Direktoratet for
e-helse

Version: December 2020

Standard Data Processing Agreement for the Health and Care Services Sector

[for processing personal health data]

Pursuant to the Norwegian Personal Data Act and

the EU's General Data Protection Regulation (GDPR) 2016/679

between

[Name of organisation]

Organisation no.: 000 000 000

Controller

and

[Name of organisation]

Organisation no.: 000 000 000

Processor

This data processing agreement is linked to the following service/assignment agreement between the parties:

Title of service/assignment agreement	Date of service/assignment agreement	Case reference for service/assignment agreement
Insert	Insert	Insert

The data processing agreement has been signed in two copies, one to each of the parties.

Place and date:

[*Place*], xx.xx.20xx

For the Controller	For the Processor
Name: Insert	Name: Insert

Signature: ________________________________	Signature: ________________________________

Contents

1. ABOUT THE AGREEMENT 3

2. DEFINITIONS 3

3. PURPOSE OF THE AGREEMENT 4

4. SCOPE 4

5. PURPOSE OF THE PROCESSING, DATA AND PROCESSING ACTIVITIES 4

6. FRAMEWORK FOR THE PROCESSING OF PERSONAL HEALTH DATA 4

7. THE CONTROLLER'S OBLIGATIONS 4

8. THE PROCESSOR'S OBLIGATIONS 5

9. USE OF SUBCONTRACTORS 7

10. TRANSFER OF PERSONAL DATA TO OTHER COUNTRIES 8

11. OBLIGATIONS OF SECRECY 9

12. AUDITS 9

13. DURATION AND TERMINATION 10

14. AMENDMENTS TO THE AGREEMENT 10

15. GOVERNING LAW, DISPUTES AND VENUE 11

APPENDIX 1 – PURPOSE OF THE PROCESSING, DATA AND PROCESSING ACTIVITIES 12

APPENDIX 2 – DETAILED REQUIREMENTS CONCERNING INFORMATION SECURITY 14

APPENDIX 3 ADMINISTRATIVE PROVISIONS 15

APPENDIX 4 – SUBCONTRACTORS 16

APPENDIX 5: AMENDMENTS TO THE GENERAL TEXT OF THE AGREEMENT UPON ENTERING INTO THE AGREEMENT 17

APPENDIX 6: AMENDMENTS AFTER THE AGREEMENT HAS BEEN ENTERED INTO 18

1. About the agreement

This data processing agreement with appendices (hereinafter “the Agreement”) regulates rights and obligations between the Controller and Processor (hereinafter “the parties”) pursuant to:

- Act no. 38 of 15 June 2018 relating to the processing of personal data (the Personal Data Act);
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereinafter “the General Data Protection Regulation”);
- Act No. 43 of 20 June 2014 relating to health data filing systems and the processing of health data filing systems (Personal Health Data Filing System Act);
- Act No. 42 of 20 June 2014 relating to the processing of health data in connection with the provision of medical care (Patient Records Act); and
- Any law, regulation or other provisions which amend or supersede the aforementioned rules.

In the event of a conflict between the provisions of the Agreement and the framework that follows from data protection regulations or relevant health legislation, the provisions of the Agreement shall cede precedence. In the event of a conflict between this Agreement and the Service/assignment agreement, this Agreement shall take precedence.

Appendices to the agreement:

- Appendix 1: Purpose of the processing, data and processing activities
- Appendix 2: Detailed requirements concerning information security
- Appendix 3: Administrative provisions
- Appendix 4: Subcontractors
- Appendix 5: Amendments to the general text of the agreement upon entering into the agreement
- Appendix 6: Amendments after the agreement has been entered into

Amendments to the general text of the agreement must be collated in Appendix 5. Such amendments replace the original text of the agreement.

2. Definitions

The terms “personal data”, “personal health data”, “processing”, “controller”, “processor”, and “personal data breach” shall be understood as they are defined in Article 4 of the General Data Protection Regulation, Section 2 of the Personal Health Data Filing System Act and Section 2 of the Patient Records Act.

3. Purpose of the Agreement

The purpose of the Agreement is to safeguard the rights of data subjects and ensure the parties' compliance with Article 28 (3) of the General Data Protection Regulation.

4. Scope

This Agreement shall apply to all processing of personal health data which the Processor carries out on behalf of the Controller in accordance with the Service/assignment agreement.

This Agreement shall also apply to other processing of personal health data based on any written agreements between the parties which are entered into between the parties during the duration of the Agreement and which entail the Processor processing personal health data on behalf of the Controller (hereinafter “subsequent written agreements between the parties"). Any such additions must be specified in **Appendix 6**. The other appendices to the Agreement shall be updated in accordance with the amendment.

5. Purpose of the processing, data and processing activities

The purpose and duration of the processing of personal health data, the scope of the personal health data that are processed, categories of data subjects and the nature of the processing activities are set out in **Appendix 1.**

6. Framework for the processing of personal health data

The Controller shall have complete control at all times over the personal health data that the Processor processes pursuant to this Agreement. The Processor shall not have any independent right of use with regard to the personal health data and shall not be entitled to process such data for its own purposes.

Unless otherwise agreed or stipulated by law, the Controller shall have the right to access and inspect the personal health data that is processed by the Processor.

7. The Controller’s obligations

The Controller shall fulfil the obligations that are stipulated in the data protection rules, cf. Article 24 of the General Data Protection Regulation, relevant health legislation and other special legislation, as well as this Agreement.

The Controller is responsible for compliance with the data protection principles, cf. Article 5 of the General Data Protection Regulation, and shall, among other things, ensure that the processing of data is specific to the intended purpose and has a valid legal basis.

8. The Processor's obligations

8.1. General

The Processor undertakes to only process personal health data in accordance with applicable regulations, this Agreement, the Service/assignment agreement, the Controller's documented instructions and other applicable agreements between the parties, as well as the "Code of conduct for information security and data protection in the healthcare and care services sector". The Processor shall not, through any act or omission, place the Controller in a situation which entails that the Controller is in breach of applicable regulations as specified in clause 1 of the Agreement.

8.1.1 The Processor shall not:

a. process personal health data for any purposes or to any greater extent or in any other manner than as specified in this Agreement, the Service/assignment agreement and any subsequent written agreements between the parties;
b. process personal health data over and above that which is necessary in order to fulfil the Processor's obligations in accordance with the agreements applicable at any one time;
c. disclose, hand over, transfer or obtain personal health data in any form to or from a third party at the Processor's own initiative, unless there is a statutory obligation or prior agreement with the Controller or with the written consent of the Controller;

8.1.2 The Processor shall:

a. maintain ongoing control over all categories of processing activities that are carried out on behalf of the Controller, cf. Article 30 (2) of the General Data Protection Regulation, 2, cf. also **Appendix 1**;
b. grant the Controller access to personal health data which are processed by the Processor on behalf of the Controller;
c. take all reasonable measures to assist the Controller with ensuring that the personal health data are accurate and updated at all times;
d. establish routines to erase data in accordance with instructions and guidelines stipulated by the Controller;
e. ensure that all persons who are granted access to personal data processed on behalf of the Controller are familiar with this Agreement and applicable agreements between the parties, and are subject to the provisions of these agreements;
f. provide the Controller with the necessary assistance to enable the Controller to fulfil its obligations with respect to the data subjects, including responding to requests from the data subjects that will exercise their rights as set out in Chapter III of the General Data Protection Regulation;
g. notify the Controller without undue delay if the Processor believes that any instructions are in breach of the General Data Protection Regulation or other provisions concerning the protection of personal data;
h. assist the Controller in ensuring compliance with the obligations of Articles 35-36 of the General Data Protection Regulation, which concern the assessment of data

protection consequences and advance discussions with the Norwegian Data Protection Authority.

i. The Processor must immediately notify the Controller if it receives a request from an authority to disclose personal data processed under the Data Processing Agreement. Unless disclosure is required by law, the Processor shall not comply with such a request without the prior written consent of the Controller.

8.2. Technical, organisational and security measures

The Processor undertakes to identify and implement all technical, organisational and security measures to ensure that there is a level of security in place at all times that is suitable when considering the risk associated with processing personal health data.

At a minimum, the Processor shall:

a. establish and comply with all necessary technical and organisational measures with regard to ensuring confidentiality, integrity, accessibility and robustness in connection with the processing of personal health data to ensure satisfactory information security in accordance with the data protection regulations, including the requirements under Article 32 of the General Data Protection Regulation, and applicable health legislation.

b. ensure that requirements concerning built-in data protection and data protection as a default arrangement are fulfilled in the Processor's solutions. This includes building in functionality in order to fulfil data protection principles and functionality in order to safeguard the rights of the data subject, including the right to restricted processing;

c. have routines for internal control;

d. have routines for authorisation and control which ensure that only the Processor's employees who have an official need for access to systems and the data in order to perform essential tasks for the fulfilment of the Service/assignment agreement are able to gain such access. The level of access shall be in accordance with an official need linked to implementation of the assignment. Strong authentication shall be established for access to personal health data;

e. establish systems and routines as necessary to safeguard information security and follow up breaches, including routines for reporting breaches, back-up routines, restoring normal status, eliminating the cause of breaches and preventing reoccurrence. Upon request, the Processor shall grant the Controller access to relevant security documentation used to process personal health data;

f. detect, register, report and close breaches linked to information security, including logging and documenting any attempts at unauthorised access and other breaches of personal data in the data systems. Such documentation shall be retained by the Processor;

g. in the event of suspected or confirmed personal data breach, the Controller must be notified without undue delay. The notification shall describe the breach and give an explanation of the cause, the period and the time at which the breach was discovered, the categories and approximate number of data subjects affected, the categories and approximate number of personal data entries affected, the name and contact details of the data protection officer or other contact point where more information can be obtained, the estimated impact of the breach and the immediate measures that have been instigated or are being considered for instigation in order to deal with the breach. If and to the extent that it is not possible to disclose all the information at the same time, it may be provided in stages without further undue delay;

h. document any breach, including the factual circumstances linked to the breach, its impact and any remedial measures that have been implemented;
i. notify the Controller without undue delay in the event of the unauthorised disclosure of personal data;
j. register all authorised and unauthorised access to data. All look-ups that are performed shall be registered so that they can be traced to the individual user concerned (i.e. an employee of the Processor, a subcontractor or the Controller). The logs shall be retained until there is no longer considered to be any use for them or as stipulated by the Agreement or Service/assignment agreement;
k. assist the Controller with ensuring fulfilment of the obligations in Articles 32-34 of the General Data Protection Regulation, including but not limited to:
   - security of processing;
   - notification of a personal data breach to the supervisory authority;
   - communication of a personal data breach to the data subject;
l. notify the Controller of circumstances related to the Processor's obligations under the Service/assignment agreement that entail or may be deemed to entail a weakness in information security;
m. obtain written approval from the Controller prior to the implementation of any change in the data processing by the Processor which is or could be of negative importance for information security when processing data in accordance with this Agreement.

Further requirements for information security are set out in **Appendix 2**.

In the event of a breach of this Agreement or the provisions of the data protection regulations, health legislation or other relevant legislation, the Controller may require changes to be made to the method of processing used or order the Processor to cease all further processing of the data with immediate effect.

The Processor shall document its routines and all measures that have been implemented in order to fulfil the requirements referred to above. Upon request, this documentation shall be made available to the Controller.

9. Use of subcontractors

The Controller permits the Processor to use subcontractors in order to fulfil the obligations applicable under this Agreement. The Processor will only use the subcontractors specified in **Appendix 4** for the services specified in said appendix.

The Processor shall:

a. ensure that the subcontractor accepts obligations corresponding to those incumbent on the Processor under the Agreement and applicable legislation;

b. maintain an updated list of the identity and location of subcontractors specified in Appendix 4 and where they process personal data. The updated list shall be available to the Controller;
c. conduct a risk assessment concerning the use of subcontractors and the significance for the service before entering into an agreement with subcontractors and, at the request of the Controller, share the assessment with the Controller;
d. at the request of the Controller, present a copy of the agreement(s) that has/have been entered into with the subcontractors (with the exception of commercial conditions). Such agreements must be established before the subcontractors commence the processing of personal health data;
e. notify the Controller of any plans to use other subcontractors or substitute subcontractors. The Controller must be given sufficient advance notice of such substitutions in order to give the Controller an opportunity to object to the change. In the event of the substitution of a subcontractor, Appendix 4 must be updated and sent to the Controller before a new subcontractor commences its work. The amendment must also be entered in Appendix 6;
f. ensure that the Controller and the supervisory authority have the same access and audit rights concerning the processing of personal data with respect to a subcontractor as the Controller has with respect to the Processor under Clause 12 of the Agreement;
g. in the event of the termination of the Agreement, ensure that subcontractors fulfil their obligation to return, erase or destroy in an appropriate manner all personal health data and any and all copies and back-up copies of the data as stipulated in Clause 13 of the Agreement.

The Processor shall at all times be responsible with respect to the Controller for all work that is performed by subcontractors and for ensuring that subcontractors comply with the provisions of this Agreement.

10. Transfer of personal data to other countries

The parties to this Agreement are in agreement that no personal health data that are processed under this Agreement shall be transferred out of Norway, except by specific agreement between the parties. In addition, documents that can be archived which contain personal health data must be located on servers in Norway (cf. Section 9 (b) of the Norwegian Archive Act), and any exceptions to this must be explicitly approved by the Controller before this processing commences.

The Processor confirms that none of the subcontractors transfer personal health data that are covered by this Agreement to other countries, with the exception of the transfers referred to in **Appendix 4**. This also encompasses remote access from other countries.

The use of subcontractors which transfer personal health data to countries outside the EU/EEA (third countries) shall be agreed in writing with the Controller in advance. In the event of the transfer of personal health data to countries outside the EU/EEA (third countries), the Processor shall use approved EU transfer mechanisms.

In connection with transfers to other countries, regardless of whether the country is within the EU/EEA or outside the EU/EEA (third countries), the Processor shall provide the necessary documentation concerning security, risk and compliance level linked to the relevant subcontractors to enable the Controller to receive the information necessary for conducting a specific risk assessment. The Controller shall be entitled to refuse consent for a particular transfer based on specific risks which are identified through the Controller’s own risk assessment.

11. Obligations of secrecy

The Processor’s employees and other parties who act on behalf of the Processor in connection with the processing of personal health data in accordance with this Agreement, the Service/assignment agreement and subsequent written agreements between the parties shall be subject to an obligation of secrecy under this Agreement and applicable regulations. Persons who are authorised to process personal health data undertake to process the data confidentially. The same applies to any subcontractors.

Employees and others who act on behalf of the Processor in connection with the processing of personal health data must have signed a confidentiality declaration. The provision shall apply correspondingly to subcontractors.

The Processor shall ensure that anyone who processes personal data under the Agreement is aware of the obligation of secrecy.

The parties shall also be subject to an obligation of secrecy concerning confidential information linked to each other’s activities which is disclosed in connection with the assignment.

The parties shall be obliged to take the precautions that are necessary to ensure that material or data is not disclosed to others in breach of this provision.

The obligation of secrecy shall also apply after termination of this Agreement.

12. Audits

Upon request, the Processor shall make available to the Controller all information necessary for demonstrating that the Processor's obligations set out in Article 28 of the General Data Protection Regulation and this Agreement have been fulfilled.

The Processor shall facilitate and contribute to inspections and audits carried out by or on assignment from of the Controller. The Processor shall submit internal audit reports, internal procedures, routines, security architecture, risk and vulnerability analyses with measures and other documents that are relevant to the audit.

The Processor shall also facilitate and contribute to inspections by the applicable supervisory authorities. The Controller's supervision of potential subcontractors must take place through the Processor, unless otherwise specifically agreed.

Specific routines for conducting audits can be agreed in **Appendix 3**.

If an audit reveals non-conformities with respect to the obligations in the applicable data protection rules or the Agreement, the Processor must rectify the nonconformity without undue delay. The Controller may require the Processor to temporarily suspend all or parts of the processing activities until such rectification has been approved by the Controller.

Each of the Parties shall cover its own costs associated with inspections by the applicable supervisory authorities and up to one annual audit initiated by the Controller. However, if an audit reveals a material breach of the obligations under the applicable data protection rules or the Agreement, the Processor shall cover the Controller's reasonable costs associated with the audit.

13. Duration and termination

The Data Processing Agreement shall enter into force from the date it is signed by both Parties and shall apply for as long as the Processor processes Personal Data on behalf of the Controller.

The Agreement will apply during this period unless other provisions that regulate the Processor's processing of Personal Data on behalf of the Controller are agreed to between the parties.

Upon termination of the Agreement, the Processor shall facilitate and contribute to the return of all personal health data that the Processor has received and processed on behalf of the Controller. The parties will specifically agree to how the transfer shall take place.

After all the data has been transferred to the Controller and receipt of the data has been confirmed, the Processor shall irreversibly erase or destroy in an appropriate manner all the data and any copies and back-ups of the data in its systems, unless other regulations require the personal health data to continue to be stored.

If shared infrastructure is used where direct erasure is not technically possible, the Processor shall ensure that data are rendered inaccessible until they have been overwritten by the system.

The Processor shall give the Controller written confirmation that the data have been transferred and erased as stipulated above.

14. Amendments to the Agreement

In the event of amendments to the legal framework or changes in services in the Service/assignment agreement which necessitate amendments to this Agreement, the parties shall work together to update the Agreement accordingly.

Amendments after the agreement has been entered into must be listed in **Appendix 6**. The Processor is responsible for ensuring that such a change catalogue is maintained and that it is kept up-to-date.

15. Governing Law, disputes and venue

The Agreement is governed by Norwegian law. Disputes shall be resolved in accordance with the provisions in the Service/assignment agreement, including any provisions relating to venue.

APPENDIX 1 – PURPOSE OF THE PROCESSING, DATA AND PROCESSING ACTIVITIES

[Version No. XX, *date/month/year*]

The table is updated in the event of changes. All changes must be entered in the change catalogue in **Appendix 6.**

A. Purpose and duration of the processing

(If the data processing agreement is linked to multiple service agreements, it must be specified as to which agreement it applies to.)

The purpose and duration of the processing of personal health data are:

Name of service	Purpose of the processing	Duration of the processing

B. Processing of personal health data

The following processing is covered by the Agreement:

Processing	Processing activities

C. Types of data

The following personal health data are processed:

Personal data	Special categories of personal data: personal health data

D. Categories of data subjects

Data pertaining to the following categories of persons are processed (data subjects):

Categories of data subjects

APPENDIX 2 – DETAILED REQUIREMENTS CONCERNING INFORMATION SECURITY

[Version No. XX, *date/month/year*]

The following requirements for information security are agreed in addition to the provisions of the Agreement:

No.	Topic	Requirement

APPENDIX 3 ADMINISTRATIVE PROVISIONS

[Version No. XX, *date/month/year*]

Contact details

Messages, notifications, reports and other communication between the Controller and the Processor shall take place in writing or be confirmed in writing to:

Controller	Processor
[Name of organisation] [Address]	**[Name of organisation]** [Address]
Name: Role: E-mail: Telephone number:	Name: Role: E-mail: Telephone number:

Other administrative provisions

The parties have agreed that:

Administrative provisions

APPENDIX 4 – SUBCONTRACTORS

[Version No. XX, *date/month/year*]

The table is updated in the event of changes. All changes must be entered in the change catalogue in **Appendix 6.**

The Processor uses the following subcontractors:

Name	Organisation no.	Address	Service type (processing)	Place of processing

APPENDIX 5: AMENDMENTS TO THE GENERAL TEXT OF THE AGREEMENT UPON ENTERING INTO THE AGREEMENT

The parties have agreed to the following amendments to the general text of the agreement:

Change table:

Clause in the agreement	Replaced with

APPENDIX 6: AMENDMENTS AFTER THE AGREEMENT HAS BEEN ENTERED INTO

[Version No. XX, *date/month/year*]

Catalogue of changes:

No.	Date	Change	Any appendices	Applies from