

Agreement between Data Processor and Sub-processor on processing personal data

Parties of the agreement:

Sikt — Norwegian Agency for Shared Services in Education and Research - 919 477 822
(Here on after referred to as the Customer or Data Processor)

and

<Enter the name and reg. no. of the Supplier>
(Here on after referred to as the Supplier or Sub-processor)

jointly referred to as the Parties.

Place and date:

The agreement is signed electronically

Contracting parties

For the Data Processor	For the Sub processor
<Name of the signatory on behalf of the Data Processor>	<Name of the signatory on behalf of the Sub-processor>
Signature	Signature

The Agreement is signed in duplicate, with each Party receiving one original.

TABLE OF CONTENTS:

1	Purpose of this Data Processing Agreement	3
2	Definitions.....	4
3	Rights and obligations of the Data Processor	4
4	Instructions from the Data Processor to the Sub-processor	4
5	Confidentiality and duty of secrecy.....	5
6	Assistance to the Data Processor	5
7	Security of processing.....	6
8	Notification of breach of personal data security	6
9	Use of Subprocessor	8
10	Transfer of personal data to countries outside the EEA	9
11	Audit.....	9
12	Erasure and return of information.....	10
13	Breach and suspension order	10
14	Duration and expiry	11
15	Governing law and legal venue	11

1 Purpose of this Data Processing Agreement

- 1.1 This Agreement (the “Data Processing Agreement”) sets out the Parties’ rights and obligations when the Supplier (Sub-processor) processes personal data on behalf of the Customer (Data Processor), as part the services delivered under the Main Agreement. The purpose of the Data Processing Agreement is to ensure that the Parties comply with the Applicable Privacy Regulation.

The Supplier accepts that it will process Personal Data as a Sub-Processor on behalf of the Customer (acting as the Data Processor), ultimately on behalf of the applicable Data Controller(s), and to comply with the terms of this Agreement when doing so.

The Data Processing Agreement comprises this document, as well as Appendices A, B, C and D.

In the event of conflict between the terms of the Main Agreement and the Data Processing Agreement, the terms of the Data Processing Agreement will take precedence regarding matters specifically related to the processing of personal data. In the event of any conflict between the Data Processing Agreement and its Appendices, the Appendices will take precedence.

In the event of a conflict, the terms of this agreement shall precede the privacy policy of the Supplier.

- 1.2 **Appendix A** of The Data Processing Agreement includes a detailed description of the processing that is to take place, as well as the purpose of processing, categories of personal data and data subjects, rules for erasure/deletion and return, and the Parties’ designated contact persons, as well as which underlying agreement(s) the processing of personal data is related to (see the definition of the Main Agreement below).
- 1.3 **Appendix B** of The Data Processing Agreement includes conditions for the use of Subprocessors, as well as a list of approved Subprocessors.
- 1.4 **Appendix C** of the Data Processing Agreement contains specific instructions for the processing of personal data under the Main Agreement, including security measures and the Customers’s right of access to and audit of the Supplier and any Subprocessors, as well as sector-specific provisions concerning the processing of personal data.
- 1.5 **Appendix D** of the Data Processing Agreement contains any subsequently agreed changes to the Data Processing Agreement.

2 Definitions

Applicable Privacy Regulation: The applicable versions of the EU's General Data Protection Regulation (2016/679) ("GDPR") and the Norwegian Act relating to the Processing of Personal Data of 15 June 2018 (the Personal Data Act) with related regulations etc., and any other relevant legislation concerning the processing and protection of personal data, as specified in Appendix C, section C.8.

Main Agreement: One or more agreements between the Data Processor and the Sub-processor concerning the provision of services which entail the processing of personal data, as specified in Appendix A. The Data Processing Agreement may apply to several underlying agreements.

Subprocessor: A company or person used by the Supplier as a subcontractor for the processing of personal data under the Main Agreement.

Article 4 of GDPR will apply to privacy terms not defined in this agreement.

3 Rights and obligations of the Data Processor

The Customer is responsible for the processing of personal data in accordance with Instructions from the Data Controller. The Customer must specifically ensure that:

- i. The Customer as a Data Processor has entered into adequate data processing agreements with its own customers (Data Controllers).
- ii. the Sub-processor at all times has, adequate instructions and information to fulfil its obligations under this Data Processing Agreement and the Applicable Privacy Regulation.

4 Instructions from the Data Processor to the Sub-processor

- 4.1 The Supplier shall process the personal data in accordance with the Applicable Privacy Regulation and the Customer's documented instructions, cf. section 4.2. If other processing is necessary to fulfil obligations to which the Supplier is subject under applicable law, the Sub-processor must notify the Customer to the extent this is permitted by law, cf. Article 28 (3) (a) of GDPR.
- 4.2 The Customer's instructions to the Supplier are stated in the Main Agreement and the Data Processing Agreement with Appendices. The Supplier must notify the Customer immediately if the Supplier believes the instructions conflict with the Applicable Privacy Regulation.
- 4.3 The Supplier must be notified of any changes to the instructions by updating Appendix D, and changes must be implemented by the Supplier by the date agreed between the Parties or, if no specific date has been agreed, within a reasonable time. The Supplier may require

the Customer to pay documented costs accrued in connection with the implementation of such changes, or the proportional adjustment of the remuneration under the Main Agreement if the amended instructions entail additional costs for the Supplier. The same applies to additional costs that accrue due to changes in the Applicable Privacy Regulation which concern the activities of the Customer or Data Controller.

5 Confidentiality and duty of secrecy

- 5.1 The Supplier must ensure that employees and other parties who have access to personal data are authorised to process personal data on behalf of the Supplier. If such authorisation expires or is withdrawn, access to the personal data must cease without undue delay.
- 5.2 The Supplier shall only authorise persons who need access to the personal data in order to fulfil their obligations under the Main Agreement, the Data Processing Agreement and any other processing that is necessary to fulfil obligations to which the Supplier is subject, in accordance with applicable law, see section 4.1, last sentence.
- 5.3 The Supplier must ensure that persons authorized to process personal data on behalf of the Customer are subject to obligations of confidentiality either by agreement or applicable law. The obligations of confidentiality shall survive the duration of the Data Processing Agreement and/or employment relationship.
- 5.4 At the request of the Customer, the Supplier shall document that the relevant persons are subject to said obligations of confidentiality, see section 5.3.
- 5.5 Upon the expiry of the Data Processing Agreement, the Supplier is required to discontinue all access to personal data that is processed under the agreement.

6 Assistance to the Data Processor

- 6.1 When requested, the Supplier shall assist the Customer, acting on behalf of the Data Controller, with the fulfilment of the rights of the data subjects under Chapter III of the GDPR through appropriate technical or organisational measures. The obligation to assist the Customer solely applies insofar as this is possible and appropriate, taking into consideration the nature and extent of the processing of personal data under the Main Agreement.
- 6.2 Without undue delay, the Supplier shall forward all enquiries that the Supplier may receive from the data subject concerning the rights of said data subject under the Applicable Privacy Regulation to the Customer. Such enquiries may only be answered by the Supplier when this has been approved in writing by the Customer on behalf of the Data Controller.
- 6.3 The Supplier must assist the Customer and the Data Controller in ensuring compliance with the obligations pursuant to Articles 32-36 of GDPR, including providing assistance with

personal data impact assessments and prior consultations with the Norwegian Data Protection Authority, in view of the nature and extent of the processing of personal data under the Main Agreement.

- 6.4 If the Supplier, at the request of the Customer, provides assistance as described in sections 6.1 or 6.3, and the assistance goes beyond what is necessary for the Data Processor to fulfil its own obligations under the Applicable Privacy Regulation, the Supplier may claim documented costs related to the assistance be reimbursed. The assistance will be reimbursed in accordance with the price provisions of the Main Agreement. In order to claim reimbursement the Supplier must notify the Customer that the costs related to this assistance will be subject to reimbursement prior to the assistance.

7 Security of processing

- 7.1 The Supplier shall implement the appropriate technical and organisational measures to ensure a level of security appropriate to the risk, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. The Supplier must, as a minimum, apply the measures specified in Appendix C of the Data Processing Agreement.
- 7.2 The Supplier shall carry out risk assessments to ensure that an appropriate security level is maintained at all times. The Supplier must ensure regular testing, analysis and assessment of the security measures, in particular with regard to ensuring sustained confidentiality, integrity, availability and robustness in processing systems and services, and the ability to quickly restore the availability of personal data in the event of an incident.
- 7.3 The Supplier must document the risk assessment and security measures and make them available to the Customer on request, and also allow for the audits agreed between the Parties, cf. section **Feil! Fant ikke referansekilden.** of the Data Processing Agreement.

8 Notification of breach of personal data security

- 8.1 In case of a personal data breach, the Supplier shall without undue delay and, where feasible, not later than 36 hours after having become aware of it, notify the Customer in writing of the breach, and in addition provide the assistance and information necessary for the Customer to be able to report the breach to the Data Controller and supervisory authorities in line with the Applicable Privacy Regulation.
- 8.2 Notification in accordance with section 8.1 must be given to the Customers's point of contact in accordance with Appendix C, section C.9, and must:

-
- a. describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned, and the categories of and approximate number of personal data records concerned
 - b. state the name and contact details of the data protection officer or other contact point from where more information can be obtained
 - c. describe the likely consequences of the personal data breach; and
 - d. describe the measures taken or proposed by the Customer to address the breach, including where appropriate, measures to mitigate possible adverse effects.

If necessary, information may be given in phases without any further undue delay.

- 8.3 The Supplier shall implement all necessary measures that may reasonably be required to rectify and avoid similar personal data breaches. As far as possible, the Supplier must consult the Customer concerning the measures to be taken, including assessment of any measures proposed by the Customer.
- 8.4 The Customer is responsible for notifying the Data Controller and Data Protection Authority (if instructed by the Data Controller to do so). The Data Controller is responsible for notifying the data subjects affected by the personal data breach. The Supplier may not inform third parties of any breach of personal data security unless otherwise required under applicable law or in accordance with the express written instructions of the Customer on behalf of the Data Controller.

9 Use of Subprocessors

- 9.1 The Supplier may only use Subprocessors with the prior general or specific written authorisation of the Customer, in accordance with Appendix B of the Data Processing Agreement. For an overview of approved Subprocessors, see Appendix B of the Data Processing Agreement.
- 9.2 If the Supplier engages a Subprocessor for carrying out specific processing activities on behalf of the Customer and the Data Controller, the same data protection obligations as set out in this Data Processing Agreement shall be imposed on the Subprocessor by way of written agreement. See section 9.7 concerning the use of standard third-party services.
- 9.3 The Supplier may only engage Subprocessors who provide appropriate technical and organisational measures to ensure that the processing fulfils the requirements in accordance with the Applicable Privacy Regulation. The Supplier must assess and verify that satisfactory measures have been taken by the Subprocessors. Upon request, the Supplier must be able to submit reports from such assessments to the Customer.
- 9.4 If the Customer objects to changes in the use of Subprocessors pursuant to Appendix B, section B.1 of the Data Processing Agreement, the Parties must negotiate in good faith with the aim of reaching a reasonable solution to how the further delivery of the services under the Main Agreement is to take place, including the distribution of any costs between the Parties. The parties must reach an agreement before changes in the use of Subprocessors can be made.
- 9.5 If the Subprocessor fails to fulfil its data protection obligations, the Supplier shall remain liable to the Customer for the performance of the Subprocessor's obligations in the same way as if the Supplier was responsible for the processing.
- 9.6 The Supplier is obligated, on request, to disclose agreements with Subprocessors to the Customer. This solely applies to the parts of the agreement that are relevant to the processing of personal data, and subject to any statutory or regulatory limitations. Commercial terms and conditions are not required to be submitted.
- 9.7 If the Supplier uses a subcontractor that provides standardised third-party services, the Parties may agree that the subcontractor's standard data processing agreement will be used and applied directly to the Data Processor as in a direct data processing relationship (i.e., not as a Subprocessor) under the following terms:
- The Customer must expressly accept under the Main Agreement that the standardised third-party services are provided on the subcontractor's standard terms
 - The Supplier must follow up on the standard terms on behalf of the Customer

-
- The standard terms must fulfil the requirements in the Applicable Privacy Regulation.

The Supplier must follow up the data processing agreement with the subcontractor on behalf of the Customer, unless otherwise agreed in each individual case.

10 Transfer of personal data to countries outside the EEA

10.1 Personal data may only be transferred to a country outside the EEA ('Third country') or to an international organisation if the Customer has approved such transfer in writing and the terms in section 10.3 are fulfilled. Transfer includes, but is not limited to:

- a) processing of personal data in data centres, etc. located in a Third Country, or by personnel located in a Third Country (by remote access)
- b) assigning the processing of personal data to a Subprocessor in a Third State; or
- c) disclosing the personal data to a Data Controller or a Data Processor in a Third Country, or in an international organisation.

10.2 The Supplier may nonetheless transfer personal data if this is required by applicable law in the EEA area. In such cases, the Supplier must notify the Customer, to the extent permitted by law.

10.3 Transfer to Third Countries or international organisations may only take place if there are necessary guarantees of an adequate level of data protection in accordance with the Applicable Privacy Regulation. Unless otherwise agreed between the Parties, such transfer may only take place on the following grounds:

- a) a decision of the European Commission concerning an adequate level of protection in accordance with Article 45 of GDPR; or
- b) standard personal data protection provisions as specified in Article 46 (2) (c) or (d) of the GDPR (EU model clauses), provided the conditions for the use of those standard contractual clauses are met ; or
- c) binding corporate rules in accordance with Article 47 of GDPR.

10.4 Any approval by the Customer for the transfer of personal data to a Third Country or international organisation must be stated in Appendix C, section C.5.

11 Audit

11.1 Upon request, the Supplier shall make available to the Customer all information necessary to demonstrate compliance with the obligations laid down in Article 28 of the GDPR and this Data Processing Agreement.

11.2 The Supplier shall allow and contribute to inspections and audits carried out by or on behalf of the Customer. The Supplier shall also allow and contribute to inspections conducted by

relevant supervisory authorities. The Customers's review of any Subprocessor shall be conducted by the Supplier, unless otherwise specifically agreed. Specific procedures for conducting audits are stated in Appendix C, section C.5.

- 11.3 If an audit reveals a breach in the obligations in the Applicable Privacy Regulation or the Data Processing Agreement, the Supplier must rectify the breach as soon as possible. The Customer may require the Supplier to temporarily stop all or part of the processing activities until the breach has been rectified and approved by the Customer.
- 11.4 Each Party shall pay its own costs associated with an annual audit. If an audit reveals significant breaches of the obligations under the Applicable Privacy Regulation or the Data Processing Agreement, the Supplier shall pay for the Customers's reasonable costs accrued from the audit.

12 Erasure and return of information

- 12.1 Upon the expiry of this Data Processing Agreement, the Supplier is obligated to return and erase all personal data processed on behalf of the Customer under the Data Processing Agreement, in accordance with the provisions of Appendix C, section C.6. This also applies to any back-up copies.
- 12.2 The Customer will determine how any return of personal data is to take place. The Customer may require return to take place in a structured and commonly used machine-readable format. The Customer will pay the Suppliers's documented costs associated with the return if this is included in the remuneration under the Main Agreement.
- 12.3 If a shared infrastructure or back-up is used and direct erasure is not technically possible, the Supplier must ensure that the personal data is made inaccessible until it has been overwritten.
- 12.4 The Supplier must confirm in writing to the Customer that the data has been erased or made inaccessible, and shall, upon request document how this has taken place.
- 12.5 Further provisions concerning erasure and return are stated in Appendix C.

13 Breach and suspension order

- 13.1 In the event of breach of the Data Processing Agreement and/or Applicable Privacy Regulation, the Customer and relevant supervisory authorities may order the Supplier to cease all or part of the processing of the data effective immediately.
- 13.2 If the Supplier fails to comply with its obligations pursuant to this Data Processing Agreement and/or Applicable Privacy Regulation, this shall be deemed a breach of the Main

Agreement, and the obligations, deadlines, sanctions and limitations of liability in the Main Agreement's regulation of the Supplier's breach will be applied, unless otherwise expressly agreed between the Parties in Appendix D.

14 Duration and expiry

- 14.1 The Data Processing Agreement will come into effect from the date it is signed by both Parties. The Data Processing Agreement shall apply for as long as the Supplier processes personal data on behalf of the Customer. It shall also apply to any personal data held by the Supplier or any of its Subprocessors after the expiry of the Main Agreement.
- 14.2 The rules concerning termination specified in the Main Agreement shall also apply to the Data Processing Agreement, to the extent this is applicable. The Data Processing Agreement may not be terminated if the Main Agreement is in effect unless it is replaced by a new Data Processing Agreement.

15 Governing law and legal venue

The Data Processing Agreement is governed by Norwegian law. Disputes will be resolved in accordance with the provisions of the Main Agreement, including any provisions concerning legal venue.

.....