Data protection impact assessment (DPIA)

**Project information**

|  |
| --- |
| **Project title:** |
|  |
| **Project manager:**  *The project manager is responsible for addressing privacy and information security aspects of the project.* |
|  |
| **The project’s affiliation:** *Department, unit, health authority.* |
|  |
| **Person/entity responsible for research**  *The Head of Department is responsible for research in all projects at the department.* |
|  |
| **Funding of the project:** |
|  |
| **Project information**  *REC-number and project period (duration of the project)* |
|  |

# Processing of personal data in the project

## Purpose of processing personal data

Describe the purpose of processing personal data. The purposes must be specified, explicit and legitimate. For research, this means that specific research questions must be formulated, which will be answered through use of the data.

|  |
| --- |
|  |

## Data sources

Check the box to indicate whether new personal data (separate data collection) and/or data that has already been registered will be collected, and specify this in the field below.

Own data collection (the project will obtain data directly from the persons to whom the data apply)

Central health registers

Health studies (existing)

Clinical quality registries

Patient records

The National Population register (Folkeregisteret)

Statistics Norway (SSB)

Internet

Other

Specify the data sources that have been checked, and describe linking if this is relevant:

|  |
| --- |
|  |

## Data subjects

Data subjects are the persons to whom the data applies, often called project participants.

Check the boxes for the categories of data subjects for which information is to be processed:

Pupils/students/kindergarten children

Patients/clients/users

Children, specify age groups

0-13

13-16

16-18

Family members/next of kin

Ethnic minorities

Deceased

Other (specify below)

Describe the sample, sub-samples if applicable, and number:

|  |
| --- |
|  |

## Categories of personal data

Check the boxes for the categories of personal data that will be processed in the project.

Categories of personal data

Name

Address

Date of birth

National identity number (11 digits)

Other information, such as telephone numbers, email addresses, IP addresses, demographic variables, socio-economic data (education, income, occupation), family status

Special categories of personal data (previously called sensitive information)

Racial or ethnic origin

Political opinions, philosophical or religious beliefs

The fact that a person has been suspected of, charged with, indicted for or convicted of a criminal act

Sexual issues

Trade union membership

Biometrics

Health matters:

Diagnoses

Use of medicinal products

Cognitive functions

Genetics

Biological material

Other, specify below

Specification of the data and the level of variables:

|  |
| --- |
|  |

## Processing of personal data

“Processing” means any operation or set of operations that is performed on personal data. Check the box for what is to be done with the personal data in the project, and specify this if applicable. The processing must be in accordance with the stated purpose.

Collection

Storage

Alignment, linking

Analysis

Disclosure by transmission

Making available

Retrieval *(for example for planned feedback to the data subjects)*

Erasure, anonymization

Other use (specify below)

## Storage location and storage media

Specify where and how personal data are to be saved and handled.

Services for Sensitive Data (TSD)

Restricted-access research file folder in the NTNU file structure

HEMIT/St. Olav's Hospital

Encrypted flash drive

Hunt Cloud

Biobank, specify

|  |
| --- |
|  |

Other, specify:

|  |
| --- |
|  |

If applicable, specify the storage of the personal data:

|  |
| --- |
|  |

## Data controller, data access and data processors

### Data controller and people with data access

Delegated data controller:

|  |
| --- |
|  |

How will the staff access data?

|  |
| --- |
|  |

If personal data are to be transmitted or in other ways shared with an external institution, Section 1.7.2 must be filled in. (Exemption for the use of TSD or similar where external parties do not have the potential for local storage.)

### Data processor

A data processor is an enterprise that processes personal data on behalf of (according to instructions from) another institution that is a controller. For more information about what a data processor agreement is, see: <https://innsida.ntnu.no/wiki/-/wiki/Norsk/Databehandleravtale>

Will the project use other data processors other than NTNU?

Yes

No

If no, go directly to 1.7.3.

If yes, please describe which organizations that will function as data processors in the project.

| Organization | Role/function | Country |
| --- | --- | --- |
|  |  |  |
|  |  |  |

How will personal data be handed over to an external institution?

|  |
| --- |
|  |

For each data processor, it must be established that they provide sufficient guarantees to ensure that the processing meets the requirements of the GDPR and the protection of the data subject’s rights.

For data processor(s), the following requirements are fulfilled:

Data processing agreement that meets the GDPR requirements

Received and reviewed risk and vulnerability assessment (ROS)

Received description of technical and organizational measures

Received list of subcontractors

If you use data processors, it is important that they themselves contribute information on protection of personal data/information security, among other aspects, and the contact should be described. Are the data processors involved in the data protection impact assessment? Describe how the data processor(s) have been involved:

|  |
| --- |
|  |

### Transfer of personal data to other countries and/or international organizations

Will personal data be disclosed/transferred to:

People/institutions outside Norway

A third country (outside the EU/EEA)

International organizations

No data will be disclosed/transferred to other countries and/or international organizations

If personal data are to be transferred to a third country and/or an international organization:

If personal data are to be transferred to countries outside the EEA or to international organizations, a description must be included to specify how the obligations under Chapter V of the GDPR will be fulfilled.

Transfers will take place on the following basis:

Decision that the country in question has an adequate level of data protection

The transfer is subject to appropriate safeguards, such as the European Commission’s standard contractual clause – describe below:

|  |
| --- |
|  |

The transfer is subject to binding corporate rules, such as registration under Privacy Shield – describe below:

|  |
| --- |
|  |

Exemptions (derogations) for specific situations – describe below:

|  |
| --- |
|  |

Explain how the personal data will be transferred and stored outside Norway:

|  |
| --- |
|  |

## NTNU’s information security policy

Is the data processing compliant with NTNU’s information security policy?

Yes

No

Not applicable

[See also NTNU’s information security policy on Innsida](https://innsida.ntnu.no/wiki/-/wiki/Norsk/Politikk+for+informasjonssikkerhet)

# Legal basis for processing personal data

## Legal basis for processing personal data

See also <https://lovdata.no/dokument/NL/lov/2018-06-15-38?q=Personopplysningsloven>

Legal authority in the EU General Data Protection Regulation for the processing of personal data.

Article 6, The processing is lawful and fulfils the following conditions (applies to if at least one condition is met):

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

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.

Other, specify:

|  |
| --- |
|  |

## Legal basis for processing special categories of personal data (sensitive data)

For processing of special categories of personal data, it is also necessary to specify whether processing of such data is subject to the exemptions in Article 9 of the GDPR and the supplementary basis in Norwegian legislation:

**1. The data subject has given explicit consent to the processing of special categories of personal data.**

**2. Processing of special categories of personal data is necessary for scientific research on the basis of** **the following legislation:**

a) 9.2 j: Processing is necessary for scientific research.

b) Section 9 of the Personal Data Act /Article 9.2 g of the General Data Protection Regulation 9.2 g: Public interest in the processing taking place clearly overrides the disadvantages for the individual (the research participants)

c) Section 35 of the Health Research Act (helseforskningsloven): Regional committees for medical and health research ethics may grant exemption from the duty of confidentiality. This may only be applied if the research in question is of significant interest to society, and the participants’ welfare and integrity are ensured.

d) Other. The legal or regulatory authority must be specified and, if applicable, more detailed reasons must be given:

|  |
| --- |
|  |

**3.** **Processing of special categories of data is necessary for purposes other than research**. The correct reference to Article 9 (2) (b) to (i) of the GDPR must be specified and if there are additional requirements for regulation in national law, the authority in law or regulations must also be specified:

|  |
| --- |
|  |

## Purpose limitations and data minimization

The purpose of the processing is specified in Section 1.1. The personal data to be processed must be adequate, relevant and limited to what is necessary for the purposes.

The following measures are planned to ensure data minimization:

|  |
| --- |
|  |

## Storage

The storage period must be described and justified.

The project manager must decide how long it will be necessary to process the personal data:

Predefined deletion dates (specify, and justify based on time for analysis, subsequent retention for documentation/archiving purposes).

Time-limited, but without a specified date (specify criteria for determining the duration)

Specify the storage period and date of deletion/anonymization:

|  |
| --- |
|  |

*Here, a provisional deletion date or a date for new assessment of the need for further retention must be determined.*

## The rights of data subjects

### Consent

*This section applies to those projects for which separate consent is to be obtained or data from already collected population-based health studies are to be used.*

Specify and assess the process for obtaining consent:

|  |
| --- |
|  |

### Information about the processing

It is necessary to describe how information about the processing of personal data will be given to data subjects. The information requirement applies to all research projects regardless of whether they are consent-based or whether only registry data are used.

Information will be provided in the following way(s):

Information letter in connection with consent

Information online

Newsletter

Letter

Email

Individual information by email or letter

Social media

Public information campaign

Other, specify:

|  |
| --- |
|  |

### Right of access, restriction of processing, rectification, erasure and portability

**Criteria for deleting data**

Data on all data subjects will be deleted on a specified date

Data on all data subjects will be deleted after a fixed interval

Data about the individual will be deleted after a specified event

No systematic deletion of data

Provide more details based on what is checked in the field above: *For example, which time interval or which event results in deletion of the data. Also refer to the deletion routines in effect if deletion is based on manual activities.*

|  |
| --- |
|  |

**Do data subjects have the opportunity to have their data corrected or erased?**

Yes

No

**Do data subjects have the opportunity to make objections and require restrictions in the data processing?**

Yes

No

If the rights of data subjects cannot be fulfilled, describe which and why:  
*Provide reasons why public interests should override individual privacy.*

|  |
| --- |
|  |

**Describe the relationship between the data subject and the collector of the data:**

*For example: patient and treatment provider; employee and employer.*

|  |
| --- |
|  |

# Privacy, risk assessment and measures

Assessment of risk for the rights and freedoms of data subjects, and planned measures to address the risks.

## Involvement in decisions, transparency and openness, predictability

Evaluation of the origin, nature, particularity and severity of the risks. The evaluation shall must be based on the data subjects’ perspective for each risk:

* Lack of real involvement in decisions
* Lack of real transparency and openness
* Lack of predictability

Clarify potential consequences, estimate severity, identify threats and estimate probability:

|  |
| --- |
|  |

## Actions

Specify measures to deal with the risk to the rights and legitimate interests of data subjects and other people affected.

* Specific guarantees to minimize the impact
* Specific security measures concerning the personal data to be processed
* General security measures to be implemented for the system where the processing is carried out
* Organizational measures (governance)

|  |
| --- |
|  |

## Overall privacy impact assessment

The project manager must prepare a summary of privacy and personal data security:

|  |
| --- |
|  |

# Involvement and discussions

## Prior consultation with the Norwegian Data Protection Authority

When the controller cannot find adequate measures to limit the risk to an acceptable level (i.e. the residual risk still is high), there is a requirement for prior consultation with the supervisory authority (the Norwegian Data Protection Authority).

Are advance discussions with the Norwegian Data Protection Authority required?

Yes

No

# Approval

*Signature from department leader.*

|  |
| --- |
| Date:  Place:  Signature: |

Submit the completed and signed data protection impact assessment to the administration at your unit/department for archival in ePhorte (Case number 2021/1374).