

Identifying the need for an impact assessment

- An impact assessment is compulsory, for example, when new technology is introduced, when sensitive or otherwise very personal data are processed or when personal data are processed on a large scale.
- The impact assessment shall be made before the service or system is put into use.
- The need to conduct an impact assessment is identified by always conducting an initial assessment connected to it, when starting to plan a new process, system procurement or construction of a system without outside help
- If the impact assessment is not made when it should have been made, then the national data protection ombudsman could consider it a breach of the Penal Code.

Tools for the impact assessment

Helsinki

Data Protection Team

City of Helsinki’s tools for conducting an impact assessment

- The City has its own tools for the impact assessment. They are used for establishing, among other things, what personal data are processed, on what grounds they are processed, where they are processed, how the data are protected and how the rights of the data subjects are carried out.

- Tools are initial assessment, data protection checklist, impact assessment tool and risk analysis form. The use of the tools always starts with the initial assessment, which guides forward to the other tools needed.

- The tools and instructions can be found on the City of Helsinki’s website https://www.hel.fi/helsinki/en/administration/information/data-protection.

Conducting the initial assessment

Helsinki

Data Protection Team

When is the initial assessment made?

- The impact assessment shall be made always when starting to plan a new process, system procurement or construction of a system in particular system development.

- An initial assessment shall also be made when planning significant changes to existing processes and systems.

- In the initial assessment, it is first established if processing of personal data is included.

- If personal data are processed, then answering the questions of the initial assessment reveals whether an impact assessment should be made or if the data protection should be taken into account using the data protection checklist.

Examples of questions in the initial assessment

- The initial assessment includes yes/no questions of whether personal data are processed and if so, then what kind of personal data.

- If the answer is yes, then further information is requested.

- Example questions:

  - Are you introducing new technology that has not been used previously?
  - Is sensitive or otherwise very personal data processed?
  - Is the personal data used for assessment and analyses, such as profiling and anticipation?
  - Is data transferred across borders outside the European Union?

Conducting the actual impact assessment

Helsinki

Data Protection Team

Conducting an impact assessment

- If the initial assessment has proved that an impact assessment must be conducted, then the impact assessment tool is introduced.

- A proven method in conducting an impact assessment is the workshop method, which starts with an initial meeting, to which all necessary experts are invited. The assignment of responsibilities takes place at the initial meeting. At the impact assessment workshop (or workshops) after the initial meeting the experts have in advance sorted out things connected to their responsibilities, whereas the documentation of the data into the tool can be made jointly.

Initial meeting / participants

- the chairperson is the one who is responsible for the matter, the “project manager” (responsible for schedule, assignment of responsibilities etc.)
- substance expert (operations representative, is familiar with the need for which the system or process is being procured)
- “user” (the one who uses the process or system, knows the daily work)
- person in charge of data protection (directs and advises the conducting of the impact assessment and the phrasing of questions)
- data security expert (tells what kind of security level is required)

- If needed also
    - procurement expert (advises in the procurement process)
    - risk management expert
    - other experts

Initial meeting / agenda

- Project summary, what is being done (chairperson)
- Description of personal data processing measure (workshop measures [slides 19–24], if wanted)
- Impact assessment:
  - The objective of the impact assessment (person in charge of the data protection)
  - Presentation of the tool (person in charge of the data security)
    - Demands are processed (2nd column, “Demand”)
  - Presentation of the risk analysis tool
- Division of responsibility:
  - Responsibilities are marked into the tool or meeting memorandum (who fills in each row in the impact assessment tool)
- Schedule:
  - Ensuring time use, conducting an impact assessment takes time
  - Agreeing on the use of the tool and the schedule for the workshops

Impact assessment workshop 1

- Before the workshop:
  - Each person in charge fills in their own rows in the tool, including identified risks
  - Each person brings the risks to the risk analysis tool on a preliminary level

- At the workshop:
  - The impact assessment tool is discussed
    - Each person presents their own rows

  - Decisions on which risks are brought into the risk analysis tool
  - Group classifies the risks
  - Group fills in the risk management measures in the risk analysis tool

  - Schedule:
  - Agreeing on the next workshop

Final measures of the impact assessment

- Filling in the Summary tab, evaluating the final result of the impact assessment (always)
- Drafting the final report for the decision-making (if needed)
- Prior consultation of the data protection authority if risks are big and they cannot be decreased independently (if needed)

Workshop task to impact assessment workshop: description of processing measures

Helsinki

Data Protection Team

Parts of the processing measure description

- Choose a familiar real system or system entity, which concerns personal data

- Under the headlines on the flap sheet comes descriptions of what they include (one headline with one-colour notes)
  - One post-it note with concrete processing parts

Sheet 1
What personal data are processed and for what purpose?

- What **personal data groups** are processed
  - E.g. name, address, personal identity code
- What **data subject groups** are there
  - E.g. clients, citizens, employees
- What is the **nature of the personal data**
  - E.g. public, confidential, sensitive
- What is the **purpose of use** of the different personal data

Sheet 2:
Where are the personal data stored and processed?

- Where does the data come from and how does it move
- Where is it stored
- Where is it processed (concretely + local dimension)
- Who processes data

Sheet 3: How and when are the personal data deleted?

- Has the storage time been defined?
  - Does the system make automatic deletions at the end of the storage time?
  - Should the data be archived and does it happen electronically?

- Can the data be obtained as a whole when the processing ends?

Combine the processing measure parts into a description

- There is a big sheet on the table
- Draw on the sheet a picture of the processing measures and place the previously drafted notes from sheets 1-3 on it

Tool tabs for the impact assessment

Helsinki

Data Protection Team

Background information tab

- Background information tab contains basic data of what kind of processing is being planned.

Short description of what kind of processing of personal data is planned:	
Maker(s) of the assessment:	
Organisation:	
Time of the assessment:	

Evaluation table tab

- The evaluation table tab has been divided into three different sections. They are:
  - ❖Systematic description of the planned processing measures
  - ❖The necessity of processing personal data and the evaluation of validity
  - ❖Evaluation of the risks caused to the rights of the data subject

- Each section has data protection demands, the fulfilment of which is evaluated.

- The next slides contain descriptions of the use of the different columns of the evaluation table.

Demand column

- This column includes the data protection demands that should be taken into consideration in the processing.
- Examples of the demands:

A functional description of the processing procedure of personal data has been drafted, which reveals the following things:

- What personal data are processed (name, address, personal identity code etc.)?
- The categorisation of the data in the system (public, confidential, sensitive etc.)
- How is the data erased?
- The data storage periods have been defined according to their purposes of use and the removal of them is carried out when the storage periods end (includes backup copies)

A data protection annex has been included in the agreement made with the processor of the personal data.

Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the data protection regulation.

The controller shall consult the supervisory authority prior to processing where this data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.

If such is the case, the controller shall provide the supervisory authority with:
a) where applicable, the respective responsibilities of the controller, joint controllers and processors involved in the processing, in particular for processing within a group of undertakings;
b) the purposes and means of the intended processing;
c) the measures and safeguards provided to protect the rights and freedoms of data subjects pursuant to this regulation;
d) where applicable, the contact details of the data protection officer;
e) the data protection impact assessment provided for in Article 35; and
f) any other information requested by the supervisory authority.

The data storage periods have been defined according to their purposes of use and the removal of them is carried out when the storage periods end (includes backup copies)

The management of the entire life cycle of the data is planned in

The data subject has a possibility to get access to his or her personal data.

A person has the right to inspect what personal data the City has of him or her, including saved data.

Describe how the requirement is carried out column

- Here comes a description of how the demand is concretely being implemented and if something is not implemented.

- Examples:
  - Demand: Personal data are collected and processed for one or several explicit and legal purposes of use, and it cannot be processed later in a way that is incompatible with these purposes.
  - Answer: The purpose of use for the personal data is organisation and implementation of health care. Personal data are not processed in other purposes of use.
  - Demand: A functional description of the processing procedure of personal data has been drafted, which reveals the following things:
    - What personal data are processed (name, address, personal identity code etc.)?
    - The categorisation of the data in the system (public, confidential, sensitive etc.)
    - How are the data deleted?
    - The data storage periods have been defined according to their purposes of use and the removal of them is carried out when the storage periods end (includes backup copies)
    - What data can be viewed, what can be edited, what can be erased?
  - Answer: Description of the processing measure has been drafted (link to the document is in the “Links to more precise documentation” column). The things mentioned in the demand are stated in the description of the processing measure. Information connected to the automatic removal of data will be elaborated relating to the storage periods and removal of data.

Links to more specific documentation, if elsewhere column

- If a comprehensive description has not been registered in the Describe how the requirement is carried out column, then links to necessary documents can be added to this column.

Does it fulfil the requirement? column

- This is for an evaluation of whether the processing is currently in its planned form in accordance with the Demand field, or if risks have emerged, for which risk management measures are still needed.
- If yes, then this section is OK. If risks are identified, they are registered in the Risks identified field.
- If no, then go to the Risks identified field.

Risks identified column

- List of the risks identified, which impair/prevent the realisation of the data protection. The risks are processed further by means of the Impact assessment risk analysis table.

- The instructions for using the risk analysis table is in this document (slide 35→).

Is the requirement fulfilled, is it possible to proceed after the risk management measures? column

- Evaluation of whether the requirement is fulfilled after the risk management measures, which are processed in the Impact assessment_Risk analysis table.

- If yes, then this section is OK.

- If not, an evaluation of whether the planned processing should be abandoned due to excessive risks or whether a prior consultation, mentioned on row 16 in the impact assessment table, should be made. Instructions for the prior consultation can be found in this document (slide 47 →).

To be observed column

- This is for necessary additional information and observations.

Summary to the decision-making tab

- Registered on this tab
  - Most important observations of the impact assessment
  - The most essential high residual risks and measures to lower them
  - Final evaluation and conclusions of the makers of the impact assessment

- The tab gives a general picture of the impact assessment to readers which has not read all the documentation related to the impact assessment.

Using the risk analysis form

Helsinki

Data Protection Team

Using the risk analysis form

- When making an impact assessment, the risk analysis form is used for evaluating the impact and likeliness of the risks and for documenting and following up the risk management measures.

- The risks are registered on the headline level in the impact assessment tool’s Risks identified column. A more detailed processing of the risks is made using the risk analysis form.

- The next slides contain descriptions of the use of the risk analysis form.

General information tab

- On the General information tab, fill in the information concerning the organisation that prepared the risk management plan and the information connected to the preparation of the plan.

Division / Department / Municipally owned company:	
Unit:	
Target of the impact assessment/risk analysis:	

Authors:	
Date of preparation:	
Previous impact assessment prepared:	

Other assessments and plans connected to the topic	Date	Authors / participants	To be observed

Impact and probability tab

- This tab includes presentations of the City of Helsinki's evaluation criteria for risk impact and probability.

Impact:

Value	Gravity of the consequence
5 Significant	• The realisation of the risk concerns special personal data groups, confidential personal data, personal identity codes or very large amounts of personal data (hundreds). o When the risk is realised, personal data can be processed by an external party. An external party can also be a party inside the City, which does not have acce o Data are processed in a manner that is incompatible with the original purpose of use • The realisation of the risk may lead to, for example, identity theft, extortion, significant financial damage, public exposure of personal data or significant reputational dan • When the risk is realised, the use of a critical data system (e.g., system containing health data) is prevented, which may cause damage related to life and health. • The realisation of the risk requires immediate response • The planned processing of personal data is illegal • The data subject cannot carry out their rights at all • The realisation of the risk causes a permanent loss of trust • The realisation of the risk requires that the data protection ombudsman and the data subject a • Plans of new activities, the risks of which are difficult to comprehend • The consequences for the data subject are long-standing (several months or even years)
4 High	• The realisation of the risks concerns to a small extent special personal data groups, confident o When the risk is realised, personal data can be processed by an external party. An ex o Data are processed in a manner that is incompatible with the original purpose of use • The realisation of the risk may lead to, for example, identity theft, extortion, momentous financial damage, public exposure of personal data or momentous reputational • When the risk is realised, the use of a critical data system (e.g., system containing health data) becomes difficult, which may cause damage related to life and health. • The realisation of the risk requires quick response • The planned processing of personal data is incompatible with the City's instructions

Probability:

Value	Class	Probability	Frequency
5	Expected	> 90 %	More than once a year
4	Very likely	< 90 %	Once in 1-5 years
3	Likely	< 60 %	Once in 5-10 years
2	Unlikely	< 30 %	Once in 10-20 years
1	Insignificant	< 10 %	Less than once in 20 years

Risk analysis tab

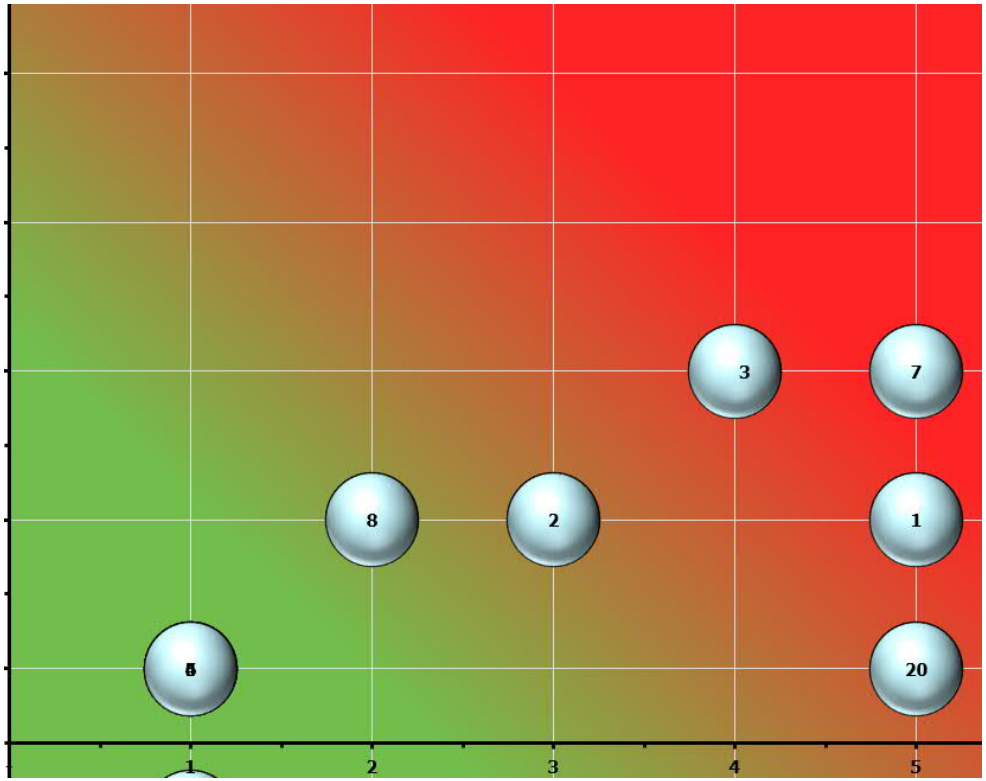
- On the Risk analysis tab, fill in the identified risks per risk class, the most probable results when the risks materialise and an estimation of the gravity of these results and the probability of materialisation.

- In the risk analysis, it is essential to identify the factors or event sequences leading to the materialisation of the risk, which the management measures are aimed at.

- In case of previously established risks, the columns “Previous risk number” and “Change” are also filled in. These are used to follow up the appropriate allocation of the risk management measures.

Risk descriptor tab

- This tab outlines a summary of the registered risks according to their significance. In the indicator, the risks have been numbered in the same way as on the “Risk analysis” tab.



Risk management measures tab

- This tab defines the management measures that reduce or prevent the risk at least for the risks whose risk figure is 8 or more, or which otherwise are deemed as risks for which measures should be allocated. On this tab the risks are filtered automatically in order according to the risk figure (biggest risk figure first).

- A person in charge must be defined for the management measures, who is in charge of their implementation and the tentative schedule, according to which the measures are carried out. The schedule should also include the agreed reporting practice concerning the advancement of the measures.

- “Degree of maturity” follows the degree of maturity at a given time for each management measure (Not started - 25% - 50% - 75% - Completed).

How are the results of the impact assessment and risk analysis utilised?

- There are many possibilities to manage the data protection risks:
  - Changes to the planned process or system
  - Organisational management measures
    - Trainings, instructions, agreements
  - Prior consultation
    - Ask the national data protection ombudsman to take a stand
  - Giving in on the project
    - If the risks cannot be managed with the above measures, then the project has to be abandoned or re-planned

Using the data protection checklist

Helsinki

Data Protection Team

Use of the checklist

- If the preliminary assessment has shown that personal data is being processed, but an actual impact assessment is not needed, then a data protection checklist shall be compiled

- The data protection checklist contains the things that always have to be considered during the development, even though the personal data being processed is not sensitive or otherwise risky.

Examples of the demands of the checklist

A data protection and non-disclosure annex has been included in the agreement made with the processor of the personal data.

Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the data protection regulation.

The processing is based on lawful grounds.

Possible grounds for processing:
a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
c) processing is necessary for compliance with a legal obligation to which the controller is subject;
d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; or
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.

The following rights of the data subject are taken into consideration:

1. The data subject has a possibility to get access to his or her personal data. *A person has the right to inspect what personal data the City has of him or her, including saved data.*

2. The data subject has a possibility to rectify and erase his or her own data. *A person has the right to request the erasure of his or her personal data. This right is exercised, if the City no longer has grounds for processing the data or if the person withdraws the consent that he or she has given to process data.*

3. The data subject has, in certain situations, the right to object or restrict the processing of his or her data.

If the accuracy of the personal data is contested by the data subject or if the lawfulness of the processing is unclear, then the processing of the data can be restricted for a period enabling the

The description of the processing actions or the other documentation (e.g. architecture description) includes a description of the data flows, which reveals:

- Where is the data stored and processed?
- Is the data processed outside the EU/EEA only in line with the data protection policy?
- What kind of APIs and user interfaces are used?
- What data can be viewed, what can be edited, what can be erased?
- In which countries is the data processed?
- Where are the servers?
- Is the data mirrored to another server room?
- Where are the backup copies?
- Can the data be accessed through a remote connection and if so then
    - by whom?
    - from where?
    - in which cases?

Prior consultation of the data protection ombudsman in high-risk processing

Helsinki

Data Protection Team

When is a prior consultation needed?

- The controller shall consult the supervisory authority prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.

- So if the risks established in the impact assessment cannot be controlled by risk management means, but there is a desire to go ahead with the processing, then a prior consultation with the national data protection ombudsman is necessary.

- The processing cannot start before the data protection ombudsman’s statement of the prior consultation.

How is the prior consultation conducted?

- For the prior consultation, the office of the data protection ombudsman shall be provided with the following things:

  a) the respective responsibilities of the controller, joint controllers and processors involved in the processing, in particular for processing within a group of undertakings;
  b) the purposes and means of the intended processing;
  c) the measures and safeguards provided to protect the rights and freedoms of data subjects pursuant to this Regulation;
  d) the contact details of the data protection officer;
  e) the data protection impact assessment provided for in Article 35; and
  f) any other information requested by the supervisory authority

- The data protection ombudsman has provided the following instructions concerning prior consultation: https://tietosuoja.fi/en/prior-consultation.


“The processing of personal data should be designed to serve mankind.”
(Recital 4 GDPR)