

**DATA PROTECTION IMPACT ASSESSMENT (DPIA)**

*Yellow=guidelines/comments that must be deleted. Green= indicates that information must be inserted.*

**Information about the processing**

Title of [*project/name of technical system/name of processing/name of work process*]:

The processing is affiliated to [*department/section*]

Data controller: OsloMet

Contact person: [*Title and name*]

**Need for data protection impact assessment**

[*Head of entity with title and name]* has found that the processing of personal data in question will entail a relatively high risk in relation to the data subjects’ rights and freedoms and thereby requires a data protection impact assessment (DPIA), cf. the General Data Protection Regulation Article (GDPR) Article 35.

*When considering the need for a DPIA, see*

[*https://ansatt.oslomet.no/personvern#Personvernkonsekvensvurdering*](https://ansatt.oslomet.no/personvern#Personvernkonsekvensvurdering)*, which includes a link to the template for the assessment and to the Data Protection Authority’s webpage on the instances where a DPIA is ALWAYS required* [*https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/vurdere-personvernkonsekvenser/vurdering-av-*personvernkonsekvenser*/nar-ma-man-gjennomfore-en-vurdering-av-personvernkonsekvenser/*](https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/vurdere-personvernkonsekvenser/vurdering-av-personvernkonsekvenser/nar-ma-man-gjennomfore-en-vurdering-av-personvernkonsekvenser/).

This is because the planned processing entails *(list the criteria that necessitate a DPIA in relation to the processing in question):*

*Examples:*

* *Personal data about vulnerable data subjects; patients, children*
* *processing of sensitive personal data (special categories), or information of a very personal nature*
* *processing of personal data on a large scale*

***Alternative choices:***

*Alternative 1:* By following the planned measures, OsloMet believes that the personal data risk has been mitigated sufficiently for the processing to take place in accordance with the General Data Protection Regulation without prior consultation with the Data Protection Authority.

*Alternative 2:* The planned measures will not sufficiently mitigate the risk for the data subject so that the processing can take place in accordance with the General Data Protection Regulation, which means that OsloMet must consult the Data Protection Authority prior to the processing, see section 4.4.

The DPIA contains:

* A systematic description of the envisaged processing of personal data
* An assessment of the necessity and proportionality of the processing activities in relation to the purposes
* An analysis of the risks to the rights and freedoms of data subjects
* Planned measures for handling the risks

**Processing overview/records**

|  |  |  |
| --- | --- | --- |
| **Has the processing activity already been registered in OsloMet’s processing records?** | | |
| Yes | No | Partly |
| If ‘Yes’ or ‘Partly’ – describe any changes from what has been registered in the current processing records: | |  |
| If ‘No’ – describe what you expect to register in the processing records (Appendix 1) | |  |

Overview of the processing of personal data (records), <https://ansatt.oslomet.no/oversikt-behandling-personopplysninger>.

**Organisation of the data protection impact assessments (DPIA) and division of responsibility**

*[The owner of the processing / owner of the technical system / owner of the work process /academic director/project manager]* (with assistance from [*the project group/group])* has carried out a data protection impact assessment. The assessment must be approved by [*head of entity with title and name*]*.*

The following persons have participated in the project group/group that carried out the data protection impact assessment:

| Name | Role/function | Unit/Institution |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

1. **Processing of personal data in [*the project/survey/technical system/other*]**
   1. **The purpose of processing personal data**

*Why do you plan to process personal data and what will the data be used for? Describe the purpose(s) of the processing/work process.*

Describe the purposes here:

Click to enter text.

Any project description/research protocol must be enclosed.

* 1. **Data sources**

The processing [*name of processing*] comprises the following data sources/data:

*State where the information is obtained from, other technical systems, the person the data concern or others.*

Own data collection (the project will obtain data directly from the persons the data concern)

Data collection from external parties

Statistics Norway

The Population Register

Other registers

The internet

Other

The data sources ticked have resulted in the following data:

*Provide details about the data source in the form of bullet points and describe any alignments where relevant.*

Click to enter text.

*Describe the data collection in general*

Click to enter text.

* 1. **Data subjects**

The data subject(s) is/are the person(s) the information concerns. Personal data are processed about the following categories of data subjects:

Specify using free text and/or use the fields below to describe the sample and, if relevant, sub-sample: Click to enter text.

Pupils/students

Patients/staff/visitors

Children, specify age groups

0–13

13–16

16–18

Other (specify below)

*Say something about the people the sample consists of, how many, whether you have been in contact with the sample, storage period etc.*

Click to enter text.

* 1. **Categories of personal data**

*Say something about the types of personal data that will be processed, general categories of personal data and/or special categories, or general categories of personal data that for various reasons should be considered sensitive.*

*Tick which of the categories of personal data will be processed.*

General personal data include the following:

Name

Email address

Date of birth

Personal ID number (11 digits)

Other information *(e.g. phone number, IP address, address, place of study, employee ID, seniority, salary, marital status etc.)*

*Specify which ‘other information’/variables are used:* Click to enter text.

**Special categories of personal data (previously called sensitive personal data)**

The following falls under special categories of personal data:

Health information:

Diagnoses

Use of medication

Cognitive abilities

Genetics

Other, specify below

Racial or ethnic origin

Political opinions, philosophical or religious beliefs

Sex life or sexual orientation

Trade union membership

Genetic or biometric data *(e.g. facial images or dactyloscopic data)*

***Specify*** *the type of information and the levels of variables. If relevant, enclose a list of variables:* Click to enter text.

**Other factors that mean that the data must be considered sensitive:**

Information about children

Information about vulnerable groups/persons

Information about a person in a vulnerable situation

Personal ID number (11 digits)

Information about criminal convictions and offences

*More detailed description of the reason:* Click to enter text.

Special categories (sensitive personal data): <https://ansatt.oslomet.no/sensitive-personopplysninger>.

* 1. **Processing of personal data**

By ‘processing’ is meant any operation or set of operations performed on personal data. *Indicate what will be done with the personal data in* [the project/survey/ technical system/other] *and specify the purpose of the processing*. The processing must be consistent with the defined purpose.

Collection

Storage

Alignment, linking

Analysis

Disclosure of data to another institution/establishment *(e.g. partner or data processor)*

Making the data available

Retrieval *(e.g. for planned feedback to the data subjects))*

Erasure *(during or when the processing ceases)*

Anonymisation *(during or when the processing ceases)*

Other use (*specify below*):

Click to enter text.

* 1. **Storage place and storage media**

Specify where and how the personal data will be stored and handled.

Tjenester for Sensitive Data (TSD)

Office 365

Public 360

Encrypted memory stick/ encrypted hard disk

Other*, please specify*: Click to enter text.

Storage guide: <https://ansatt.oslomet.no/lagring>

* 1. **Data controller, access to data and data processors**

**1.7.1 Data controller and persons with access to data**

**Data controller (head of entity / line manager):**

Click to enter text.

**The following employees, students and other personnel will have access to data in [the project/survey/technical system/other]:**

| Name | Role/function | Access to all / selected personal data? | How will they have access? | Unit/Institution |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

If the personal data are to be transferred or otherwise shared with an external institution, fill in section 1.7.2.

**1.7.2 Division of responsibility**

*Control question: Will the personal data be sent/stored outside OsloMet?*

|  |  |  |
| --- | --- | --- |
| **Division of responsibility** | | |
| Has an agreement or contract been signed with any external institutions regarding a mutual understanding of responsibilities and roles? |  |
| Does the agreement reflect the limitations that apply to the processing of personal data? |  |
| Is a data processor being used? |  |
| Have all the data processors been identified and has the relationship with any such data processors been clarified through a contract (GDPR Article 28(3)? |  |
| About the data processor agreement | |
| Does the data processor provide sufficient guarantees that it will implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the Regulation (GDPR Article 28(1)? |  |
| Have the principles relating to processing of personal data, e.g. purpose limitation, data minimisation, storage etc. been safeguarded in the contract? |  |
| Have the rights and freedoms of the data subjects been safeguarded in the contract? |  |

Templates relating to data protection: <https://ansatt.oslomet.no/avtalemaler-for-personvern>.

How will the personal data be disclosed/transferred to the external institution/establishment?

Click to enter text.

**Data processors**

The following establishments will act as data processors in the project.

*If one or more data processors are used, fill in the following information:*

| Establishment | Role/function | Country |
| --- | --- | --- |
|  |  |  |
| *Example: UiO (TSD)* | *Storage and analysis. Institutional agreement* | *Norway* |
| *Example: Statistics Norway* | *Administrator of connection key* | *Norway* |
|  |  |  |
|  |  |  |
|  |  |  |

For data processor(s), the following requirements apply:

Data processor agreement that meets the GDPR requirements

Received and completed ROS (risk and vulnerability analysis). (To be enclosed).

Received a description of technical and organisational measures

Received overview of sub-suppliers

If data processors are used, it is important that they provide information themselves about data protection/information security, and the contract should be described. If the data processors were involved in the data protection impact assessment, describe how: Click to enter text.

**1.7.3 Transfer of personal data to other countries and/or international organisations**

Not relevant – Proceed to section 1.7.4

Persons/institutions in the EU/EEA – Proceed to section 1.7.4

Third countries (outside the EU/EEA)

International organisations

To the extent that personal data will be transferred to **third countries** (outside the EU/EEA) and/or **international organisations**, it must be described how the obligations set out in Chapter V of the General Data Protection Regulation will be met. Contact the data protection officer if you need help assessing this.

The transfers will take place on the following basis:

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

The transfer is subject to appropriate safeguards, such as the EU’s standard agreements, please describe:

Click to enter text.

The transfer is subject to binding corporate rules, please describe: Click to enter text.

Derogations for specific situations, please describe: Click to enter text.

Explain how the personal data are transferred and stored outside Norway: Click to enter text.

Transfer of personal data abroad: <https://ansatt.oslomet.no/overforing-personopplysninger-utlandet>.

**1.7.4 Risk assessment for personal data security**

A risk assessment relating to the security of personal data shall be carried out before new processing of data commences and in connection with changes in existing processing (requirements set out in the General Data Protection Regulation Article 32 ‘Security of processing’). Such assessments must cover the risk to the data subject seen from his/her perspective.

The risk assessment shall identify areas that may entail a risk relating to accessibility, confidentiality and integrity, such as accidental or unauthorised (unlawful) access, alteration, erasure, loss, or disclosure of personal data. This is in order to identify the need for measures and if necessary be able to implement risk mitigation measures to a ensure an acceptable level of security when processing personal data.

In practice, the risk assessment is carried out before, at the same time, or after a DPIA. The results of such an assessment will form an important basis for a personal data impact assessment. Note that the requirement to carry out a risk assessment is a separate requirement and that the DPIA comes in addition.

Below is a list of several questions that can help to identify the risk associated with the security of personal data. If a risk assessment has already been carried out, it is enough to refer to this assessment. If such a risk assessment has not been carried out, this should be done.

|  |  |  |
| --- | --- | --- |
| **Questions about the existing risk assessment** | | |
| If already assessed, where is the relevant documentation stored? | [Reference or link to the saved document] | |
| What does the risk assessment cover? |  | |
| Are there any scenarios that specifically address the data subject’s situation or risks/consequences relating to the data subject in the risk assessment? Please specify. |  | |
| Are there any remaining risks where adequate measures have not been implemented? | Yes  [Description required below] | No |
| If ‘Yes’, describe the risk(s): |  | |

If no risk assessment has been carried out, the following table must be filled in. The answers to these selected questions are topics that are typically included in a risk assessment. The intention is to obtain a minimum overview of the risks and the need for pertaining technical and organisational measures that help to increase the security of personal data.

|  |  |
| --- | --- |
| **Questions for cases where a risk assessment has not been carried out – measures must be described** | |
| Have adequate measures been implemented to prevent unauthorised disclosure and access to personal data? | [Describe the measures. Example: procedures and training to prevent snooping] |
| Have adequate measures been implemented to prevent accidental or unlawful destruction, loss or alteration of personal data? | [Describe the measures. Example: back-up of systems and file areas, version control] |
| Have adequate measures been introduced to detect and log alterations? | [Describe the measures. Example: technical logs and follow-up of logged alterations] |
| Have adequate measures been introduced to handle security breaches? | [Describe the measures. Example: procedures for notification and handling of non-conformities] |

Risk assessment: <https://ansatt.oslomet.no/risikovurdering-personvern>.

**Purpose limitation, data minimisation, legal basis, storage period and the rights of data subjects**

**2.1. Purpose limitation and data minimisation**

The purpose of the processing is stated in section 1.1. Personal data may only be processed for specified, explicit and legitimate purposes. The principle of data minimisation entails limiting the amount of personal data to what is necessary for achieving the purpose of the processing. The following measures are planned to ensure data minimisation. If the data material has already been collected, describe the measures that were implemented when the data were collected: Click to enter text.

Measures shall contribute to ensuring that the processing is proportionate and necessary on grounds of being adequate, relevant and limited to necessary personal data (Article 5(1)(c)), see <https://www.datatilsynet.no/globalassets/global/dokumenter-pdfer-skjema-ol/regelverk/artikkel29gruppen/Veileder-i-vurdering-av-personvernkonsekvenser-wp-248-norsk.pdf> . See especially Appendix 2.

**2.2. Legal basis for processing of personal data**

There must be legal basis for processing personal data in [the project/survey/technical system/other]. All legal basis for processing are described in the General Data Protection Regulation Article 6. Specify using free text and with reference to the correct alternative in Article 6, or tick the boxes below where the alternatives describe the basis that are assumed to be most relevant for the processing.

**1.** **The data subject has given consent to the processing of his or her personal data for one or more specific purposes, cf. the General Data Protection Regulation Article 6(1)(a).** *Enclose a copy of the declaration of consent and information letter.*

**2.** **Processing is necessary**

**a) 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, cf. the General Data Protection Regulation Article 6(1)(b).** *Enclose a copy of the contract or request.*

**b) for compliance with an ‘obligation’ to which OsloMet is subject, cf. the General Data Protection Regulation Article 6(1)(c).**

**c) for the performance of a task carried out in the public interest, cf. the General Data Protection Regulation Article 6(1)(e),**

**d) in the exercise of official authority vested in OsloMet, cf. the General Data Protection Regulation Article 6(1)(e).**

**If legal basis No 2 (b), (c) or (d) apply, there is an additional requirement for additional basis to exist in other legislation,** cf. the General Data Protection Regulation Article 6(3)(b). In such case, *one* of the following must be ticked:

I. Processing of personal data in research in accordance with the Personal Data Act Section 8.

II. Processing of personal data in student administrative systems in accordance with the Act relating to Universities and University Colleges Section 4-15.

III. Processing of personal data on appointment of employees in accordance with the Working Environment Act Section 13-4

V. Other. The statutory or regulatory basis must be specified and, if relevant, explained in more detail: Click to enter text.

**Some types of processing also require dispensation or exemption from the duty of secrecy**

I. The processing of personal data requires dispensation or exemption from the duty of secrecy from the Directorate of Health or REK or Health Personnel Act or Health Research Act. *Write:* [*An application has been or will be submitted for such a decision and the decision will be enclosed with the data protection impact assessment when this has been carried out].*

II. The processing of personal data requires dispensation from the duty of secrecy from a sector ministry or other agency. Specify the agency here: Click to enter text.. *Write*: [*An application has been or will be submitted for such a decision and the decision will be enclosed with the data protection impact assessment when this has been carried out].*

III. The processing of personal data requires a decision on dispensation from the duty of secrecy in order to make available indirectly identifiable health data from health registers established pursuant to law under the Personal Health Data Filing System Act (Section 19 e). *Write*: [*An application has been or will be submitted for such a decision and the decision will be enclosed with the data protection impact assessment when this has been carried out].*

**3.** **Processing is necessary for the purposes of a ‘legitimate interest’ pursued by OsloMet or by a third party, except where such interests are overridden by the interests of the data subject, cf. the General Data Protection Regulation Article 6(1)(f).** *Justify and assess OsloMet’s interest in the processing against the disadvantage to the data subject’s privacy, see webpadge Data protection impact assessment (DPIA),* [*https://ansatt.oslomet.no/personvernkonsekvensvurdering*](https://ansatt.oslomet.no/personvernkonsekvensvurdering) *:* Click to enter text.

**Legal basis for processing special categories of personal data are defined in the** [General Data Protection Regulation Article 9(1)](https://lovdata.no/dokument/NL/lov/2018-06-15-38/KAPITTEL_gdpr-2#KAPITTEL_gdpr-2)**.**

Special basis must exist for processing special categories of personal data, e.g. health data, cf. the exemptions set out in the General Data Protection Regulation Article 9.

**1. The data subject has given explicit consent to the processing of special categories of personal data, cf. the General Data Protection Regulation Article 9(2)(a).** Enclose a copy of the declaration of consent and information letter.

**2. Processing of special categories of personal data is necessary for scientific research purposes, cf. the General Data Protection Regulation Article 9(2)(j) on the basis of** (e.g. a statutory decision, statutory or regulatory basis):

a) Statutory decision, statutory or regulatory basis, see the alternative in section 2.2 No 2 c).

b) The interest of society in processing the data clearly outweighs the disadvantages for the individual and the conditions of the Personal Data Act Section 9 are met.

c) Other. The statutory or regulatory basis must be specified and, if relevant, explained in more detail:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**3.** **Processing of special categories of personal data is necessary for achieving a purpose other than research, cf. the alternatives set out in the General Data Protection Regulation Article 9(2)(b) to (i).** The correct reference to the Regulation Article 9(2)(b) to (i) must be provided and if an additional requirement applies for regulation by national law, the law or regulatory basis must be specified: Click to enter text.

**2.3.** **Duration of processing**

The duration of processing must be described and justified.

A decision must be made about how long it will be necessary to process the personal data.

Pre-defined erasure 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).

*Here, a preliminary erasure date or date for new assessment of the need for further retention must be provided.*

Specify the duration of processing and the date for erasure/anonymisation of the personal data and, if relevant, connection key: Click to enter text.

**2.4. The rights and freedoms of data subjects**

### 2.4.1 Consent

*This section applies to processing /work processes where separate consent must be obtained ..*

Specify and assess the process for obtaining consent: Click to enter text.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*Declaration of consent must be enclosed.*

### 2.4.2 Information about the processing

Describe how the data subjects will be given information about the processing of personal data. The duty to provide information applies regardless of whether the processing is based on consent or whether already collected data are used or the data are collected on a basis other than consent.

The information will be provided in the following manner(s):

Information letter sent out in connection with consent (enclosed)

Information online

Newsletter

Letter

Email

Individual information by email or letter

Social media

Public information campaign

Other, please specify: Click to enter text.

The information material must be enclosed (or a link included to the information online)

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

Describe what actions and procedures have been established to safeguard the data subjects’ right of access, to object (restriction of processing), to rectification and erasure and (if relevant) how the right to data portability is met, as well as how any demands that the data controller receives will be complied with in relation to the data processors. In the case of processing/projects that do not have directly personally identifiable data or access to the connection key, enquiries must be directed to the administrator of the connection key.

OsloMet has the following guidelines and information on its website to safeguard the rights of the data subjects:

* <https://ansatt.oslomet.no/personvernerklering>.

The following actions have been implemented in the project/processing/work process:

Contact information for the processing/project – *in the information letter*

Template for standard response *– this can be prepared if the plan is to provide feedback to participants on e.g. analysis results.*

Data processor agreement with clauses that safeguard the rights of the data subjects as regards access, rectification and erasure – *only relevant in cases where a data processor is used*

Other, specify below

Click to enter text.

### 2.4.4 Safeguarding the freedoms of the data subjects

|  |  |
| --- | --- |
| Assess how the freedoms of the data subjects have been safeguarded as regards the European Convention on Human Rights (ECHR) | |
| **Topics for assessment** | **Assessment** |
| The right to a private life and protection of personal data in communication |  |
| The right not to be discriminated |  |
| Freedom of thought, belief and religion |  |
| Freedom of expression and information |  |

1. **Data protection, risk analysis and measures**

**3.1. Co-determination, transparency, predictability and trust**

An analysis must be carried out of the risks to the rights and freedoms of the data subjects.

**I: Potential undesirable circumstances/incidents:** Clarify the potential consequences for the protection of the data subject’s personal data for each risk scenario.

Incidents that mean that rights and freedoms are not met can include physical, material and non-material damage. The consequences of the processing for the data subjects do not depend on an incident occurring, **but may also arise through the processing itself.** Examples include:

* The processing may lead to a financial loss for the data subject
* The processing may impact the data subject’s reputation
* The processing may entail a possibility of stigmatisation
* The processing may be discriminatory
* The processing may lead to differential treatment of applicants at OsloMet
* The processing may lead to identity theft or fraud due to inadequate security measures
* The processing may be a direct violation of privacy
* The processing may entail interference with the data subject’s freedom of expression or freedom of thought
* The processing may limit the data subject’s freedom of action
* The processing may have a negative impact on the data subject’s confidence
* The processing may lead to the individual not having his/her privacy rights met:
  + Right of access
  + Right to information
  + Right to object to automated processing
  + Right to make an objection
  + Right to rectification
  + Right to be forgotten (erasure)
  + Right to data portability
  + Right to restriction of processing

What specific rights and freedoms are at risk of not being met? Examples are provided in the table below.

**II: Probability:** Estimate the likelihood that an incident will occur. Specified as **very low, low, medium, high, very high.**

**IIl: Impact:** Estimate the degree of severity for each risk, especially in relation to the interference the potential consequence entails for the data subject. Specified as **very little, low, moderate, serious, very serious**

**Comments:** Discuss how relevant this risk is in [the project/technical system/survey/other].

*Table to assist with filling in the risk matrix under section 3.2*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **1** | **2** | **3** | **4** | **5** |
| **Probability** | very low | low | medium | high | very high |
| **Impact** | very low | low | moderate | serious | very serious |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Risk** | I: **Potential undesirable incident/circumstance** | II: **Probability in the project** | IIl: **Impact** | **Comment** |
| **Lack of genuine co-determination** | 1. The data subject has no genuine choice as regards participation. | Click to enter text. | Click to enter text. | Click to enter text. |
|  | 2. The data subject has received inadequate information | Click to enter text. | Click to enter text. | Click to enter text. |
|  | 3. The data subject has no access to the data the project/institution collects about him/her | Click to enter text. | Click to enter text. | Click to enter text. |
|  | 4. The data subject cannot withdraw from the project/processing/work process | Click to enter text. | Click to enter text. | Click to enter text. |
|  | 5. Inclusion of participants who have not consented (for *consent-based project/processing/work process*) | Click to enter text. | Click to enter text. | Click to enter text. |
|  | 6. The processing may result in discrimination or loss of reputation for the data subject | Click to enter text. | Click to enter text. | Click to enter text. |
|  | 7. The processing entails unauthorised access, accidental alteration or loss of data | Click to enter text. | Click to enter text. | Click to enter text. |
|  | ...more, if relevant | Click to enter text. | Click to enter text. | Click to enter text. |
| **Lack of genuine transparency** | 8. Failure to clearly explain the processing or the expected results of aligning the data with other data sets. | Click to enter text. | Click to enter text. | Click to enter text. |
|  | 9. The processing entails unauthorised access, accidental alteration or loss of data | Click to enter text. | Click to enter text. | Click to enter text. |
|  | ...more, if relevant | Click to enter text. | Click to enter text. | Click to enter text. |
| **Lack of predictability** | 10. The processing is outside of what the data subject will expect. | Click to enter text. | Click to enter text. | Click to enter text. |
|  | 11. More personal data are collected than necessary to achieve the purpose of the processing | Click to enter text. | Click to enter text. | Click to enter text. |
|  | 12. The personal data that will be processed are not correct or up to date | Click to enter text. | Click to enter text. | Click to enter text. |
|  | 13. Personal data are stored for longer than is necessary to achieve the purpose of the processing | Click to enter text. | Click to enter text. | Click to enter text. |
|  | 14. The processing entails unauthorised access, accidental alteration or loss of data | Click to enter text. | Click to enter text. | Click to enter text. |
|  | ...more, if relevant | Click to enter text. | Click to enter text. | Click to enter text. |
| **Lack of trust** | 15. The data subject cannot trust that he/she is provided with correct information | Click to enter text. | Click to enter text. | Click to enter text. |
|  | 16. The data subject cannot trust that data are used correctly and for the stated purpose | Click to enter text. | Click to enter text. | Click to enter text. |
|  | 17. The processing entails unauthorised access, accidental alteration or loss of data | Click to enter text. | Click to enter text. | Click to enter text. |
|  | 18. The participants are unintentionally directly identifiable *(e.g. through the use of free text in questionnaires etc.)* | Click to enter text. | Click to enter text. | Click to enter text. |
|  | 19. The electronic solution used has not been risk-assessed | Click to enter text. | Click to enter text. | Click to enter text. |
|  | ...more, if relevant | Click to enter text. | Click to enter text. | Click to enter text. |

**3.2. Risk matrix**

Plotting in the various scenarios in this risk matrix will give you an overview of the risk the various scenarios represent in relation to each other. This can help to communicate the risk and be a tool when prioritising which measures to implement.

**PROBABILITY**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Very high** | **5** | ​ | ​ | ​ | ​ | ​ |
| **High** | **4.** | ​ | ​ | ​ | ​ | ​ |
| **Medium** | **3** | ​ | ​ | ​ | ​ | ​ |
| **Low** | **2.** | ​ | ​ | ​ | ​ | ​ |
| **Very low** | **1** | ​ | ​ | ​ | ​ | ​ |
|  |  | **1** | **2** | **3** | **4** | **5** |
|  |  | **Very low** | **Low** | **Moderate** | **Serious** | **Very serious** |

**IMPACT**

**3.3. Planned measures for handling risks**

Once the risks and consequences for the data subject have been assessed, it is important to introduce sufficient measures to mitigate the risk. The objective is to ensure an acceptable level of security and safeguard the data subject’s privacy during the processing.

Fill in the necessary measures identified through the scenarios in the table below, with reference to the data protection scenarios targeted by the measure. It must also be documented whether a data protection risk exists that cannot be mitigated through the identified measures (residual risk). One example of such a risk is if the personal data must be erased manually in the system once the processing is complete, which entails a risk of human errors.

Residual risk is to be expected, as eliminating all risk will in many cases be impossible. The important thing is to have an awareness of the risk you are left with after measures have been implemented, and whether the responsible owner of the assessment accepts this risk. The data protection officer will also assess the residual risk and use it as a basis for providing a recommendation.

*Examples of types of measures:*

* *Specific guarantees for minimising interference*
* *Specific security measures that concern the personal data to be processed*
* *General security measures to be implemented in relation to the system where the processing takes place*
* *Organisational measures (management)*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Reference to relevant data protection scenario** | **Identified need for measures** | **Person responsible** | **Deadline** | **Residual risk?** |
| [No?] | [Measure: Update the application form with sufficient information to users about how their personal data will be processed] | [Ole Olsen] | [End of quarter] | [Acceptable – green] |
| [No? | [Measure: Review the section’s personal data and stipulate storage period/dates of erasure] | [Kari Karlsen] | [End of the year] | [Acceptable – yellow] |
| [No? | [Measure: Notify the owner of the major joint system that a risk assessment relating to the security of personal data / information security should be carried out] | [Kari Karlsen] | 1 Jan. 2001. | [Not acceptable – red] |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**3.4. The risk situation after measures have been implemented**

Risk will be mitigated if the necessary measures are implemented. The measures can either reduce the likelihood of a data protection consequence arising or reduce the severity of a consequence when it does arise. Plotting in the status of the various scenarios after measures have been implemented will give you an overview of the total risk OsloMet is facing in this area.

**PROBABILITY**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Very high** | **5** | ​ | ​ | ​ | ​ | ​ |
| **High** | **4.** | ​ | ​ | ​ | ​ | ​ |
| **Medium** | **3** | ​ | ​ | ​ | ​ | ​ |
| **Low** | **2.** | ​ | ​ | ​ | ​ | ​ |
| **Very low** | **1** | ​ | ​ | ​ | ​ | ​ |
|  |  | **1** | **2** | **3** | **4** | **5** |
|  |  | **Very low** | **Low** | **Moderate** | **Serious** | **Very serious** |

**IMPACT**

**3.5. Overall assessment of data protection**

The project manager/owner of the processing or work process must summarise the data protection status and security of personal data.

*Assess whether the identified risks are adequately handled and whether data protection is thus sufficiently safeguarded, with particular emphasis on the most important measures for mitigating data protection risks that have been or will be implemented:*

Click to enter text.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. **Involvement and discussions**

**4.1. The data subjects**

In principle, you must seek the views of the data subjects or their representatives on the processing where appropriate. Examples include patient organisations, focus groups, the ombudsperson for students, student parliament, trade unions etc.

Views have been sought: [Yes/no], reason:  
  
Click to enter text.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**4.2. Data manager**

By data manager is meant the institution that discloses the data. The data manager may have views about the processing and any contact with the data manager and their views should be described.

Views have been sought: [Yes/no], reason: Click to enter text.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**4.3. Assessment from OsloMet's own data protection officer**

The data protection officer must be involved in the preparation of data protection impact assessments, and their views must be incorporated.

*This section must be filled in by the data protection officer*

The data protection officer’s assessment of the processing/project is as follows: Click to enter text.

Conclusion:

**4.4. Prior consultation with the Data Protection Authority**

Should the Data Protection Authority be contacted for prior consultation? This is relevant when the project/processing/work process entails a high data protection risk for which OsloMet is unable to implement adequate risk mitigation measures.

*This section must be discussed with the data protection officer.*

Conclusion: [Yes/no].

1. **Change log**

The log can be used to keep an overview of the DPIA versions so that it is clear what has changed in [the project/technical system/survey/other].

| Version | Date | Revision |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

1. **Approval**

| Date | Version of DPIA | Approved by authority (data controller) |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Please note: REMEMBER TO STORE THE DPIA WITH APPENDICES IN P-360.**

1. **Appendices**

Remember to include documentation or state the archive reference

Fields that must be filled in and registered in OsloMet’s processing overview/records

Research protocol/project description

List of variables

Information letter and declaration of consent

Contract or request

Decision concerning dispensation from the duty of secrecy

**Appendix 1**

**Fields that must be filled in and registered in OsloMet’s processing overview/records:**

|  |  |
| --- | --- |
| **FIELD and help texts** | **Answer types and alternatives** |
| **Organisational unit**  Which organisational unit ‘owns’ the process described here? | Drop-down menu – organisational unit |
| **Contact person for the processing**  Who is the contact person for this processing? | Enter name (will be indexed) |
| **Name of processing**  Processing is always connected to a process, and frequently also to one or more ICT systems, or it can take place by means of documents, video, audio etc. What is the actual processing of personal data called in the organisation? For example: Payroll run, Appointment process, Course administration, Quality assurance etc. | Free text |
| **Purpose of processing**  Why do you plan to process personal data and what will the data be used for? | Free text |
| **Brief description of the data flow** | Free text |
| **Type of personal data**  What type of personal data will be processed? E.g. name, address, personal ID number, age, email address, gender, diagnoses etc. | Free text |
| **Sensitive personal data**  Will any sensitive personal data be processed? | Drop-down menu:  YES  NO |
| **Type of sensitive personal data**  If yes, what type of sensitive personal data will be processed? | Drop-down menu – several options possible:   * Race or ethnicity * Trade union membership * Genetic information or biometric information * Health-related data * Information about children * Information about penalties or convictions * Information about vulnerable groups/persons * Political opinion, * religion or beliefs, * Sex life or sexual orientation |
| **Legal basis for the processing**  On which provision of the Personal Data Act is the processing based? | Drop-down menu – select:     * Art. 6(1)(a) Consent * Art. 6(1)(b) Contract * Art. 6(1)(c) Legal obligation to which OsloMet is subject * Art. 6(1)(e) Official authority or public interest * Art. 6(1)(f) Legitimate interest |
| **Article 6: Additional legal basis**  If you selected (c) or (e), basis must also exist in national law, cf. GDPR Art. 6(3)(b). State these basis. | Free text |
| **Reason for legal basis**  If you selected (b) or (f), you must describe the contract or why there is a legitimate interest. | Free text |
| **Legal basis for processing special categories of personal data**  This concerns (sensitive personal data) GDPR Art. 9(2). | Drop-down menu – select:   * Art. 9(2)(a) Consent * Art. 9(2)(b) For the purposes of carrying out an obligation and exercising specific rights * Art. 9(2)(g) Public interest * Art. 9(2)(i) Public interest in the area of public health, or ensuring high standards of quality and safety of health care and of medicinal products * Art. 9(2)(j) Research purposes |
| **Article 9: Additional legal basis**  If you selected (b), (g), (i) or (j), additional legal grounds must exist in other legislation. State these grounds. | Free text |
| **Information about criminal convictions and offences**  Are you processing information about criminal convictions and offences, cf. GDPR Art. 10, cf. the Personal Data Act Section 11? | Drop-down menu:  YES  NO |
| **Whose personal data have been registered**  Employees, students, both, other (in such case, who?) | Drop-down menu – select one or more categories, e.g. employees, guests etc. |
| **Source system for information**  Are the data obtained from a system at OsloMet? | Drop-down menu – select one or more categories of systems at OsloMet. (Begin typing and the options will appear) |
| **Other sources of data**  From where are the data obtained: other systems, the data subject him/herself or others? | Drop-down menu – select one or more categories:   * Directly from the data subject * Other persons * Other enterprises * Other ICT systems * Other |
| **Storage period**  Will the data be erased and, in such case, when? If the data will not be erased once the purpose for which they were processed has been achieved, you must briefly describe why and how. | Free text |
| **ICT system/solution**  What ICT systems offered via OsloMet are used for the processing? | Drop-down menu – select one or more categories of systems at OsloMet. (Begin typing and the options will appear) |
| **Others ICT systems/solutions**  What other ICT systems are used for the processing? | Enter name (will be indexed) |
| **Risk assessment**  Has an assessment been carried out of the risk of breaches to information security and the security of personal data? | Drop-down menu:  YES  NO  DON'T KNOW |
| **Date of risk assessment**  If yes, when was the most resent risk assessment carried out? | DATE FIELD |
| **Data protection impact assessment (DPIA)**  Has a DPIA been carried out in connection with this processing? | Drop-down menu:  YES  NO  NOT REQUIRED  DON'T KNOW |
| **Procedures**  Have procedures been prepared for the processing of data, either orally or in writing, and, in such case, what are they called and where can they be found? | Free text |
| **Security**  What security measures do you yourself employ when processing personal data? | Enter text (will be indexed) |
| **Additions**  Who has access to the personal data? E.g. a pre-defined group in the organisation, persons with various roles/functions or others? | Free text |
| **Transfer**  Will the personal data at any time be transferred to an external party? Provide a brief explanation. | Free text |
| **Data processing agreement**  Has a data processor agreement been signed in connection with this processing? | Drop-down menu:  YES  NO  DON'T KNOW |
| **Documentation**  Enter the case number of any agreements and assessments (e.g. ROS analyses) in Public 360 together with any links. | Free text |
| **Comments**  Do you have any other comments to the processing? | Free text |