# Policy for the Processing of Personal Data

| | |
|---|---|
| Type of document | Topic specific policy |
| Managed by | Director of Organization and Infrastructure |
| Approved by | Director of Organization and Infrastructure |
| Valid from | 12.06.2023 |
| Next revision by | 12.06.2025 |
| Classification | Open |
| Reference ISO | ISO 27002:2022; 5.10, 5.34, 8.10, 8.11 |
| Reference NSM's core principles for ICT safety | |
| Reference LOV/Rule | EUs personvernforordning (General Data Protection Regulation (GDPR) article 5 (core principles) and 24 |
| Reference intern documents | The Policy for the Processing of Personal Data is subject to NTNU's policy for information security and ICT regulations. |

## 1. Purpose

The purpose of this policy is to:

a. Ensure that personal data about applicants, employees, research participants, and others processed by NTNU is managed in accordance with applicable laws.
b. Protect individuals from violations of their privacy.
c. Ensure that individuals have access to the information registered about them upon request.
d. Facilitate research involving the collection and processing of personal data while ensuring that the rights and requirements of research participants under applicable laws are properly safeguarded.

## 2. Applies to

a. All employees at NTNU
b. All students at NTNU
c. Anyone who has access to and/or processes and manages personal data through NTNU's ICT infrastructure.

### 2.1. Scope

The policy applies to all areas of operation at NTNU. It applies to electronically processed personal data, either in whole or in part. The policy also applies to manual processing of personal data included or intended to be included in a register, i.e., it can easily be traced back to individuals.

Personal data includes pseudonymized information, indirect information, and confidential information. Anonymous information is not considered personal data.

## 3. Key terms and Definitions

**Personal data:** Information and assessments that can be linked to an individual, either directly or indirectly, such as name, identification number, photograph, online identifier, IP address, or any specific elements related to the individual's physical, psychological, genetic, mental, economic, cultural, or social identity. Indirectly identifying personal information refers to background information that can be used to trace the information back to an individual, such as place of residence or institutional affiliation combined with information about age, gender, occupation, nationality etc.

**Health information:** Personal data about a person's physical or mental health, including information about received healthcare services that provide insight about the person's health condition.

**Special categories of personal data:** Information about racial or ethnic origin, political opinions, religion, beliefs or trade union membership, processing of genetic data and biometric data for the purpose of uniquely identifying a person, health information, or information about a person's sexual life or sexual orientation.

**Pseudonymization:** Processing of personal data in a way that the data can no longer be attributed to a specific person without the use of additional information, provided that such additional information is stored separately and subject to technical and organizational measures ensuring that the personal data cannot be attributed to an identified or identifiable individual. The data is still considered personal data under the law.

**Indirect personal data:** Background information that can be used to trace the information back to an individual, such as place of residence or institutional affiliation combined with information about age, gender, occupation, nationality, etc.

**Confidential information:** Information about someone's personal matters (e.g., family, illness, health, personal financial matters). Special categories of personal data are a separate category in the EU's General Data Protection Regulation (GDPR) that require additional security measures (e.g., information about health, sexual life, ethnic origin, political opinions). Both confidential information and special categories of personal data are classified as confidential or strictly confidential according to NTNU's Policy for Information Classification.

**Anonymous information:** Information from which names, identification numbers, and other personal identifiers have been removed, making it impossible to link the information to an individual. Only when it is certain that the information cannot be linked to a group of fewer than five individuals is it considered anonymized. Anonymized information is not considered personal data and is not regulated by data protection legislation.

**Processing of personal data:** Any operation or set of operations performed on personal data, whether automated or not, such as collection, recording, organization, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or any other form of making available, alignment or combination, restriction, erasure, or destruction.

**Record:** Any structured collection of personal data accessible according to specific criteria, whether the collection is centralized, decentralized, or dispersed on a functional or geographical basis.

**Data controller:** A physical or legal person, public authority, agency, or other body that, alone or jointly with others, determines the purposes and means of the processing of personal data. NTNU is the data controller in most cases involving the processing of personal data at NTNU. If two or more data controllers jointly determine the purposes and means of processing, they are joint data controllers.

**Legal basis for processing:** The legal basis for processing personal data. Processing of personal data must have a legal basis to be lawful. The legal bases are stated in the General Data Protection Regulation (GDPR), Article 6 (personvernforordningen art 6) for general personal data and Article 9 (art. 9) for special categories of personal data.

**Data processor:** An external or legal, public authority, institution, or any other entity that processes personal data on behalf of the data controller. Blackboard, which is the provider of the learning support system for NTNU, is an example of a data processer.

**Consent:** Any voluntary, specific, informed, and unambiguous expression of will from the data subject, by means of a statement or a clear affirmative action, indicating their consent to the processing of personal data relating to them. Must be documented.

# 4. Requirements for the Processing of Personal Data

## 4.1. General Principles for Privacy

Privacy involves the right to privacy and the right to decide one's own personal data. Individuals should, to the greatest extent possible, be able to determine their own personal data. The rules for processing personal data are based on some fundamental principles. These principles are set out in Article 5 of the EU General Data Protection Regulation (GDPR), and other provisions of the GDPR are built upon them. All processing of personal data must comply with these principles, which are:

a. **Lawfulness, fairness, and transparency –** There must be a legal basis (processing justification) that permits the processing of personal data. At least one of the bases specified in the EU General Data Protection Regulation must be met. The processing of personal data should be done with respect for the interest of the data subjects and establish trust. The processing of personal data must be understandable and predictable for the data subject, enabling them to exercise their rights. Transparency in processing is a prerequisite for individuals to be able to exercise their rights and interests.
b. **Purpose limitation –** Personal data should only be processed for specific, explicit, and legitimate purposes. Personal data cannot be reused for purposes incompatible with the original purpose. Further processing for archival purposes in the public interest, for scientific or historical research purposes, or for statistical purposes is considered compatible with the original purposes. This requires the implementation of technical and organizational measures to ensure the rights of the data subjects, particularly to ensure compliance with the principle of data minimization. Appropriate measures may include pseudonymization. If the measures can be fulfilled by further processing that does not allow the identification of the data subjects, the purposes must be fulfilled in this manner (anonymization of personal data). Further processing assumes compliance with the EU General Data Protection Regulation and the law during the initial collection of personal data.
c. **Data minimization –** The amount of collected personal data must be limited to what is necessary for the purpose of the collection.
d. **Accuracy –** Processed personal data must be accurate and, if necessary, updated.
e. **Storage limitation –** Personal data must be erased or anonymized when they are no longer necessary for the purposes for which they were collected, unless the personal data are subject to archiving obligations (I.e., they are included in documents that are subject to administrative processing and have value as documentation). Public authorities are subject to archive information about employees and students.
f. **Integrity and confidentiality –** This mean that the data controller (NTNU or anyone acting on behalf of NTNU) must implement measures to prevent accidental and unlawful destruction, loss, or alteration of personal data. This must take precedence over availability.

g. **Accountability –** NTNU must act in accordance with these principles and ensure that the rights of data subjects are protected. NTNU must be able to document that it has implemented necessary organizational and technical measures to comply with the EU General Data Protection Regulation.

## 4.2. Record of Processing Activities

a. The record must contain information as specified in Article 30 of the EU General Data Protection Regulation
b. The record must be kept in NTNU's joint system for recording processing activities.
c. The data registry of Sikt privacy services for research, which designated NTNU employees have access to, provides an overview of the processing of personal data in student and research projects reported to Sikt.
d. Health research projects for which the Faculty of Medicine and Health is responsible must be included in NTNU's register of health research projects (SharePoint solution).
e. Health research projects for which other faculties are responsible must be reported to Sikt and will be registered in Sikt's data registry.

## 4.3. Basis of Treatment

### 4.3.1. General

Processing of personal data requires a legal basis (lawful ground), meaning that there is a law (e.g., the EU General Data Protection Regulation, the Personal Data Act, the Universities and University Colleges Act) or regulation that allows for the specific processing.

To process personal data, one of the bases in Article 6(1) of the EU General Data Protection Regulation (GDPR) must be fulfilled. The basis can be consent or one of the other alternatives. At least one of the following conditions must be met:

a. The data subject has given consent (which must be documented) to the processing of their personal data for one or more specific purposes.
b. The processing is necessary to:
    i. Fulfil a contract with the data subject
    ii. Protect the vital interest (life and health) of the data subject or another physical person
    iii. Comply with a legal obligation imposed on the data controller
    iv. Perform a task carried out in the public interest
    v. Exercise official authority vested in the data controller

For the last three alternatives, an additional basis in national law is also required. Provisions in the Personal Data Act, the Universities and University Colleges Act, or other laws can serve as such additional legal basis.

If special categories of personal data (health information, information about ethnicity, political opinions, etc.) are to be processed, one of the points in Article 9(2) of the EU General Data Protection Regulation must also be fulfilled.

Article 6(1)(f) of the EU General Data Protection Regulation allows for the processing of personal data if the processing is necessary for the legitimate interest pursued by the data controller, provided that the data subject's interests or fundamental rights and freedoms do not override those interests. This provision generally cannot be used as a basis for processing personal data about students since it does not apply to processing carried out by public authorities in the performance of their tasks. However, this provision may be a basis for processing personal data about employees.

### 4.3.2. Personal Data About Applicants, Students, and Doctoral Candidates

Section 4-15 of the Universities and University Colleges Act allows for the processing of personal data about applicants, students, and doctoral candidates (hereinafter referred to as students) in administrative systems for the following purposes:

a. The purpose must be to safeguard the rights of the data subject or to fulfil the institution's tasks and obligations under the Universities and University Colleges Act
b. Names, national identification numbers, temporary identification numbers (D-numbers), and grades from secondary education and universities and university colleges obtained from public authorities, public systems for diplomates, state, county municipality, and private educational institutions can be processed when necessary to fulfil the purpose.
c. Information about health, social conditions, and other sensitive information provided by the student to the institution or to which the student has consented can be processed when necessary for the purpose mentioned above.

If personal data is to be processed for other purposes, the student must give consent, or another legal basis must be present.

### 4.3.3. Personal Data About Employees

The legal basis for processing basic employee information is Article 6(1)(b) of the EU General Data Protection Regulation, which means that the processing is necessary to fulfil a contract with the data subject. For special categories of personal data, one of the conditions in Article 9(2) of the GDPR must also be fulfilled. Section 6 of the Personal Data Act provides an additional basis for processing special categories of personal data when necessary to fulfil employment-related obligations or rights.

Provisions regarding access to an employee's email account and camera surveillance in the workplace are established by the relevant department as regulations to the Working Environment Act, based on sections §§ 9-5 and 9-6 of the Act.

### 4.3.4. Consent as Basis of Treatment

Consent from the data subject can be legal basis for processing personal data. This requires that the following conditions are met:

a. **Voluntary –** The consent must not be tied to any benefits or negative consequences. If the university considers relying on consent from students and employees for processing, the balance between the parties must be considered. This may mean that the consent is not considered truly voluntary.
b. **Specific** – The purposes for which the consent is given must be clear.
**c. Informed –** The scope of the consent must be clear when the data subject consents.
d. **Unambiguous –** It must be clear that the individual has given consent, including the date of consent and the name of the person giving consent. The data controller must be able to demonstrate this, either through written or electronic documentation.

The data subject must be able to withdraw consent at any time, and it must be as easy to withdraw as it is to give consent.

## 4.4. Risk Assessment

The risk assessment aims to prevent unwanted incidents or deficiencies in the processing of personal data at NTNU that could have consequences for students, employees, research participants, and/or society in general. Key factors in the risk assessment include the scope of the project/processing, the sensitivity of the information, the threat landscape associated with the environment in which the

information is processed and stored, and the duration of the project/processing. All assessments and measures should be documented.

NTNU's Policy for Risk Management for Information Security provides guidance on how to conduct a risk assessment. Additionally, there is support material available on Innsida for risk assessment of information security (risikovurdering av informasjonssikkerhet ) and risk assessment of research projects involving personal data (risikovurdering av forskningsprosjekt som inneholder personopplysninger.).

## 4.5. Assessment of Privacy Implications and Prior Consultation with the Norwegian Data Protection Authority

### *4.5.1 General Information About Data Protection Impact Assessments (DPIA)*

If it is likely that a type of processing will result in a high risk to individuals' rights and freedoms, the data controller must assess the consequences that the planned processing will have on privacy, in accordance with Article 35 of the EU General Data Protection Regulation.

This may be relevant, for example, when using new technology, when performing automated processing that will have legal effects on individuals, processing large-scale special categories of personal data, or systematically monitoring a public area on a large scale. The Norwegian Data Protection Authority has development a guide for assessing privacy implications. The guide provides an overview of when a Data Protection Impact Assessment (DPIA) must be conducted. The DPIA is carried out in consultation with the Data Protection Officer. NTNU's template should be used, and the assessment should be documented in NTNU's case and archive system.

An assessment that concludes that it is not necessary to perform a DPIA should also be documented, either in NTNU's joint system for tracking the processing of personal data or in the case and archive system.

Please refer to the Norwegian Data Protection Authority's guide and checklist for assessing privacy implications (DPIA) and NTNU's website for assessing privacy implications.

### *4.5.2 Obligations to Consult with the Norwegian Data Protection Authority in the Case of Persistent High Risk*

NTNU is required to consult with the Norwegian Data Protection Authority if the conclusion is that, even after implementing technical and/or organizational measures, the processing will still entail a high risk, no measures are taken to reduce the risk, and it is still desirable to proceed with the planned processing. Rector decides whether NTNU should request a preliminary consultation with the Norwegian Data Protection Authority. Any inquiries should be made by the Rector.

## 4.6. Data Processor Agreement

If external parties (a company or individual) are to process personal data on behalf of NTNU, a data processor agreement must be concluded. An agreement can only be made with data processors who provide sufficient guarantees that they will implement appropriate technical and organizational measures to ensure that the processing of persona data meets the requirements of the EU General Data Protection Regulation and protects the rights of the data subjects.

The agreement must meet the requirements that appear in Article 28 of the EU General Data Protection Regulation. In collaboration with the higher education sector, NTNU has developed a standard data processor agreement that should be used. If NTNU's template for the data processor agreement cannot be used, the proposed agreement should be reviewed by a jurist at NTNU before it is concluded.

NTNU's procedure for entering into a data processor agreement must be followed (see NTNU's website) and should be reviewed every other year, as well as revised if necessary.

The data processor must not engage another data processor (sub-processor) without the written approval of NTNU as the data controller. NTNU is responsible for the data processors and any sub-processors processing of the personal data and is responsible for assessing and verifying their competence to process the relevant personal data in accordance with the EU General Data Protection Regulation.

The data processor must regularly conduct security audits of their work to ensure the protection of personal data against unauthorized or unlawful access, alteration, deletion, damage, loss, or unavailability. The data processor must document these security audits, and NTNU must be granted access to the audit reports.

When NTNU, together with other data controllers, jointly determines the purposes and means of processing personal data, a joint data controller arrangement exists. In such cases, an agreement specifying the parties' responsibility must be entered. NTNU's template can be used for this purpose.

### 4.7. Transfer of Personal Data to Countries Outside the EU/EEA

Personal data should only be transferred to countries or international organizations outside the EU/EEA if the requirements of the EU General Data Protection Regulation Chapter V (Articles 44 and onwards) are met. Note that *transfer* also includes granting access to personal data.

A risk assessment of the transfer must be conducted to ensure that information security is satisfactory. The risk assessment must be documented.

a. Transfers to countries outside the EU/EEA can take place if the European Commission has approved that the country ensures an adequate level of protection for personal data.
b. Transfers beyond this require the use of the EU's standard contractual clauses for the transfer of personal data to controllers or processors in third countries, or the transfer is permitted under other provisions of the EU General Data Protection Regulation Chapter V. The EU's standard contractual clauses are available on the Data Protection Authority's website.
c. Transfers based on Article 49 of the EU General Data Protection Regulation provide exceptions for special cases. This applies, for example, if the data subject has explicitly consented to the specific transfer or if the transfer is necessary for the performance of a contract between the data subject and the data controller or another physical or legal person. An example of this is members residing outside the EU/EEA in expert committees.

Agreements on the transfer of personal data abroad must be submitted to the IT Division and reviewed by a jurist before the agreement is concluded.

### 4.8. Rights of the Data Subjects

The term *data subject* refers to individuals, applicants, students, employees, research participants, and others whose personal data is processed by NTNU. The data subjects have several rights related to being informed when information about them is collected, access to their own personal data that is processed by the organization, the right to request rectification, erasure, restriction of processing, objection, and the right to data portability (EU General Data Protection Regulation Articles 12-23).

There are several exemptions from these rights, both in the EU General Data Protection Regulation and in the Norwegian Personal Data Act Sections 16 and 17. For example, exceptions apply to information that is confidential (where access would reveal information about other individuals or security measures). There are also specific exemptions related to archival, research, or statistical purposes. As a public institution, NTNU is subject to the Archives Act, which means that personal

data about employees and students is often subject to archiving requirements and cannot be requested to be deleted.

Data subjects who wish to exercise their rights, such as access to information, must follow NTNU's procedures and identify themselves before access can be granted. The processing of requests for access must comply with NTNU's procedures. The Records Management Division must be the recipient of access requests in accordance with NTNU's procedures.

### 4.9. Photo, Video-, and Audio Recordings

The person who intends to publish a photograph publicly (e.g., on the internet, intranet, learning support system, in print) of an individual or a small group of people must obtain consent from the person(s) depicted. The consent must be in writing or can be documented in another way, e.g., electronically.

According to the Copyright Act of June 15, 2028, section 104, a photograph depicting a person cannot be reproduced or publicly displayed without the consent of the person depicted. Exceptions apply if:

a. The depiction is of current and general interests
b. The depiction of the person is less important than the main content of the image
c. The image portrays gatherings, outdoor public events, or matters or events of general interest

Video and/or audio recordings of identifiable individuals require consent from each individual. The same applies to publishing, for example, on the internet, intranet, and learning support system.

Consent forms and guidance/procedures should be available on NTNU's website.

### 4.10. Camera Surveillance

It must be clearly indicated by signage that the premises are under surveillance, including whether audio recording is involved, and who is the data controller (NTNU through the Property Division). The need for camera surveillance is assessed regularly.

Recordings must be deleted *one week* after they are made. If it is likely that the recording will be handed over to the police in connection with investigation of criminal acts or accidents, the recordings can be stored for up to 30 days.

Disclosure of recordings can only occur in the following cases:

a. The person depicted gives consent
b. The disclosure is made to the police in connection with investigation of criminal acts or accidents, and statutory confidentiality does not prohibit the disclosure
c. It is otherwise provided by law that the disclosure can take place

### 4.11. Access Control

Personal data from NTNU is transferred daily from the shared database to NTNU Security and Service. The personal data transferred includes the individual's name, social security number/student number, email address, workplace, and start date. The information must only be used to produce access cards. Only dedicated employees in Security and Service should have access to the information.

### 4.12. General Processing of Personal Data

NTNU's case and archive system support digital workflow, signing, and secure digital communication.

Confidential or special category personal data must be processed in NTNU's case and archive system or in another approved specialized system. These are information classified as confidential or strictly confidential according to NTNU's classification system.

Paper documents containing confidential, sensitive, or other personal data that is exempt from public access based on its content must be stored in locked cabinets in offices/areas that are locked outside regular working hours.

Documents containing confidential or special category personal data that are electronically sent to member of boards and committees must be separated from other matters so that members can delete this information once the case is processed. Electronic transmission should only be used if the digital solution is classified for transmitting confidential or special category personal data.

NTNU has created an overview of file and document storage, specifying which systems/tools can be used for what purpose. This must be available on NTNU's website.

### 4.13. Confidentiality

Anyone who routinely handles confidential personal data must be familiar with the privacy regulations and sign a confidentiality agreement.

Employees, as well as consultants and suppliers who, through maintenance and operation of NTNU's ICT infrastructure and systems, gain access to confidential personal data, must be familiar with the regulations on the processing of personal data and sign a confidentiality agreement. Requirements for, and information on, the duty of confidentiality for members of committees, boards, and councils must be included in the appointment letter to the members.

### 4.14. Storage, Deletion, and Archiving

Personal data must not be stored longer than necessary to fulfil the purpose of the processing, unless otherwise is specified by law or, for example, in connection with research funding. This follows the principle of storage limitation and data minimization.

Each employee is responsible for deleting personal data stored in their personal user area.

a. Personal data that is not be retained under the Archived Act or other legislation, must be deleted.
b. Personal data must be deleted or cleaned up continuously, and no later than six months after an employee leaves or a student graduates/leaves.
c. Personal data, temporarily stored on personal areas in connection with the performance of a work task, must be deleted when the purpose is no longer present.
d. Members of councils and committees who receive electronically sent documents containing confidential or special category personal data should delete the material received once the case is processed.
e. Documents subject to archiving, i.e., documents subject to case processing and have value as documentation, must be archived in the institution's archive system.

### 4.15. Use of National Identification Numbers

a. National identification numbers and other unique identifiers can only be processed when there is a legitimate need for secure identification, and the method is necessary to achieve such identification, in accordance with the Personal Data Act § 12.
b. National identification numbers can be sent via secure digital communication. National identification numbers should not be accessible to anyone other than the recipient. If national identification numbers are sent by mail, they must not be visible in the envelope window or written on the outside of the envelope.
c. If national identification numbers are to be sent via email, the email must be encrypted.

## 4.16. Use of E-mail

In accordance with the policies of the Norwegian Data Protection Authority, the following must not be sent via email.

a. Confidential or special category personal data
b. National identification numbers and other unique identification numbers
c. Personal data about many individuals, such as spreadsheets or lists

The points apply to both emails sent internal at NTNU and external.

If email and/or attached files are encrypted, email may be used on exceptional occasions. The risk must be assessed, passwords must be sent separately (via SMS or verbally) and must comply with NTNU's password requirements, as outlined in the "Policy for Cryptographic Controllers".

## 4.17. Disclosing Information About Students and Employees to External Parties

Information collected and stored for general personnel management and administrative purposes regarding students must not normally be disclosed to external partied unless those requesting the information have a right of access under the Freedom of Information Act. The disclosure of personal data from NTNU's systems for purposes other than those for which they were collected must be approved by the system owner. The system owner is responsible for ensuring that the disclosure is documented in a manner that allows the information obligation to be fulfilled in the event of a request for access from the data subject.

If it concerns information that is not subject to access rights under the Freedom of Information Act, the requesting entity (e.g., the Norwegian Labour and Welfare Administration, the National Service Administration) must refer to a legal basis that entitles them to obtain the information. Such requests must be processed by the system owner. The system owner is responsible for examining whether the necessary legal basis for the disclosure exists and, if necessary, requesting it.

Confidential information may be disclosed if the conditions of the Public Administration Act § 13 b are met, for example, to a lawyer representing a student or employee in a case at NTNU.

If access is granted, it must be stated that the recipient must have a separate legal basis for any further electronic processing of the information.

## 4.18. Relationship to Access Rights Under Other Laws

Questions regarding access to public documents are regulated by the Act of 19 May 2006 on the right to access public documents (The Freedom of Information Act). Access for parties involved is regulated by the Act of 10 February 1967 on the Procedure in Administrative Cases (the Administrative Procedure Act).

According to Article 86 of the EU General Data Protection Regulation, each state can establish rules regarding access to public documents. The provisions on access for everyone under the Freedom of Information Act and access for parties under the Administrative Procedure Act therefore take precedence over the provisions of the EU General Data Protection Regulation and the Personal Data Act. This means that when it comes to questions of access to documents at NTNU, access can be granted to documents containing personal data if authorized by the Freedom of Information Act. The concept of "document" under the Freedom of Information Act will then determine which documents can be accessed. The same applies to access by parties under the Administrative Procedure Act. The case processor, possibly in consultation with their superior, decides on access questions.

### 4.19. Privacy by Design

Privacy by design and Privacy by Default mean that privacy considerations are taken into account in all phases of the development of a system or solution. This is an obligation that the organization has under Article 25 of the EU General Data Protection Regulation.

The purpose of Privacy by Design is for the data controller to consider privacy issues before and during the procurement/development of systems and services. The requirement for Privacy by Design and Privacy by Default applies regardless of the level of risk.

## 5. Control and Compliance

Institutes must annually report to the faculty regarding the processing of personal data, using a self-assessment template. The same applies to sections within departments in the central administration. The faculty/department must compile the collected information using the template. Departments must also report on the control of research projects. A summary of this information must also be included in the faculty's report.

Deans/department heads must ensure that a report is prepared and submitted to the Department of Corporate Governance. The report is then forwarded to the Director of Organization and infrastructure for the Rector's review. The reports shall, among other things, form the basis for the Rector´s annual briefing to the NTNU Board on the work related to information security, including the processing of personal data.

## 6. The Processing of Personal Data in Research

According to recital 159 (considerations) of the EU General Data Protection Regulation, the processing of personal data for purposes related to scientific research should be interpreted broadly and may include technological development and demonstration, fundamental research, applied research, and privately funded research.

### 6.1. Notification to Sikt Privacy Services

Research-, student-, and quality assurance projects that process personal data, as well as health research where a faculty other than the Faculty of Medicine and Health Sciences is the research controller, must be notified to Sikt Privacy Services. The same applies to projects where personal data is processed on paper if they are included or intended in a personal register.

Sikt has an advisory role. Sikt must assess whether the project complies with the requirements of the EU General Data Protection Regulation. The processing of personal data cannot commence until Sikt has provided feedback to the project leader stating that the planned processing is considered to be in accordance with the EU General Data Protection Regulation, and that necessary prerequisites, recommended measures, and assessments are carried out. In case of questions regarding Sikt's assessment, there will be a dialogue between Sikt and NTNU to align necessary actions. If Sikt and NTNU have different assessments of what is sufficient, the final decision will be made by the Research Controller in consultation with the jurist in Divison for Governance and Management Systems.

If a student or researcher is collecting data abroad, the notification obligation to Sikt applies to the processing of personal data, just as it does for data collection in Norway.

The project must be notified at least 30 days before the data collection is scheduled to begin. Sikt also offers archiving of project data at the end of the project.

According to the EU General Data Protection Regulation, it is a requirement for the organization to keep a record (protocol) of all processing activities involving personal data. Sikt must, on behalf of NTNU, maintain a record of all research, student, and quality assurance projects that are notified to

Sikt. The record will serve as the basis for supervision and control of research projects, as outlined in the policies section on Monitoring and Compliance – Research Projects (6.9)

## 6.2. Health Research – Pre-approval by REK

Medical and health-related research (health research) involves research on humans, human biological material, or health information with the purpose of obtaining new knowledge about health and disease. This also applies to research involving pilot studies and experimental treatment.

Health research must receive prior approval from the Regional Committees for Medical and Health Research Ethics (REK) before the project can commence, as stated in the Health Research Act §33. REK must conduct an ethical assessment of the project. REK's pre-approval is not a sufficient legal basis for the processing of personal data in health research. The processing of personal data must also have a legal basis in the EU General Data Protection Regulation. The research controller will be responsible for assessing whether the processing of personal data in health research projects complies with the EU General Data Protection Regulation.

This policy provides the overarching principles for health research as well. NTNU's portal for medical and health-related research (NTNUs portal for medisinsk og helsefaglig forskning) provides more detailed research administrative procedures and policies.

In cases where a faculty other than the Faculty of Medicine and Health (MH) is the research controller in health research projects, the research project must be notified to Sikt Privacy Services in addition to the application to REK. Sikt will assess whether the planned processing of personal data in the project complies with the requirements of the EU General Data Protection Regulation. The processing of personal data cannot commence until Sikt has provided feedback on its assessment.

In general, it is recommended to submit/notify project information to Sikt and REK as soon as possible, preferably in parallel. Sikt will assess on a case-by-case basis whether they consider the project to be ready for assessment or if they will await REK's assessment of the project.

## 6.3. Evaluation of Privacy Consequences (DPIA)

If a certain type of processing is likely to result in a high risk to individuals' rights and freedoms, the data controller must assess the potential impact the planned processing will have on privacy, in accordance with Article 35 of the EU General Data Protection Regulation. This also applies to research.

Sikt takes the initiative to initiate and assist in the evaluation of privacy consequences (Data Protection Impact Assessment – DPIA) for the projects reported to Sikt. Sikt will conduct the DPIA assessment in consultation with the Data Protection Officer.

The Faculty of Medicine and Health Sciences has developed a specific template for evaluating privacy consequences in health research projects. The project leader is responsible for ensuring that an assessment of privacy consequences is carried out. The Data Protection Officer must provide advice on the assessment of privacy consequences upon request and monitor its implementation.

## 6.4. Legal Basis for Processing

### *6.4.1. In General*

If personal data is to be processed in connection with research, a legal basis is required (consent from participants or a law that permits it). According to research ethics principles, consent is the general rule for research involving information that can be linked to individual participants. According to recital 33 of the EU General Data Protection Regulation, research participants should be able to give consent to certain areas of scientific research when this is in accordance with recognized ethical standards for scientific research. Research participants should have the opportunity to consent only to

certain research areas or parts of the research project to the extent permitted by the intended purpose. Further information on participant information and consent can be found at Sikt.

For the processing of ordinary personal data, the legal basis will be:

a. Consent according to Article 6(1)(a) of the EU General Data Protection Regulation, or
b. If not consent: the processing is necessary for the performance of a task carried out in the public interest and related to scientific research, as specified in Article 6(1)(e), and the supplementary basis in the Personal Data Act § 8
c. The processing must include necessary measures to ensure compliance with the EU General Data Protection Regulation and the protection of research participants' privacy.

For the processing of special categories of personal data, the legal basis will be:

d. Consent according to Article 9(2)(a), or
e. If not consent: the processing is necessary for scientific research, provided that the societal interest in the processing outweighs the individual's disadvantages, as stated in Article 9(j) and the supplementary basis in the Personal Data Act § 9.
f. The processing must be subject to necessary safeguards, such as pseudonymization of personal data so that the information is no longer directly linked to the individual without additional information, access control, and logging.

For the processing of personal data concerning criminal convictions and offenses, the legal basis will be:

g. Consent according to Article 6(1)(a), or
h. If not consent: the same as for special categories of personal data, where the societal interest in the processing outweighs the individual's disadvantage. The assessment must take into account that the processing takes place without the consent of the data subject. The assessment must be documented. Legal basis: article 6(1)(e) and article 10 with supplementary basis in the Personal Data Act § 11
i. The processing must be subject to necessary safeguards to protect the privacy of research participants, as described above for special categories of personal data.

#### *6.4.2. Health Research*

Decisions on exemptions from confidentiality obligations will constitute an additional legal basis. The research ethics assessment conducted by the Regional Committees for Medical and Health Research Ethics (REK) (prior approval according to §§ 9 and 33 of the Health Research Act) will serve as an appropriate and specific measure to protect the rights and interests of the data subjects. As part of the research ethics assessment, REK will also assess the processing of personal data.

#### *6.4.3. Further Processing for Research Purposes*

Further processing of personal data for research purposes, based on already collected personal data, is considered compatible with the original purpose. This requires the implementation of technical and organizational measures to protect the rights of the data subjects, particularly to ensure compliance with the principle of data minimization. Relevant measures may include pseudonymization.

If research purposes can be achieved using anonymized information, further processing must be conducted in this manner. Further processing for research purposes assumes that the already collected data has been processed in accordance with the regulations.

If the further processing involves disclosure to another data controller (i.e., entities other than NTNU), the recipient of the data must have a separate legal basis for the processing.

## 6.5. Data Management Plan (DMP)

All research projects must have a data management plan. The data management plan should describe how research data will be collected, stored, and shared to ensure secure and proper handling of the data.

The plan must be an active document that is updated throughout the project, documenting how research data is processed and organized. A data management plan must also include considerations related to ethics and privacy. The plan must comply with requirements from funding sources and be in line with NTNU's policy for the processing of personal data.

## 6.6. Storage of Active Research Data

Personal data must not be stored longer than necessary for the purpose for which it was collected, unless otherwise specified by law or, for example, in relation to research funding.

## 6.7. Access to Research Data by Project Staff

Research data must only be accessible to approved project staff until the end of the project. The project leader determines which project staff members should have access to pseudonymized personal data and the linking key. The project leader must maintain a documented overview of those who have access to the data, which must be available to the research supervisor.

In general, project staff should not have access to the linking key. In cases where they do have access to the linking key, the data is no longer considered pseudonymized but directly identifiable, which increases the requirements for proper handling and storage.

## 6.8. Conclusion of Research Projects

Personal data must be anonymized or deleted if there is no requirement for storage based on the granted approvals or in relation to the financing of the research project. Necessary confirmations must be sent to REK and Sikt.

## 6.9. Monitoring and Compliance – Research Projects

The research supervisor must implement systematic measures to ensure that the project is conducted in accordance with the guidelines and that the processing of personal data complies with laws, regulations, and NTNU's own policies.

A sample of 10% of the research projects collectively must be monitored annually. The sample must be drawn from different stages of the implementation: initiation, execution, and conclusion.

### 6.9.1 Monitoring of Initiation

Research projects that have been awarded research funding and other known projects must be checked against the notification overview at Sikt. This is to verify whether the obligation to consult has been complied with.

### 6.9.2 Monitoring of Execution

The research supervisor checks whether the research project has obtained any necessary approvals/permits and whether the consultation obligation with Sikt and the data protection officer has been fulfilled. The monitoring aims to ascertain whether the project is being carried out in accordance with the information provided to REK/Sikt and the granted approvals/advice.

### 6.9.3 Monitoring of Conclusion

The research supervisor must verify whether the procedures related to conclusion have been followed and that research data stored electronically or in other archives have been deleted or anonymized.

In the management dialogue with their superior, the research supervisor must report on the extent to which laws, policies, and procedures are being complied with and what measures have been taken.

# 7. The Processing of Personal Data in Connection with Teaching

## 7.1. Video- and Audio Recordings

It is not necessary to obtain consent from the instructor to stream/record teaching sessions that are necessary to fulfil NTNU's obligation to provide students with education and require NTNU login to access. The legal basis for processing is provided by Article 6(1)(f) of the EU General Data Protection Regulation. NTNU may have a legitimate interest in streaming the teaching sessions, for example, to make them accessible to students across multiple campuses. The privacy impact is considered low when NTNU login is required to access the teaching sessions.

If the recording is to be made publicly available on the internet, consent from the instructor is always required. NTNU's agreement form for online accessibility must be used.

If students are present, it must be clearly indicated at the entrance and in the room that the teaching session is being recorded on video.

Video and/or audio recordings of students that may enable their identification require consent from the student. This applies, for example, when students are presenting a project or similar activities. The consent must meet the requirements for valid consent as described in the section "Consent as a Legal Basis" and must be documented.

Students who wish to make recordings (video and/or audio) of teaching sessions must obtain consent from the instructor unless there is an accommodation decision in place (vedtak om tilrettelegging.). The student can only use the recording for their own studies. The student cannot use the recording in any other way or publish it without written consent from the instructor (e.g., on the internet or in other contexts).

If video recordings of students are an obligatory part of the teaching to achieve learning objectives, this must be specified in the study plan. In such cases, the legal basis for recording and using the recordings is provided by Article 6(1)(e) of the EU General Data Protection Regulation with additional grounds in § 4-15 of the Universities and University Colleges Act.

## 7.2. Image, Video, and Audio Recordings – Students in Internships/Practical Training

If students in internships or practical training wish to take photos or make video and/or audio recordings of individuals, consent from the person is required, as stated in the section "Consent as a legal basis". Consent from parents or guardians is required for capturing images, videos, or audio recordings of minors. Images from internships must not be posted on the internet or social media.

## 7.3. Learning Platforms

NTNU's chosen learning platforms, which have approved data processing agreements, must be used to coordinate, and manage course content and for communication in teaching, among other things.

## 7.4. Student Projects

When processing personal data in connection with bachelor's, master's/thesis, and doctoral projects, the rules for processing personal data in research must be followed, as outlined in Chapter 5.

## 8. Compensation and Restitution for Privacy Breaches

Violations of privacy regulations can result in administrative fines from the Norwegian Data Protection Authority (Datatilsynet) and the affected individuals may be entitled to compensation or restitution. If NTNU is fined, the unit where the breach occurred is responsible for covering the fine. The same applies to any compensation or restitution amounts payable to the affected individual.

## 9. Roles and Responsibility

Rector has delegated the authority to approve, coordinate, and implement necessary measures to the Director of Organization and Infrastructure. This includes imposing obligations on faculties and departments in the joint administration, to ensure that the processing of personal data complies with NTNU's goals, overarching policies, legal requirements, and that information security is functioning satisfactorily.

Line managers, system owners, and process owners have key roles in the processing of personal data.

### 9.1. Board

a. Has overall responsibility for the processing of personal data at NTNU.

### 9.2. Rector

a. Is the highest data controller for the processing of personal data at NTNU.
b. Must annually inform the Board about the processing of personal data in the organization.

### 9.3. Director of Organization and Infrastructure

a. Has been delegated the task of approving, coordinating, and implementing necessary measures to ensure that the processing of personal data complies with legal requirements and NTNU's policies.
b. Is responsible for collecting and reporting to the management's annual review.
c. Must ensure that relevant parties are notified of serious breaches of privacy.
d. Is responsible for implementing necessary measures to ensure appropriate treatment of nonconformity.

### 9.4. Division Directors and Head of Sections in the Joint Administration

a. Are responsible for compliance with requirements for the processing of personal data within their respective units.
b. Are responsible for ensuring compliance with legislation, procedures, approvals, and closing discrepancies.
c. Are responsible for maintaining an up-to-date overview of ICT systems used.
d. Are responsible for ensuring that employees within the unit receive sufficient training in the processing of personal data and can fulfil their duty to assess risks in new projects and treatments, as well as report discrepancies related to information security.
e. Are responsible for ensuring that all employees within the unit have access to services and materials so that users can protect the privacy of the data subjects.
f. Are responsible for systematically reviewing data processing agreements and other significant agreements, as well as reviewing deviations within the unit on at least an annual basis.
g. Are responsible for ensuring that internal control functions within the unit.

### 9.5. Dean/Museum Director

a. Are responsible for compliance with requirements for the processing of personal data at their respective faculties/museums
b. Are responsible for ensuring that all heads of departments are familiar with current procedures and policies for the processing of personal data

c. Are responsible for establishing necessary local procedures as needed
d. Are responsible for ensuring compliance with legislation, procedures, approvals, and closing discrepancies.
e. Are responsible for maintaining an up-to-date overview of ICT systems used.
f. Are research managers/data controllers within their own faculty and must have an overview of the faculty's research portfolio.
g. Are responsible for ensuring that employees within the unit receive sufficient training in the processing of personal data and can fulfil their duty to assess risks in new projects and treatments, as well as report discrepancies related to privacy breaches.
h. Are responsible for providing necessary training in the processing of personal data to NTNU students.
i. Are responsible for ensuring that all employees within the unit have access to services and materials so that users can protect the privacy of the data subjects.
j. Are responsible for conducting dialogues with respective subordinate units, including follow-up on procedures and deviations, on at least an annual basis.
k. Are responsible for ensuring that internal control functions related to the processing of personal data function within the faculty/museum.

### 9.6. Head of Department

a. Is responsible for compliance with requirements for the processing of personal data at the department.
b. Is responsible for ensuring that employees are familiar with relevant laws and regulations, as well as procedures for the processing of personal data and research ethics guidelines.
c. Is responsible for enabling employees to fulfil their obligations to assess risks in new projects and treatments, as well as report discrepancies related to privacy breaches.
d. Is responsible for ensuring that internal control for the processing of personal data functions at the department.

### 9.7 Head of the IT Division

a. Is responsible for maintaining an up-to-date overview of NTNU's ICT infrastructure and ensuring information security within and between systems.
b. Is responsible for ensuring that all employees and students at NTNU have access to services and materials that allow them to protect the privacy of data subjects.

### 9.8. Head of the Digital Security Section

a. Is responsible for implementing security requirements for NTNU's ICT infrastructure and receiving reports of discrepancies.

### 9.9. System Owner

The leader responsible for developing, managing, and/or operating an information system on behalf of NTNU. A data custodian may also be considered a system owner.

a. Is responsible for ensuring that the development, management, and/or operation of the IT system meet the requirements of information security, including the processing of personal data.
b. Has the responsibility to keep a record of the processing of personal data (log) for the system they are the system owner of, and is also responsible for keeping the record updated and maintained.
c. Is obliged to ensure that a risk assessment is conducted before the processing of personal data can commence.
d. Must ensure that a DPIA (Data Protection Impact Assessment) is conducted when required, in consultation with the Data Protection Officer.

e. Is responsible for entering into a written data processing agreement if external parties (a business or individual) are to process personal data on behalf of NTNU.
f. Is responsible for reviewing the data processing agreement every two years and revising it, if necessary, as well as obtaining documentation from the data processor's security audit.
g. Is responsible for personal data that is to be transferred to countries or international organizations outside the EU/EEA only transferred if the requirements according to the EU General Data Protection Regulation Chapter V (Articles 44 et seq.) are met.
h. Must ensure that the data subject is informed and that inquiries from the data subject are followed up in accordance with the requirements of the EU General Data Protection Regulation.
i. Must appoint a system contact person who can assist with access requests when the data subject requests a copy of personal data from a given system.
j. Is responsible for developing procedures to minimize the security risk associated with the processing of personal data in systems for which they are the system owner, which also includes deletion procedures.
k. Must ensure ongoing deletion/cleanup of unnecessary personal data within 6 months after an employee leaves or a student graduates or leaves.
l. Must approve the disclosure of personal data from NTNU's systems for purposes other than those for which they were collected.
m. Is responsible for the disclosure being documented so that the obligation to provide information in the event of a request for access from the registered person can be met.
n. Is responsible for investigating whether the necessary legal basis exists for the disclosure of personal data for their system and, if necessary, requesting it.
o. Is responsible for ensuring that the processing related to video and audio recordings in teaching (use, storage, deletion, etc.) complies with privacy regulations and follows NTNU's processes, procedures, and selected solutions.
p. Must ensure that privacy by design is implemented in accordance with Article 25 of the EU General Data Protection Regulation during development and procurement. The data protection officer shall be involved.

### 9.10. Line Manager

A manager with personnel responsibility (vice-rectors, directors, department heads, deans, museum directors, institute heads, section heads)

a. Is responsible for maintaining a record (log) of the processing of personal data carried out in their unit and is also responsible for keeping the record updated and maintained.
b. Is obliged to ensure that a risk assessment is conducted before the processing of personal data can commence.
c. Must ensure that a DPIA is conducted when required, in consultation with the data protection officer.
d. Is responsible for entering into a written data processing agreement if external parties (a business or individual) are to process personal data on behalf of NTNU.
e. Is responsible for reviewing the data processing agreement every two years and revising it, if necessary, as well as obtaining documentation from the data processor's security audit.
f. Is responsible for personal data that is to be transferred to countries or international organizations outside the EU/EEA are only transferred if the requirements according to the EU General Data Protection Regulation Chapter V (Articles 44 et seq.) are met.
g. Must ensure that the data subject is informed and that inquiries from the data subject are followed up in accordance with the requirements of the EU General Data Protection Regulation.

h. Is responsible for ensuring that the processing (use, storage, deletion, disclosure, etc.) of images, video, and audio recordings complies with the privacy regulations and follows NTNU's processes, procedures, and selected tools/systems.
i. Is responsible for ensuring that the physical conditions are conductive to the secure processing of personal data in their unit.
j. Is responsible for developing procedures to minimize the security risk associated with the processing of personal data in their unit, which also includes deletion procedures.
k. Is responsible for ensuring that personal data is deleted from shared areas in their unit.
l. Shall ensure ongoing deletion/clean-up of unnecessary personal data within 6 months after an employee leaves or a student graduates or leaves.
m. Is responsible for ensuring that employees receive necessary training on the provisions related to the processing of personal data.

### 9.11. Process Owner (Will be the Directors)

A process owner is a leader in the joint administration who is responsible for overall administrative processes at NTNU. The process owner is responsible for common procedures and policies and is responsible for managing, improving, and following up on the overall processes within their area of responsibility.

a. Is responsible for overall administrative processes at NTNU.
b. Must maintain a record (log) of the processing of personal data for overall administrative processes and is also responsible for keeping the record updated and maintained.
c. Is responsible for common procedures and policies and shall continuously manage, improve, and follow up on the overall processes to ensure compliance with the requirements for the processing of personal data.
d. Must conduct an overall risk assessment of processes that process personal data.
e. Is responsible for entering into a written data processing agreement if external parties (a business or individual) are to process personal data on behalf of NTNU.
f. Is responsible for reviewing the data processing agreement every two years and revising it, if necessary, as well as obtaining documentation from the data processor's security audit.
g. Is responsible for personal data that is to be transferred to countries or international organizations outside the EU/EEA are only transferred if the requirements according to the EU General Data Protection Regulation Chapter V (Articles 44 et seq.) are met.
h. Is responsible for developing procedures to minimize the security risk associated with the processing of personal data in overall administrative processes, which also includes deletion procedures.
i. Must ensure ongoing deletion/clean-up on unnecessary personal data within 6 months after an employee leaves or a student graduates or leaves.

### 9.12. The Research Responsible

The research responsible is the person who exercises the data controller's responsibility on behalf of the Rector in research projects. The research responsible is the dean who has overall responsibility for all research projects carried out at the faculty. The dean can delegate tasks to the department head.

a. Must facilitate research conducted in such a way that ethical, medical, health-related, scientific, privacy, and information security aspects are safeguarded from planning to completion and for post-management of research data and human biological material.
b. Must establish procedures, infrastructure, and internal control systems for research activities in accordance with applicable laws and policies and ensure that these are implemented and followed in practice.

c. Is responsible for reporting the project to Sikt/REK and must be informed of the outcome of the processing.
d. Must, before or after, assess whether the project falls within the unit's strategy and whether the necessary resources are available.
e. Must approve the project after it has been pre-approved by REK or assessed by Sikt before it can commence.
f. Must have an overview of their research portfolio.
g. Must cease research that is ethically or legally indefensible or that conflicts with the project's assumptions.
h. Must implement systematic measures that promote good research and ensure that research is planned, organized, conducted, and completed in accordance with current regulations.
i. Must follow up on inquiries regarding access and other matters from research participants and ensure compliance with the obligations to provide information to them.

### 9.13. Project Manager and Supervisor for Student Projects

a. Must conduct risk assessments and assess privacy implications in research-, student-, and quality assurance projects.
b. Must ensure that measures are implemented regarding research data that correspond to the actual risk based on a risk assessment.
c. Must ensure that students are familiar with the rules for the processing of personal data in relation to student projects.
d. Is responsible for the data collected and used in the project and must have access to all research data covered by the project.
e. Allocates access rights and keeps track of who has access to the data.
f. Must follow up on inquiries regarding access, and other matters from research participants, and ensure compliance with the obligation to provide information to them.
g. Has the operational responsibility and must ensure internal control during the implementing of the research project, from planning to completion, including compliance with relevant laws, research ethics, and internal policies for information security and privacy.
h. Must ensure the necessary application to REK or notification to Sikt and that the forms are completed in accordance with how the project is conducted in practice.
i. Must involve the research responsible before submitting an application to REK or notification to Sikt and present the application and notification form if requested by the research responsible.
j. Must develop a data management plan, according to the section Data Management Plan (DMP)
k. Must ensure that the agreements required for safeguarding information security and privacy are concluded (for entering into data processing agreements, see the section Data Processing Agreement)
l. Is responsible for ensuring that relevant and necessary documentation requirements are met in the project.
m. Must assess whether the personal data can be pseudonymized.
n. Must report serious, undesirable, and unexpected medical events to the research responsible and the Norwegian Board of Health Supervision. Research participants must also be promptly informed if they have suffered harm or complications as a result of the research project.
o. Must ensure that personal data is anonymized or deleted at the end of the research project if there is no requirement for retention based on approvals given or in connection with the financing of the research project and must ensure that necessary confirmations are sent to REK and Sikt.

PhD candidates can be project managers. Students at lower levels cannot be project managers. If there is only one researcher, that person is the project manager.

### 9.14. Research Data @NTNU

a. Provides advice and guidance related to the processing of personal data in research projects.
b. Must collaborate with and serve as a point of contact for Sikt for the follow-up of specific projects.

### 9.15. Data Protection Officer at NTNU

a. Must provide NTNU's management and employees with information and advice on NTNU's obligations under the EU General Data Protection Regulation (GDPR) and other relevant privacy legislation.
b. Must provide advice on the assessment of potential privacy implications (DPIA) and oversee its implications.
c. Must monitor compliance with the EU General Data Protection Regulation and other relevant privacy legislation and internal policies.
d. Must stay informed about and follow up on incidents of privacy breaches.
e. Must collaborate with and serve as a point of contact for the Norwegian Data Protection Authority and data subjects.

### 9.16. Privacy Advisor for Sikt Privacy Services

a. Must provide advice on how NTNU, as the data controller, can best safeguard privacy interests in research projects.
b. Must receive notifications regarding the processing of personal data in research projects and maintain a record/register of such processing in a separate archive.

### 9.17. Director of Property Management

a. Is responsible for the storage of personal data in production of access cards.
b. Decides whether surveillance cameras should be installed and is responsible for ensuring that procedures for storage, deletion, and potential disclosure are followed. This applies to all NTNU premises and buildings.

### 9.18. All Users

a. Users who handle personal data are responsible for familiarizing themselves with relevant legislation regarding the processing of personal data.
b. They are responsible for familiarizing themselves with policies and procedures for the processing of personal data when using NTNU's ICT infrastructure and in research projects and other projects.
c. They are required to report incidents (unwanted events) involving privacy breaches in accordance with NTNU's Policy for Incident Reporting and Management in Information Security and Privacy.
d. Each individual employee is responsible for deleting personal data stored in their personal user areas.

## 10. References

### 10.1. Key Laws and Regulations Include:

a. EU General Data Protectional Regulation (GDPR) - provides rules for electronic processing of personal data related to individuals, obligations for NTNU as the data controller, and rights for data subject.

b. Personal Data Act – enacts the EU General Data Protection Regulation into Norwegian law and includes additional provisions.
c. Universities and University Colleges Act – provides rules (supplementary legal basis) for the processing of personal data about applicants, students, and PhD candidates, the national diploma and grade portal, and reporting to higher education and scientific publishing databases.
d. Constitution § 102 – sets requirements for the protection of personal integrity.
e. Working Environment Act, regulation for Chapter 9
    i. Regulation on camera surveillance in the workplace
    ii. Regulation on the employer´s access to email accounts and other electronically stored material.
f. Public Administration Act – provides rules on administrative procedures, including confidentiality and access to records by parties involved.
g. Public Access to Information Act – provides rules on the obligation to grant access to documents and exceptions to the right of access.
h. Archives Act – provides rules on which documents are subject to archiving requirements and requirements for archiving.
i. Health Registry Act – provides rules on the collection and processing of health information.
j. Health Personnel Act – provides rules on confidentiality and exemptions for research purposes.
k. Health Research Act – provides rules on the organization, roles, responsibilities, and advance approval of health research.
l. Research Ethics Act – provides rules that research should adhere to recognized research ethical norms.
m. Copyright Act – provides rules on the use of images (§ 104).

The list is not exhaustive; other laws and regulations may also apply.