Felleskjøpet

DATA PROCESSING AGREEMENT

Versjon 2. Sist revidert 28.12.2022

Table of Content

Guidance:

GDPR is short for *The General Data Protection Regulation*.
The Processor is the part which process personal data on behalf of the Controller. This is usually an enterprise.
The Controller is the part which decides the purpose of processing the personal data and which tools to be used. This is usually an enterprise.

The red text marked in brackets [Alt 1] is to be edited related to the agreement.
Appendix 1-3 to be filled in when needed related to the agreement.

1. Filled in by the Controller, usually the customer
2. Filled in by the Processor, usually the supplier
3. Filled in by the Processor, usually the supplier

https://www.datatilsynet.no/
https://lovdata.no/dokument/NL/lov/2018-06-15-38

1. BACKGROUND AND PURPOSE

1.1 This data processing appendix (the “**Data Processing Agreement**”) forms part of [insert name of main agreement] dated [insert date] (the "**Main Agreement**") between [name] (the "**Controller**") and name (the "**Processor**"), each a "**Party**" and jointly the "**Parties**". This Data Processing Agreement also applies for processing of personal data that the Processor carries out on behalf of [name] pursuant to section 12.

1.2 The purpose of this Data Processing Agreement is to set out the rights and obligations of the Parties concerning the data processing operations carried out by the Processor on behalf of the Controller under the Main Agreement.

1.3 [**Alt**]This Data Processing Agreement supersedes any previous agreements or clauses between the Parties specifically concerning data protection.

1.4 Except as modified herein, the terms and conditions of the Main Agreement remains in full force and effect. [**Alt1**]In the event of inconsistency between the Main Agreement and this Data Processing Agreement on matters specifically concerning data protection, the latter shall prevail. [**Alt2**]In the event of inconsistency between the Main Agreement and this Data Processing Agreement, the former shall prevail.

2. DEFINITIONS

2.1 In this Data Processing Agreement, the following terms shall have the meanings set out below.

2.2 "**Applicable data protection law**": Applicable data protection and privacy law, including but not limited to the Norwegian Personal Data Act and the GDPR (as from 25 May 2018).

2.3 "**GDPR**": The EU General Data Protection Regulation 2016/679.

2.4 "**Standard contractual clauses**": EU Commission Standard Contractual Clauses (or SCCs) 2021/914 (ec.europa.eu).

2.5 "**Sub-processor**": Another processor engaged by the Processor.

2.6 "**Third-country**": A country outside the EEA that the EU Commission has not approved as offering an adequate level of data protection.

2.7 Other terms shall have the meaning as defined in the GDPR.

3. SCOPE

3.1 This Data Processing Agreement applies to any personal data that the Processor has received, is given access to, or has generated in connection with the Main Agreement.in connection with the Main Agreement.

3.2 [**Alt**]The subject-matter of this Data Processing Agreement shall, to the extent relevant, also include the processing of non-personal data to which the Processor has received, is given access to, or has generated in connection with the Main Agreement. Accordingly, the term "personal data" shall, to the extent relevant also be understood as non-personal data.

3.3 The nature and the purpose of the processing of personal data, the type of personal data, and the categories of data subjects, are set out in Annex 1.

4. GENERAL OBLIGATIONS

4.1 The Controller is responsible for all personal data being processed in accordance with applicable data protection law.

4.2 The Controller decides the purpose of the processing of the personal data and which tools to be used.

4.3 The Processor warrants it has implemented and will maintain throughout the term appropriate technical and organisational measures in such a manner that the processing will meet the requirements of applicable data protection law and ensure the protection of the rights of the data subject.

4.4 The Processor shall process the personal data solely for the purpose and within the scope as set out in Annex 1, and otherwise in accordance with the Controller's documented instructions.

4.5 The Processor shall immediately inform the Controller in writing if, in its reasonable opinion, (i) an instruction from the Controller will cause the Processor to infringe applicable data protection law, or (ii) a legal requirement laid down by law in a EEA country requires the Processor to process personal data beyond the scope of the Controller's documented instructions, unless that law prohibits such information on important grounds of public interest (if so, the Processor shall inform the Controller as soon as permitted by law). In the event of (i) or (ii), the Parties shall in good faith discuss how to solve the issue without adversely affecting the protection of the rights of the data subjects.

4.6 If the Processor is subject to an approved code of conduct as referred to in Article 40 of the GDPR or an approved certification mechanism as referred to in Article 42 of the GDPR, the Processor warrants that it will adhere such code or mechanism.

5. ASSISTANCE TO THE CONTROLLER

5.1 The Processor shall assist the Controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to and comply with requests for exercising the data subject's rights laid down in chapter III of the GDPR, including requests for information, access, rectification, erasure, restriction, data portability, objection, and not to be subject to automated individual decision-making.

5.2 Taking into account the nature of processing and the information available to the processor, the Processor shall assist the Controller with the obligations pursuant to Article 32 to 36 of the GDPR, including the obligations of data security (as further described in clause 6), personal data breach notification (as further described in clause 9), data protection impact assessments, and prior consultation.

5.3 The Processor shall not engage in direct communication with data subjects or supervisory authorities unless approved in advance by the Controller. The Processor shall promptly forward to the Controller any request or complaint received from a data subject. Moreover, the Processor shall promptly forward any request from a supervisory authority requiring inspections, investigations, access to, or information regarding personal data, unless prohibited by law (if so, the Processor shall inform the Controller as soon as permitted by law).

6. TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

6.1 The Processor shall implement and maintain throughout the term appropriate technical and organisational data security measures to protect the personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access. As a minimum, the Processor shall take all those measures as required pursuant to Article 32 of the GDPR, and all those measures set out in or referred to in Annex 2.

6.2 The Processor shall not disclose or make available the personal data to any third party except with the prior written approval of the Controller, and except to any approved sub-processors on a need-to-know basis.

6.3 The Processor shall ensure that only authorized persons have access to the personal data and that the Processor deprives the access if the authorisation expires or for any other reason no longer applies to the person. The Processor shall only authorize persons who, for the necessary reasons, must have access to the personal data.

The Processor shall ensure that all persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. At the Controller's request, the Processor shall provide the Controller with a copy of confidentiality undertakings signed by such persons. The confidentiality obligations also apply after the data processing assignment is completed.

7. USE OF SUB-PROCESSORS

7.1 [**Alt 1**]The Processor may only engage a sub-processor with the specific written authorisation of the Controller. Authorised sub-processors, if any, are listed in Annex 3. [**Alt 2**]The Controller authorises the Processor to engage sub-processors. Upon the Controller's request, the Processor shall provide information about the identity of each sub-processor and their processing locations. The Processor shall inform the Controller of any intended changes concerning the addition or replacement of sub-processors and allow the Controller to object to such changes or to require termination of this Data Processing Agreement following the change.

7.2 Subject to clause 7.1, the Processor shall only engage sub-processors that has implemented and will maintain throughout the term appropriate technical and organisational measures in such a manner that the processing will meet the requirements of applicable data protection law and ensure the protection of the rights of the data subject. The Processor shall perform appropriate audits of the sub-processors to verify their level of data protection. The Processor shall make available to the Controller reports of such audits.

7.3 Sub-processing shall only be done by way of a written agreement with the sub-processor which imposes appropriate data protection obligations on the sub-processor. Where the sub-processor is engaged for carrying out specific processing activities on behalf of the Controller, the Processor shall by way of a written agreement impose on the sub-processor the same data protection obligations as set out in this Data Processing Agreement. At the Controller's request, the Processor shall provide the Controller with a copy of such written agreements with sub-processors, however commercial and other business sensitive information may be redacted.

7.4 The Processor remains fully liable to the Controller for the performance of the sub-processors' obligations.

8. INTERNATIONAL DATA TRANSFER

8.1 The Processor may only transfer personal data to a third country or an international organisation with a written authorisation of the Controller. Prior to any international data transfer, the Processor shall ensure and document that the level of data protection is essentially equivalent to the data protection provided by the GDPR. If necessary, the Processor shall implement supplementary measures to ensure an adequate level of data protection. The Processor may however transfer personal data to a third country or an international organisation if required by applicable law in the EEA; in such a case, the Processor shall inform the Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest (if so, the Processor shall inform the Controller as soon as permitted by law).

8.2 If the use of an approved sub-processor requires the transfer of personal data to a third country, and such transfer is approved by the Controller, the Controller empowers the Processor, in the name of and on behalf of the Controller, to enter into the standard contractual clauses in un-amended form with such sub-processor, if required to satisfy the requirements of applicable data protection law. Once concluded, the Subcontractor shall provide a copy thereof to the Controller. Any such standard contractual clauses shall automatically terminate upon the termination of this Data Protection Agreement.

9. PERSONAL DATA BREACHES

9.1 In the event of breach of this Data Processing Agreement or a personal data breach, the Processor shall promptly, and no later than 36 hours after becoming aware of it, notify the Controller in writing about the breach.

9.2 The notification of a personal data breach must, to the extent relevant, at least:

a. describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

b. if possible, the identities of the affected data subjects;

c. communicate the name and contact details of the data protection officer or other contact point of the Processor where more information may be obtained;

d. describe the likely consequences of the personal data breach;

e. describe the measures taken or proposed to be taken to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects;

f. include other information required for the Controller to comply with applicable data protection law.

9.3 The Processor shall without undue delay take all those measures described in e. above, as well as to take all those measures reasonably required for the purpose of avoiding the re-occurrence of similar personal data breaches. Without limiting the Processor's obligations, the Processor shall allow the Controller to investigate, determine the cause of, and to verify the measures taken or proposed by the Processor to address the personal data breach. The Processor shall, insofar as this is possible, consult with the Controller with respect to the measures to be taken and take due consideration to any reasonable input that the Controller may have.

9.4 The Controller is solely entitled to notify the relevant supervisory authority and the data subjects about a personal data breach. The Processor shall refrain from communicating about a personal data breach to the public or any third party.

10. AUDITS

10.1 The Processor shall maintain necessary records and make available to the Controller all information necessary to demonstrate compliance with this Data Processing Agreement and applicable data protection law.

10.2 The Processor shall allow for and contribute to audits of the Processor's processing operations conducted by the Controller or another auditor mandated by the Controller. The Processor shall also allow for and contribute to such audits by a supervisory authority.

10.3 The Processor shall, by itself or by another auditor mandated by the Processor, perform regular audits of its processing operations. The Processor shall provide a copy of audit reports resulting from such audits to the Controller. The Controller shall be entitled to disclose such reports to its auditors and to supervisory authorities.

10.4 The Processor shall promptly notify the Controller if it receives a request from an authority for disclosure of personal data processed under this Data Protection Agreement. Unless required by law, the Processor shall not comply with such request without the prior written approval of the Controller.

10.5 If an audit reveals deviations from the obligations set out in this Data Processing Agreement, the Processor shall (and, if relevant, shall procure that the relevant sub-processor shall) without undue delay remedy such deviation. The Controller may require whole or parts of the processing activities to temporarily cease until successful remedy is confirmed.

10.6 A party shall cover its own costs associated with an audit. However, if an audit reveals deviations from the obligations set out in this Data Processing Agreement, and such deviations are not insignificant, all costs of the audit shall be borne by the Processor, including reasonable costs of the Controller and another auditor mandated by the Controller.

11. INDEMNIFICATION

11.1 The Processor shall indemnify and hold harmless the Controller from and against any costs (including reasonable legal costs) and losses caused by a claim by a third party (including supervisory authorities and data subjects) that the processing of personal data involves a breach of applicable data protection law, and the claim is caused by the Processor's breach of its obligations under this Data Processing Agreement, including processing of personal data beyond the Controller's written instructions.

11.2 The indemnification is contingent upon (i) that the Controller promptly notifies the Processor of the claim, and (ii) the Processor is given the possibility to cooperate with the Controller in the defence and settlement of the claim.

12. [ALT.] OTHER CONTROLLERS

12.1 The Processor acknowledges that the personal data is also processed on behalf of the Controller's affiliates/customers/clients. [or insert name of relevant company] Such other controllers may enforce this Data Processing Agreement as if they were a contracting party to it, however the enforcement shall be made through the Controller that is the contracting party.

12.2 The Controller may forward any instruction from such other controllers, and the Processor shall act in accordance to such instruction as if they were the Controller's own instructions.

12.3 The Controller may forward any documentation and information received by the Processor to such other controllers.

13. TERM AND TERMINATION

13.1 This Data Processing Agreement will remain in force as long as the Processor processes personal data on behalf of the Controller under the Main Agreement.

13.2 The Controller has the right to terminate this Data Processing Agreement if the Processor no longer meets the requirements of Article 28 of the GDPR.

13.3 Upon expiry or termination, the Processor shall, at the choice of the Controller, delete or return all personal data to the Controller, and delete any copies thereof and certify to the Controller that it has done so, unless applicable law in the EEA requires the Processor to store the personal data (if so, the Processor will securely store, but not actively process, the personal data, and will delete the personal data once permitted by law).

For and behalf of the Controller:

Signature: ___________________________

Name:

Date:

For and behalf of the Processor:

Signature: ___________________________

Name:

Date:

ANNEX 1: SCOPE OF THE PROCESSING

Guidance:

Personal data means any information relating to an identified or identifiable natural person. "Any information" must be understood very broadly and contain no limitations as to the nature, content or form. Personal data can be conveyed through text, numbers, images, video, audio recordings, or any other kind of information production. The information must regard a natural person. It is not a requirement that the person must be identified - it is sufficient that it is possible to identify the person.

The name of the sole proprietorships may be personal data.

Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, deletion or destruction.

The description of the processing

Insert a detailed description of the processing. Specifically describe what you as the Processor will actually do.

Purpose of the processing

Insert. The purpose of the processing is for the Processor to perform its obligations pursuant to the Main Agreement.

Nature and subject matter of the processing

Insert description or insert reference to relevant parts of the Main Agreement or annexes to the Main Agreement. Example may be *hosting of data on a cloud-based platform*.

Categories of data subjects

Insert.

Examples: Current, former and potential employees of the Controller; current, former and potential employees of the Controller's customers

Categories of personal data

Insert.

Examples: Name, sex, date of birth, phone number, address, email address (such as name.surname@company.com), position, employee ID, salary, education and other professional qualifications, nature and details of current and historic pension arrangements pension amounts, pension contributions, employee benefits, marital status, beneficiary details, bank details, an identification card number, national insurance number and/or ill-health status, credit information, relationships with governmental authorities and officials, immediate family members, information received through searches in public sources and discussions/interviews; transactions, an Internet Protocol (IP) address, behaviour details (incl. e.g. URLs visited, events triggered on defined actions such as page loads, clicks, logins and purchases); geo-location data.

Special categories of personal data (if relevant)

Insert.

Also called sensitive personal data. Personal data that requires additional protection, such as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, data concerning health, sexual orientation, and more.

ANNEX 2: TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

Guidance:

The Processor shall, as a minimum, take all those measures set out in or referred to below. Without the Controller's written approval, the Processor may not do changes to such measures that reduces the level of data security. The Processor shall continuously work to improve its data security measures and to keep it up-to-date with technological developments.

Alt 1: Insert reference to Data Security Policy

Alt 2:

Pseudonymisation measures

Pseudonymisation means processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

Insert description of pseudonymisation measures, if any.

Encryption measures

Encryption is the process of encoding data in such a way that only an authorized party can access the data. *The following personal data is recommended to encrypt, cf. Article 32 of the GDPR: Special categories of personal data (sensitive personal data), national identity number, personal data of many, personal data that the Controller has classified as worthy of protection.*

Insert description of encryption measures, if any.

Measures to ensure the confidentiality of personal data

Insert description. Example may be measures for access control, and for segregation of the data from data that the Processor processes on behalf of other controllers.

Measures to ensure integrity of the personal data

Insert description. Example may be measures for monitoring changes to data.

Measures to ensure availability of the personal data

Insert description. Example may be back-up measures.

Measures to ensure resilience of processing systems and services

Insert description. Example may be measures for disaster-recovery and redundancy.

Other data security measures:

Insert description, or "N/A".

ANNEX 3: APPROVED SUB-PROCESSORS

Guidance:

Processing often involves several participants. In such cases, when the Processor wants to use sub-processors, the Controller shall have control over the data flow and the participants. The Processor shall obtain prior permission from the Controller to engage another processor.

The Processor has full responsibility towards the Controller for its sub-processors, and the sub-processors shall under separate agreement be subject to the same obligations as under this Data Processing Agreement.

Company name	Company address	Processing location