Norsk helsenett

Data Processing Agreement

Agreement on the processing of personal data in accordance with the Norwegian Personal Data Act and the EU's General Data Protection Regulation (Regulation (EU) 2016/679)

in connection with *the service that is to be provided*

(hereinafter "the agreement")

Between

Controller company

Org. no. *XXXXXXXX*

Controller

and

Processor company

Org. no. *XXXXXXXX*

Processor

1. About the agreement

Norsk helsenett SF (NHN) and <processor company> have entered into a data processing agreement concerning <the service that is to b provided>.

This agreement regulates rights and obligations between the controller and the processor (hereinafter referred to as "the parties") pursuant to:

- Act No. 38 of 15 June 2018 on the processing of personal data (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 referred to as the "General Data Protection Regulation");

- Any law, regulation or other regulation that amends or supersedes the above legislation.

In the event of a discrepancy between the provisions of the agreement and the framework that follows from the personal data legislation, the provisions of the agreement shall cede priority.

2. Definitions

The terms "personal data", "processing", “controller", “processor" and "personal data breach" shall be interpreted as defined in Article 4 of the General Data Protection Regulation. "Nonconformity" is a breach of information security and use of the information system in breach of established procedures.

Use of the information system that is not in accordance with the instructions issued by the controller or applicable data protection legislation shall be treated as a nonconformity.

3. Background and purpose of the agreement

This agreement has been entered into between the parties and outlines the general conditions for the processing of personal data that the processor carries out on behalf of the controller.

The purpose of the agreement is to secure the processing of personal data on behalf of the controller to ensure that the personal data is not used improperly or disclosed to unauthorised persons.

4. Scope

This agreement applies to all processing of personal data that the processor performs on the basis of <enter name of service/assignment agreement> (hereinafter referred to as the "service/assignment agreement"). In the event of a discrepancy between this agreement and the service/assignment agreement, this agreement shall take precedence.

Services covered by this agreement are those which form part of the service/contract agreement, and which involve the processing of personal data.

This agreement will also apply to the further processing of personal data based on any written agreements between the parties entered into during the term of this agreement which entail the processor processing personal data on behalf of the controller (hereinafter referred to as "subsequent written agreements between the parties").

Personal data shall only be used for the purposes set out in this agreement, the service/assignment agreement and subsequent written agreements between the parties insofar as is strictly necessary to implement and meet the requirements of the agreements.

5. Purpose of the processing, information and processing operations

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

A more detailed description of the processing, the purpose of the processing and the personal data that is covered is set out in the service/assignment agreement and subsequent written agreements between the parties where relevant.

6. Framework for the processing of personal data

The controller has complete control over the personal data that the processor has the opportunity to process under this agreement. The processor does not have an independent right to exercise control over the personal data and may not process it for its own purposes.

Unless otherwise agreed or provided for by law, the controller shall have the right to access and examine the personal data that is processed by the processor.

7. The controller's obligations

The controller shall comply with the obligations set out in the Personal Data Act, the General Data Protection Regulation, and other relevant special legislation, as well as this agreement.

8. The processor's obligations

8.1. General

The processor undertakes to only process personal data in accordance with all relevant laws and regulations, this agreement, the service/assignment agreement, the controller's documented instructions and other applicable agreements between the parties. Through action or omission, the processor shall not place the controller in a situation where the controller breaches any provision in applicable laws or regulations.

The processor shall not:

a. process personal data for other purposes or to a greater extent than that which follows from this agreement, service/assignment agreement and any subsequent written agreements between the parties;
b. process personal data beyond what is necessary in order to fulfil the processor's obligations under applicable agreements at all times;
c. disclose, make available or transfer personal data in any form on its own initiative unless agreed in advance with the controller or with the written consent of the controller;
d. collect/transfer personal data from/to a third party;
e. process personal data to which it has access through the assignment from the controller in any way other than as stipulated in this agreement, the service/assignment agreement and any subsequent written agreements between the parties.

The processor shall:

a. have a continually updated overview of all categories of processing activities that are performed on behalf of the controller;
b. give the controller access to personal data processed by the processor;
c. prepare and maintain an overview of all information and processing operations or, where relevant, a record of its own processing activities in accordance with Article 30 of the General Data Protection Regulation;

d. take all reasonable steps to ensure that the personal data is correct and up-to-date at all times;
e. establish procedures for erasing information when it is no longer needed based on the purpose of the processing and for erasing information in accordance with established procedures and guidelines;
f. have procedures and technical provision to restrict processing of the personal data of a data subject if the data subject so wishes pursuant to applicable legislation;
g. ensure that all persons granted access to personal data that is processed on behalf of the controller are familiar with this agreement and any applicable agreements between the parties and are subject to the provisions of these agreements;
h. ensure compliance with requirements regarding built-in data protection and data protection as a default setting in the processor's solutions. This includes building in functionality in order to fulfil the principles of data protection and functionality to safeguard the rights of data subjects;
i. provide the controller with the necessary assistance to ensure that the controller is able to fulfil its obligations with respect to data subjects;
j. cooperate with and assist the controller in fulfilling the rights of data subjects regarding access to information, including responding to requests from data subjects for the purpose of exercising their rights as set out in Chapter III of the General Data Protection Regulation;
k. immediately notify the controller if the processor believes that an instruction is in breach of the General Data Protection Regulation or other provisions concerning the protection of personal data;
l. assist the controller in ensuring fulfilment of the obligations of Articles 35-36 of the General Data Protection Regulation concerning data protection impact assessments and prior consultation with the Norwegian Data Protection Authority.

8.2. Technical, organisational and security measures

The processor shall be obliged to determine and implement all necessary and adequate planned and systematic technical, organisational and security measures to ensure that there is satisfactory information security in place in connection with the processing of personal data at all times.

The processor shall:

a. establish and comply with necessary technical and organisational measures with regard to ongoing confidentiality, integrity, availability and robustness in connection with the processing of personal data in order to ensure satisfactory information security in accordance with the provisions of the personal data legislation, including the requirements of Article 32 of the General Data Protection Regulation, and applicable health legislation. This includes, amongst other things, depending on what is relevant, necessary measures to prevent

accidental or unlawful destruction or loss of data, unauthorised access to or dissemination of data, as well as any other use of personal data that is not in accordance with this agreement, and measures to restore availability and access to the data following events;

b. have good and appropriate internal control procedures;

c. have procedures for authorisation and management which ensure that only the processor's employees who have a genuine need for access to systems and the data in order to perform essential tasks for the execution of the service/assignment agreement have such access. The level of access shall be in accordance with the genuine need relating to performance of the assignment;

d. establish the necessary systems and procedures to safeguard information security and follow up nonconformities, which shall include procedures for nonconformity reporting, restoring the normal situation, eliminating the cause of the nonconformity and preventing recurrence. Upon request, the processor shall give the controller access to relevant security documentation and the systems that are used for the processing of personal data;

e. uncover, record, report and close nonconformities linked to information security, including logging and documenting any and all cases of attempted unauthorised access and other breaches of data security in the computer systems. Such documentation shall be stored by the processor;

f. in the event of a suspected or confirmed nonconformity, notify the controller immediately. The notification shall provide information on the nonconformity, including an explanation of the cause, time period and the time at which the nonconformity was discovered, the categories and approximate number of data subjects affected, the categories and approximate number of records of personal data affected, the name and contact details of the data protection officer or other point of contact where more information can be obtained, the predicted impact of the nonconformity and the immediate measures that have been initiated or are being considered in order to deal with the nonconformity;

g. document any and all nonconformities, including the actual circumstances relating to the nonconformity, its impact and any measures implemented;

h. immediately notify the controller in the event of the unauthorised disclosure of personal data;

i. record all authorised and unauthorised access to information. All lookups that are performed shall be registered so that they can be traced to the individual user (i.e. employee of the processor, subcontractors and controller). The logs shall be retained until there is no longer considered to be any use for them or in accordance with the provisions of the service/contract agreement;

j. assist the controller in ensuring compliance with the obligations of Articles 32–34 of the GDPR, i.e.:
    a. security in connection with the processing;
    b. notification of the supervisory authority of any breaches of personal data security;
    c. notification of data subjects in the event of a personal data breach;

k. in connection with security audits conducted by the controller or a third party appointed by the controller, provide internal audit reports, internal procedures, routines, security architecture, risks and vulnerability analyses with measures and other documents of significance to the audit;

l. notify the controller of any and all circumstances that entail a change in the risk picture;

m. obtain approval from the controller prior to the implementation of any changes in the processing by the processor which have or could have an impact on information security.
n.

Further requirements regarding the processor's information security are set out in Appendix 2 (where applicable).

In the event of a breach of this agreement or the provisions of personal data legislation, health legislation or other relevant legislation, the controller may require changes to be made to the method of processing used or to order the processor to cease further processing of the data with immediate effect.

The processor shall document its procedures and all measures that are taken to fulfil the requirements set out 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 under the agreement. The processor uses subcontractors as specified in Appendix 3 for the services specified therein and confirms that no other subcontractors are used.

The processor shall:

a. ensure that the subcontractor assumes equivalent obligations to the processor under the agreement and applicable legislation;
b. ensure that subcontractors only process personal data in accordance with this agreement and not to any greater extent than is necessary to fulfil the relevant service provided by the subcontractor;
c. maintain an up-to-date list of the identity and location of subcontractors as specified in Appendix 3. An updated list shall be available to the controller;
d. conduct a risk assessment of the use of subcontractors and the significance for the service before entering into any agreement with a subcontractor and, at the request of the controller, share the assessment with the controller;
e. at the request of the controller, provide a copy of the agreement(s) entered into with the subcontractors (with the exception of commercial conditions). Such agreements shall be established no later than before the subcontractors commence the processing of personal data;
f. notify the controller of any plans to use other subcontractors or replace subcontractors. Notice of such replacements shall be given in good time so that the controller is given the opportunity to object to the change. In the event of the replacement of a subcontractor, Appendix 3 shall be updated and sent to the controller's contact person;
g. ensure that the controller and the supervisory authorities have the same right to access and verify the processing of personal data by a subcontractor that the controller has with respect to the processor under clause 12 of the agreement;
h. upon termination of the agreement, ensure that subcontractors fulfil the obligation to erase or satisfactorily destroy all personal data and any copies and backups of the information stipulated in clause 13 of the agreement in the same way as the processor, to the extent that such erasure or destruction does not conflict with other statutory provisions.
i.

The processor shall be liable in full at all times with respect to the controller for all work that is performed by subcontractors and for the subcontractors' compliance with the provisions of this agreement.

Access to personal data for third parties shall require a specific agreement over and above this agreement between the parties for all parties other than the processor's subcontractors.

10. Transfer of personal data abroad

The parties to this agreement agree that no personal data processed under this agreement shall be transferred out of Norway, unless specifically agreed between the parties. Any exceptions that involve transfer abroad shall be explicitly approved by the controller prior to the commencement of processing.

The processor confirms that none of the subcontractors shall transfer personal data covered by this agreement abroad, except for such transfers as are stipulated in Appendix 3. This also includes remote access from abroad.

The use of subcontractors that transfer personal 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 data to countries outside the EU/EEA (third countries), the processor shall use approved EU transfer mechanisms.

In connection with transfer abroad, irrespective of whether such transfer 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 relevant subcontractors so that the controller receives the necessary information in order to conduct a special risk assessment. The controller may refuse consent to the transfer concerned based on specific risks which become apparent through the controller's own risk assessment.

11. Confidentiality

The processor's employees and others acting on behalf of the processor in connection with the processing of personal data under this agreement, the service/assignment agreement and subsequent written agreements between the parties (hereinafter referred to as "persons authorised to process the personal data") shall be subject to a duty of confidentiality pursuant to this agreement and applicable regulations. Persons authorised to process the personal data undertake to treat the data confidentially. The same shall apply to any and all subcontractors.

The processor shall ensure that anyone who processes personal data under the agreement is aware of the duty of confidentiality.

Employees and others acting on behalf of the processor in connection with the processing of personal data shall have signed a non-disclosure agreement. The provision applies correspondingly to subcontractors.

In addition, the parties shall be subject to a duty of confidentiality regarding confidential information relating to each other's activities, which is communicated in connection with the assignment.

The parties shall be obliged to take the precautions that are necessary to ensure that material and information are not disclosed to third parties in breach of this clause.

The duty of confidentiality shall continue to apply after termination of the agreement.

12. Access, verification and auditing

The controller may at any time require access to and verification of the processor's processing of personal data belonging to the controller, including access to and verification of documentation for fulfilment of the requirements regarding information security and the processor's internal control system.

The right of access shall apply to all technical, organisational and administrative circumstances that are relevant to the security of the processing that is carried out by the processor on behalf of the controller, and other access rights laid down in law. If the controller requests access, general information from the audit shall be made available to other controllers which use the same service with the processor.

Insofar as is possible, the controller shall give the processor reasonable notice in the event that access and verification are required, normally at least 30 days' notice. In the event that document access is required, at least 14 days’ notice should be given. The controller shall contribute to ensuring that access and verification may be coordinated between several controllers who receive services from the processor. Access and verification may be carried out by the controller or a third party appointed by the controller. The processor may claim reimbursement for documented added costs which are incurred in connection with such audits.

The processor shall give the Norwegian Data Inspection Authority and other relevant supervisory authorities access and insight to the processing of personal data as set out in relevant legislation.

The processor shall correct any nonconformities without delay. Nonconformities that are due to the processor or its subcontractors shall be corrected at no cost to the controller. The processor shall provide a written explanation of the corrective measures and an implementation plan.

13. Duration and termination

This agreement shall take effect from the date on which it is signed by the parties and shall remain in force until termination of the agreement and all applicable agreements between the parties which entail the process processing personal data on behalf of the controller.

Upon termination of the agreement, the processor shall facilitate and contribute to the return of all data that the processor has received and processed on behalf of the controller. The parties shall agree on precisely how transfer shall take place in concrete terms.

After all data has been transferred to the controller and confirmed as having been received by the controller, the processor shall irreversibly erase or duly destroy all data and all copies and backups of the data on its systems, unless statutory rules require that the personal data continue to be stored.

If shared infrastructure is used where direct erasure is not technically possible, the processor shall ensure that data is rendered unavailable until this data is overwritten by the system.

The processor shall provide the controller with written confirmation that the data has been transferred and erased as stipulated above.

14. Amendment of agreement

In the event of changes to applicable legislation, final judgment which provides a different interpretation of applicable law, or changes to services in the service/assignment agreement which necessitate amendments to this agreement, the parties shall cooperate to update the agreement accordingly.

15. Notices

Notices, notification or other communication between the controller and the processor shall take place in writing or be confirmed in writing to:

Controller	**Processor**
Controller company *Address*	***Processor company*** *Address*
Name: *Role:* *E-mail:* *Mobile no.:*	*Name:* *Role:* *E-mail:* *Mobile no.:*

16. Governing law and legal venue

The agreement is subject to Norwegian law. Disputes shall be resolved in accordance with the provisions of the service/assignment agreement, including any provisions regarding legal venue.

17. Signatures

This agreement has been prepared in duplicate, with each party retaining one copy.

Place and date:

[state place], xx.xx.20xx

Controller	Processor
Name	Name

APPENDIX 1 – PURPOSE OF THE PROCESSING, INFORMATION AND PROCESSING OPERATIONS

The tables are updated on an ongoing basis.

[*date/month/year*]

A. Purpose and duration of the processing

The purpose and duration of the processing of personal data is: [*remember that <u>each</u> processing operation must be linked to specific and expressly stated purposes)*

Name of service	Purpose of the processing	Duration of the processing

B. Processing of personal data

The following processing operations are covered by the agreement: *[here, list the processing operations involving personal data that are covered – see the examples below]*

Processing	Processing activities
Collection	The processor shall have mechanisms in place for data during transport, processing and storage in order to safeguard integrity and confidentiality.
Registration	Personal user names and passwords shall be used in connection with access to data for professional purposes. The processor shall have established a password policy.
Organisation	
Structuring	
Storage	
Adaptation or change	
Retrieval	
Compilation	
Erasure or destruction	
Disclosure/Transfer	

C. Types of information

The following health and personal data is processed: [here, list the health and personal data that is covered – see the examples below]

Personal data	Health data
E.g. name and e-mail address	

D. Categories of data subjects

Information is processed about the following categories of persons (data subjects): [here, list the categories of data subjects that are covered – see the examples below]

Categories of data subjects		
E.g. employees, healthcare professionals		

APPENDIX 2 – DETAILED REQUIREMENTS REGARDING INFORMATION SECURITY

[here, list detailed requirements regarding information security – see the examples below]

No.	Theme	Requirement
1.	Securing of data	Personal user names and passwords shall be used in connection with access to data for professional purposes. The processor shall have established a password policy.
2.	Authentication	Personal user names and passwords shall be used in connection with access to data for professional purposes. The processor shall have established a password policy.
3.	Denial of service attack	
4.	Logging and traceability	
5.	Redundancy and scaling	
6.	Test data	
7.	Erasure and return	
8.	Storage period	
9.	Backup and restore	
10.	Encryption upon saving	
11.	Encryption in communication	
12.		
13.		
14.		

APPENDIX 3 – SUBCONTRACTORS

[here, list the subcontractors that are used by the processor – see the examples below]

The tables are updated on an ongoing basis.

[*date/month/year*]

Name of subcontractor	Delivery area	Location