



## JOINT CONTROLLER AGREEMENT

According to applicable Norwegian personal data legislation and the EU General Data Protection Regulation 2016/679 of 27 April 2016 («GDPR»)

---

**[Subtitle related to the relevant relationship/project]**

between

**[Name of institution/company]**

*[org.no.]*

**("Name 1")**

and

***[Name of institution/company]***

*[org.no.]*

**("Name 2")**

*[More institutions/companies can be added depending on the relevant relationship/project]*

*Text in italics should be removed and replaced with relevant text, or one of several text alternatives should be chosen where applicable.*

## **1. Purpose**

The purpose of this agreement on joint controllership (“the Agreement”) is to regulate the parties’ respective responsibility for compliance with applicable personal data legislation when the relevant processing of personal data related to the specific relationship/project as specified on the Agreement’s front page (“the Main Agreement”) entails that there is a joint controllership between the parties.

The parties are joint controllers for the personal data processed under this Agreement, on the basis that the parties jointly decide the purpose of the processing of the personal data and what means are to be used, cf. Article 26 of the GDPR.

The Agreement establishes the contractual arrangement required by Article 26 of the GDPR and sets out each of the parties’ respective responsibilities to comply with the obligations of the GDPR, regarding the exercise of the data subjects’ rights and the obligation of the parties to comply with the information requirements of Articles 13 and 14 of the GDPR.

In the event of conflict, the terms of this Agreement will take precedence over the parties’ respective privacy policies or terms of any other agreement entered into between the parties in connection with the data processing under the Agreement.

The purpose of the processing, the types of personal data to be processed, relevant categories of data subjects, and an overall description of each of the party’s respective roles related to the data processing and the obligations applicable to the controller according to Chapter 4 of the GDPR, are specified in Appendix 1 of the Agreement. These specifications cannot be changed by any of the parties unless either a new agreement or an amendment letter to this agreement is signed between the parties.

## **2. Purpose limitation**

The parties shall not process the personal data for purposes other than those specified in the Agreement, unless otherwise provided for by statutory obligations.

## **3. Compliance with applicable personal data legislation**

By signing this Agreement, each party undertakes the following:

- The parties shall comply with all requirements of applicable privacy legislation with respect to the processing of personal data in relation to this Agreement, including the obligation to carry out risk assessments, and to enter into data processing agreements with its suppliers that process personal data comprised by this Agreement.
- The parties confirm that, pursuant to Article 32 of the GDPR, they have taken adequate technical, physical and organizational security measures to protect personal data comprised

by this Agreement against unauthorized or unlawful access, alteration, deletion, damage, loss or inaccessibility.

- If a party detects errors or indications of errors in connection with the transfer of personal data under this Agreement, the party that detects the error shall immediately inform the other party.
- Each party has a sufficient legal basis for its respective processing of personal data as specified in this Agreement, in accordance with Article 6 of the GDPR.
- In consultation with the other party, to comply with Articles 33 and 34 of the GDPR to report personal data breach to the Norwegian Data Protection Authority and to the data subjects, respectively, when the conditions for such notification exist in the individual case.

#### **4. The rights of the data subjects**

Each party shall respect the rights of the data subjects as regulated in Chapter 3 of the GDPR.

Each Party shall ensure that clear and sufficient information on the processing of personal data is made available to the data subjects, in accordance with Article 12-14 of the GDPR.

In connection with the compliance with this information obligation, each party shall make the essential content of this Agreement between the joint controllers, available to the data subjects pursuant to Article 26 of the GDPR. This entails that as a minimum, the following information shall be provided:

- information that there is a joint controllership
- the identity of the joint controllers
- information on the most important roles of the respective controllers in the processing of personal data on the data subjects
- that each of the controllers is required to fulfill the data subjects' rights pursuant to Chapter 3 of the GDPR
- the contact point for the data subjects, cf. section 14

#### **5. Confidentiality**

The content of the Agreement and the information processed are subject to a duty of confidentiality between the parties. However, each party may share information about the Agreement and information processed with advisers and subcontractors to the extent deemed necessary for the fulfillment of their respective tasks for the respective party, provided that the receiving party is made subject to a corresponding confidentiality obligation as set forth in this provision. Each party may also share such information as set out in section 4 with the data subjects.

Norwegian law may limit the extent of the duty of confidentiality for each of the parties.

#### **6. Information and meeting obligation**

Each party is obliged to keep the other party informed on an ongoing basis of relevant information in connection with the parties' respective controllership under this Agreement. This applies in particular

when receiving requests from data subjects regarding the exercise of the data subjects' rights to rectification and deletion etc. pursuant to Chapter 3 of the GDPR, or in the event of a party's implementation of its own measures to comply with those rights to the extent it must be presumed that this may be of relevance to the other party. This also applies to any inquiries from the Norwegian Data Protection Authority with requests for information, notification of inspections etc.

Each party has the right to call the other party to a meeting to discuss matters concerning the exercise of the joint controllership with a minimum of 10 working days' written notice. A proposal to a meeting agenda shall follow the call for a meeting. Meetings may not be required more frequently than once a quarter, unless there are special reasons justifying more frequent meetings.

## **7. Obligation to notify in case of security breach**

Each party shall notify the other party without undue delay if personal data processed by the respective party are exposed to a security breach which entails a risk for violations of the privacy of the data subjects (Articles 33 and 34 of the GDPR).

The notification to the other party shall, as a minimum, include information that describes the security breach, which data subjects are affected by the breach, what personal data are affected by the breach, what immediate measures are implemented to address the breach and, if applicable, what preventive measures have been established to avoid similar incidents in the future.

The party responsible for the system or process underlying the security breach in question is responsible for notifying the security breach to the Norwegian Data Protection Authority or to the data subjects, as applicable, where this is required by Articles 33 and 34 of the GDPR. To the extent possible based on statutory deadlines, the other party shall be consulted before the notice is sent. A copy of the notice shall be sent to the other party.

## **8. Sub-processors**

Each party is obliged to enter into separate data processor agreements with any sub-processors that govern the sub-processors' processing of personal data on behalf of the respective controller in connection with this Agreement. All data processor agreements shall comply with all requirements pursuant to Article 28 of the GDPR and moreover forward all obligations which are necessary for the respective controller being able to comply with its obligations towards the other party.

Each party shall verify that its sub-processors comply with their contractual obligations, in particular that data security is satisfactory and that employees of the sub-processors are familiar with their obligations and fulfil them.

At the time of the execution of the Agreement, the parties agree on the use of data processors as specified in Appendix 1. Changes in the use of data processors must be approved in advance by the other party before new agreements are entered into. A copy of the data processing agreements entered into shall be submitted to the other party upon request.

## 9. Transfer of data to countries outside the EU/EEA

*Comment: If the Agreement entails that personal data may be transferred to countries outside the EU/EEA (third countries), such transfer may only take place on certain conditions. The rules for transfer to third countries are found in Articles 45-47 and 49 of the GDPR. These rules imply, among other things, that the transfer will be lawful if it takes place to EU-approved third countries, to American companies in the U.S. that have joined the Privacy Shield framework for the types of personal data covered by their Privacy Shield self-certification, or on the basis of the EU Commission's standard contractual clauses for transfer of personal data to third countries.*

*Include only if relevant:*

Personal data processed in accordance with this Agreement will be transferred to, or accessed from, the following recipient countries outside the EU/EEA:

..... (name of recipient country)

The legal basis for transferring personal data to the aforementioned recipient countries outside the EU/EEA is:

..... (brief explanation of the transfer basis)

## 10. Security audits

The parties will regularly implement security audits of their own work with safeguarding of personal data from unauthorized or unlawful access, alteration, erasure, damage, loss, or unavailability.

The parties shall carry out security audits of the information security in the organization. Security audits shall include the party's security objectives and security strategy, security organization, guidelines and procedures for security work, established technical, physical and organizational security measures and its sub-contractors work on information security. It shall also include routines for notification of joint controllers in the event of security breaches and routines for testing of contingency and continuity plans.

The parties shall document the security audits. On request, each of the controllers shall be given access to the other controller's audit reports.

If an independent third party conducts security audits at a party, the other party shall be informed of the auditor used and, upon request, be given access to summaries of such audit reports.

*Comment: The parties may agree that the respective data controller shall conduct the security audit at the other party, or how any costs incurred in connection with such an audit should be allocated. This can be set out here, or alternatively in the Main Agreement.*

## **11. Termination for breach**

In the event of a material breach of the terms of this Agreement caused by a party's errors or omissions, the other party may terminate the Agreement and the Main Agreement with immediate effect.

## **12. Compensation**

Each of the parties may require compensation for any financial loss suffered as a consequence of the other party's breach of its obligations under this Agreement. Compensation cannot be claimed for indirect losses. Indirect losses include, but are not limited to, lost profits, lost savings, losses due to data loss and third-party claims.

Aggregate liability per calendar year is limited to

*Comment: Choose suitable alternative depending on project/agreement:*

*Alternative 1:*

an amount equal to the aggregate annual remuneration under the Main Agreement excl. VAT.

*Alternative 2:*

a fixed amount of one million Norwegian kroner (1 MNOK).

The above limitations on liability do not apply in the event of gross negligence or willful misconduct.

## **13. Term of agreement**

This Agreement applies as long as the Main Agreement is in force and thereafter for as long as at least one of the parties still processes personal data which have its basis in the Main Agreement.

When all processing of the parties' respective processing of personal data under the Agreement has ceased, each of the parties is obliged to document to the other party that the relevant personal data have been deleted in accordance with Article 17 of the GDPR.

## **14. Contacts**

Contact person at [Name 1] for any questions related to this Agreement is: \_\_\_\_.

[Unit, position, contact information, address, telephone and email]

Contact person at [Name 2] for any questions related to this Agreement is: \_\_\_\_.

[Unit, position, contact information, address, telephone and email]

*[The following paragraph should be included if deemed appropriate between the parties (optional).  
Note that each of the parties is in any case responsible for complying with the rights of the data subjects upon requests from the data subjects, cf. section 4.]*

The contact point for the data subjects regarding the processing of personal data related to this Agreement shall be: \_\_\_\_\_.

*[Unit, position, contact information, address, telephone and email]*

## 15. Choice of Law and Legal Venue

*Comment: Choose the appropriate alternative depending on the contracting party:*

*Alternative 1 - applies when NTNU's contracting party is a private entity / non-governmental university or college:*

The Agreement is governed by Norwegian law. The parties agree on *[fill in name of district court]* as the agreed legal venue.

*Alternative 2 - applies when NTNU's contracting party is another governmental university or college:*

The Agreement is governed by Norwegian law. Any disputes arising out of this Agreement shall first be sought resolved through negotiation. If the parties do not reach agreement through negotiations, the dispute shall be resolved with binding effect by the Ministry of Education and Research. Either party may request that the dispute be forwarded to the Ministry.

\*\*\*

This Agreement is executed in two – 2 – copies, of which each party retains one copy each.

Place and date

.....

On behalf of *[Name 1]*

On behalf of *[Name 2]*

.....

.....

*(signature)*

*(signature)*

# APPENDIX 1 – SPECIFICATION OF DATA PROCESSING

## 1. Purpose

The purpose of the parties' processing of personal data under this Agreement is:

*Comment: Provide a clear description of the parties' purpose with the data processing. If the purpose is described in another agreement between the parties, include a reference to such an agreement.*

## 2. Types of personal data

The following types of personal data will be processed by the parties under this Agreement:

*Comment: Give a brief summary (preferably point by point) of the main categories of personal data that will be processed by the parties. Indicate whether they are sensitive and whether the data are directly identifiable or de-identified (i.e. whether the data appears to be anonymous, but it is actually possible to go back and find out who the data/information concerns).*

## 3. Categories of data subjects

The personal data which are processed under this Agreement concern the following categories of data subjects:

*Comment: Provide a brief summary of whom the information pertains to, for example, students and staff at the institution.*

## 4. Description of roles

[Name 1] will mainly have the following role and perform the following processing activities under the Agreement:

*Comment: Provide an overall description of the party's role in the data processing and the main types of processing activities it will perform.*

[Name 2] will mainly have the following role and perform the following processing activities under the Agreement:

*Comment: Provide an overall description of the party's role in the data processing and the main types of processing activities it will perform.*

## 5. Approved data processors

The parties have agreed that the following data processors may be used by the respective parties under the Agreement:



[Name 1]'s data processors:

*[List any approved data processors.]*

[Name 2]'s data processors:

*[List any approved data processors.]*