Instructions for data protection impact assessments

Ref. No 1-282/2022

Effective as of 2022-03-11

NOTE: This is a translation of the Swedish version (Anvisningar för konsekvensbedömning avseende dataskydd). In the event of any discrepancy between the versions, the Swedish version constitutes the official decision and the Swedish wording will prevail.

Karolinska Institutet

Instructions for data protection impact assessments

Ref. No 1-282/2022

Contents

Document No: 1-282/2022	**Document No of previous version:** -	**Decided:** 2022-03-11	**Effective from:** From 2022-03-11 until further notice
Decided by: Head of Legal Office		**Document type:** Instructions	
Administrative division/unit: Legal Office, Data Protection Officer		**Prepared in consultation with:** Legal Unit and Information Security Unit	
Revision with respect to: New regulatory document			

1 Introduction

A data protection impact assessment shall always be carried out if the processing of personal data is likely to result in a high risk to the rights and freedoms of natural persons[1].

The purpose of an impact assessment is to anticipate risks before they arise.

The impact assessment is a process for

- ascertaining the risks accompanying the processing the personal data,
- producing procedures and measures for dealing with such risks, and
- demonstrating KI's compliance with the General Data Protection Regulation 2016/679 (GDPR).

2 Purpose

The purpose of these instructions is to support KI's operational units in their performance of an impact assessment. The instructions explain what such an assessment involves, if and when one must be carried out, and how to perform it.

The instructions are for everyone involved in the processing of personal data at KI. When processing personal data, the processor must decide if an impact assessment is required.

Appended to these instructions is a template that can be used as a basis for the impact assessment process.

3 The impact assessment

Begin by judging whether the processing can entail a high risk to the rights and freedoms of natural persons (risk analysis). If so, or in cases of doubt, an impact assessment must be carried out.

If the processor (i.e. the person in charge of a project or an activity that includes, the processing of personal data) judges the risk to be so low that an impact assessment is not required, he/she must document his/her reasons in an appropriate manner.

Risk shall be assessed in the first instance from the perspective not only of data and privacy but also of basic human rights, such as the freedom of expression and opinion, freedom of movement and freedom from discrimination.

[1] Article 35 of the General Data Protection Regulation (GDPR)

The impact assessment shall comprise

- a description of the planned personal data processing and its purpose,
- an assessment of the need for and the proportionality in the processing relative to its purpose,
- an assessment of identified risks to the freedoms and rights of the data subjects,
- a description of the planned risk management measures, including protection and security measures and procedures for ensuring the protection of personal data and demonstrating compliance with the GDPR with respect to the rights and due interests of the data subjects and other affected persons,
- a description of how these measures will be followed up to ensure their long-term effectiveness and relevance.

Impact assessments shall be documented. Such documentation shall include the decisions made to justify why personal data may be processed and any measures taken to ensure that the processing can be carried out.

If a required impact assessment is not carried out or is carried out incorrectly, KI will risk a possible fine.

4 When must an impact assessment be carried out?

An impact assessment must be carried out on the following instances:

- On the large-scale processing of sensitive personal data, such as genetic and biometric data, data on health, sex life and sexual orientation, ethnicity, political opinion, religious or philosophical conviction, or data concerning crimes committed or suspected.

- On the large-scale and systematic surveillance of public places.

- On automated personal decision-making (and profiling); i.e. the use of data to create individual profiles based on personal aspects and when such profiles are used for the making of automated decisions (e.g. recruitment without personal contact and fully automated admission).

Large-scale refers to the number of data subjects, the amount of personal data registered, the duration of the processing, the size of the geographical catchment area, etc.

An impact assessment shall also be carried out if the planned personal data processing meets *at least two* of the following criteria and is likely to result in a *high risk.*

- It concerns evaluating or ranking natural persons
- It is done to make automated decisions that have legal or similarly significant consequences for the data subjects

- It involves systematically monitoring natural persons (e.g. CCTV surveillance of public places or the collection of personal data from internet use in public environments)
- It concerns sensitive personal data
- It concerns the large-scale processing of personal data
- It combines personal data from two or more processings in a way that departs from the reasonable expectations of the data subjects (e.g. through the cross-referencing of registries)
- It processes data from natural persons who for some reason are in a disadvantaged or dependent position and therefore vulnerable (e.g. children, staff, asylum seekers, elderly people or patients)
- It uses new technology or new organisational solutions (e.g. mobile apps, the Internet of Things or smart sensors)

Should any change occur in the processing of personal data, a new impact assessment must be considered.

5 When does an impact assessment not have to be carried out?

An impact assessment need not be carried out if the processing

- is likely not to result in a high risk to the rights and freedoms of natural persons,
- is very similar to another processing for which an impact assessment has been carried out and documented (i.e. where the processing of the personal data, its purpose and method is almost identical to the other processing).

This assessment shall be documented within the project or activity to which it belongs.

Any queries concerning impact assessments may be directed to the data protection officer at KI.

6 Carrying out an impact assessment

A template is available to assist in the impact assessment process.

All documentation must be saved within the project or activity to which it belongs. It is the responsibility of the person in charge of a project or an activity to ensure that the assessment is carried out.

The accomplishment may engage persons representing different competencies in a participatory or advisory capacity in order to ensure a comprehensive assessment of the personal data processing; for example

- project manager
- principal investigator or delegated researcher
- departmental data protection manager

- divisional IT and information security manager
- information owner
- system owner
- archivist
- legal officer
- data protection officer

In some cases, it might be appropriate to obtain the views of the data subjects. If it is not appropriate (i.e. if it is disproportionate, impractical, constitutes a breach of security or if it does not fulfil the purpose of the processing), a note shall be made in the impact assessment accordingly.