|  |  |
| --- | --- |
| Ahus | *Appendix to EQS document 33714* |
| **Data Processing Agreement** |

**DATA PROCESSOR AGREEMENT**

According to the Personal Data Act and the

EU General Data Protection Regulation 2016/679

between

**Akershus universitetssykehus HF**

Org. no.: 983 971 636

*Data Controller*

and

**[Name of the Enterprise]**

Org. no.: 000 000 000

*Data Processor*

Dated: xx.xx.20xx

Content

[1 About the Agreement 2](#_Toc433157)

[2 Definitions 2](#_Toc433158)

[3 Background Info and Objectives of the Agreement 4](#_Toc433159)

[4 Scope 4](#_Toc433160)

[5 Objectives of processing, information and processes 5](#_Toc433161)

[6 Framework for processing health data and personal information 5](#_Toc433162)

[7 Data Controller’s obligations 5](#_Toc433163)

[8 Data Processor's obligations 5](#_Toc433164)

[8.1 Generalities 5](#_Toc433165)

[8.2 Technical, organizational and security measures 6](#_Toc433166)

[9 Use of subcontractors 8](#_Toc433167)

[10 Transfer of personal data to other countries 9](#_Toc433168)

[11 Duty of confidentiality 10](#_Toc433169)

[12 Inspection of documents, verification and revisions 10](#_Toc433170)

[13 Duration and termination 11](#_Toc433171)

[14 Altering the Agreement 11](#_Toc433172)

[15 Notification 11](#_Toc433173)

[16 Choice of law and legal venue 12](#_Toc433174)

[17 Signatures 12](#_Toc433175)

**APPENDIX 1 – OBJECTIVES OF PROCESSING, INFORMATION AND PROCESSING**

**APPENDIX 2 – SECURITY REQUIREMENTS**

**APPENDIX 3 – SUBCONTRACTORS**

# About the Agreement

This Data Processing Agreement (henceforth called the "Agreement") governs the rights and obligations between the Data Controller and the Data Processor (henceforth called "the Parties") pursuant to:

* The Act of 15 June 2018 no. 38 concerning the processing of personal data (Personal Data Act);
* EU Regulation 2016/679/EC of 27 April 2016 concerning the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (henceforth called GDPR);
* The Act concerning Personal Health Data Filing Systems and Processing of Health Data of 20 June 2014 no. 43 (Personal Health Data Filing Systems Act);
* The Act concerning the processing of health data when performing health care of 20 June 2014 no. 42 (Health Records Act); and
* Any acts, regulations or other rules that might replace these.

The governing laws and regulations stated in the provisions of personal data protection legislation or relevant health care legislation shall take precedence over this Agreement if the information in this Agreement conflicts with such legislation.

The Data Controller's name, enterprise registration number and other contact information are found in the Data Processor's customer records filing system based on the information provided by the Data Controller.

This Agreement shall only be used when Sykehuspartner HF is not a party to the agreement, and the external data processor shall not utilise any of the region's infrastructures. If Sykehuspartner HF is involved, the region's standard data processing agreement shall be used.

# Definitions

The terms "personal data", "processing", "data controller", "data processor", "breach of information security" and "health data" shall be understood such as they are defined in the GDPR § 4, the Personal Health Data Filing System Act § 2 and the Health Record Act § 2 as effective.

Deviation: breach of the information security and the use of the information system contrary to stipulated routines.

The use of the information system which is not in accordance with instructions from the Data Controller or the applicable privacy legislation shall be deemed to be a deviation.

# Background Info and Objectives of the Agreement

This Agreement describes the general terms and conditions for processing health data and personal information that the Data Processor process on behalf of the Data Controller.

The objective of this Agreement is to ensure that health data and personal information being processed on behalf of the Data Controller in accordance with the requirements laid down in personal data protection legislation, according to this Data Processing Agreement and according to instructions provided by the Data Controller.

# Scope

This Agreement applies to all health data and personal information being handled and processed by the Data Processor on behalf of [*write the name of the service and or assignment contract*] (henceforth called "Service/Assignment Contract").

The services that involve processing health data and personal information are stated in Appendix 1 of this Agreement. The Data Processor shall limit the processing of health data and personal information to process the data necessary for the Data Processor to perform the agreed services. A risk assessment shall be done prior to processing. The Risk Assessment contains all relevant requirements and information according to the GDPR and will be summarised and updated in the Data Processor's existing Protocols for data processing activities.

In the event of a conflict between this Agreement and the Service/Assignment Contract, this Agreement shall take precedence.

The Services described in this Agreement are those stated in the Service/Assignment Contract which involve processing health data and personal information.

If the Data Controller decides to use new services offered by the Data Processor, the terms of processing must be clarified in advance and must form part of the objectives that are governed by this Agreement. If the objectives of the new services are the same as the other services, this Data Processing Agreement shall be applicable to the new services as well.

Any change to the Data Processor’s processing routines that are or could be significant to information security shall be subject to a risk assessment and must be approved by the Data Controller before the change can be executed, and any further measures or instructions to be implemented by the Data Controller. Only the Data Controller can accept changes to a risk, so the Data Controller must approve the use of the services indicated by the risk assessment based on the completed and processed risk assessment before data processing can start. This also includes replacing any subcontractors the Data Processor uses.

This Agreement shall also apply to further processing of health data and personal information based on any written agreements between the Parties that are signed during the duration of this Agreement and that involve the Data Processor processing health data and personal information on behalf of the Data Controller (henceforth called "Later Written Agreements between the Parties").

Health data and personal information shall only be used for the objectives stated in this Agreement in the Service/Assignment Contract and Later Written Agreements between the Parties to the extent this is strictly necessary to execute and comply with the requirements stated in these agreements.

# Objectives of processing, information and processes

[Description]

# Framework for processing health data and personal information

The Data Controller has complete control over the health data and personal information that the Data Processor has agreed to handle pursuant to this Agreement. The Data Processor has no independent right over the health data and personal information and cannot process it for own objectives.

Unless otherwise agreed or pursuant to statutory regulations, the Data Controller is entitled to access all health data and personal information being processed by the Data Processor.

# Data Controller’s obligations

The Data Controller shall comply with the obligations stated in personal data protection legislation, as well as that stated in this Agreement, the Norms for Information Security and the hospital's information security management system.

# Data Processor's obligations

## Generalities

The Data Processor is obligated to process health data and personal information in accordance with personal data protection legislation, this Agreement, the shared regional information security management system at the Southern and Eastern Norway Regional Health Authority (HSØ) and the Data Controller's management system, Service/Assignment Contract, the Data Controller's documented instructions and other current agreements between the Parties, as well as the Norms for Information Security in the Health and Care Services. When handling, processing or omitting the handling or processing of data, the Data Processor shall not put the Data Controller in any situation that violates the provisions of existing acts, regulations and legislation.

The Data Processor is responsible for any harm caused by the Data Processor's processing, yet only if the obligations stated in personal data protection legislation that are directed at the Data Processor in particular are not fulfilled, or if the Data Processor's conduct has conflicted with the instructions provided by the Data Controller.

If a subcontractor fails to fulfil its obligations with regard to personal data protection legislation and/or this Data Processing Agreement, the Data Processor shall accept full responsibility for the subcontractor's fulfilment or failure to fulfil these obligations.

The Data Processor must not:

1. process health data and personal information for any other purpose or to any greater extent than that stated in this Agreement, the Service/Assignment Contract and any Later Written Agreements between the Parties;
2. process health data and personal information beyond that which is necessary to fulfil the Data Processor's obligations according to current applicable agreements;
3. distribute, hand-over or transfer health data and personal information in any form on own initiative unless this is agreed with the Data Controller in advance or the Data Controller has approved this in writing;
4. collect or transfer health data and personal information from/to a third party;
5. process health data and personal information that one gains access to or acquires on assignment for the Data Controller in any other way than that stated in this Agreement, the Service/Assignment Contract and any Later Written Agreements between the Parties.

The Data Processor shall:

1. monitor and document all categories of data processing activities completed on behalf of the Data Controller;
2. give the Data Controller access to and the right to inspect all health data and personal information being processed by the Data Processor;
3. keep and maintain an overview of all information and processing or, if this is relevant, keep protocols on its data processing activities according to Article 30 of the GDPR;
4. implement any and all reasonable measures to ensure that health data and personal information is always correct and updated;
5. establish routines for deleting data when it is no longer necessary based on the objectives for its processing and delete information according to established routines and guidelines;
6. have routines in place for, and technical options available to, limit processing of the Data Subjects’ registered health data and personal information if the Data Subject desires this, based on the legal authority of current legislation;
7. ensure that all persons who are given access to personal data being processed on behalf of the Data Controller have read and understood this Agreement and current agreements between the Parties, and that they understand that they are subject to the provisions of these agreements;
8. ensure that the requirement for built-in security for personal data protection have been implemented, and that personal data protection is a standard setting in the Data Processor's solutions. This includes building in a functionality to fulfil the principles of personal data protection as well as a functionality to protect the Data Subjects’ rights;
9. assist the Data Controller when needed so the Data Controller can fulfil its obligations in respect of the data subjects;
10. cooperate with and assist the Data Controller in protecting the data subjects' right to access to information, which includes responding to requests from the Data Subjects with the intent of exercising their rights as laid down in Chapter III of the GDPR;
11. the Data Processor shall inform the Data Controller immediately of any suspicion that the instructions conflict with the GDPR or personal data protection legislation;
12. assist the Data Controller in ensuring compliance with the obligations stated in GDPR articles 35-36 that deal with assessing the consequences for personal data and prior consultation with the Data Inspectorate.

## Technical, organizational and security measures

The Data Processor is responsible for the decisions about and systematic implementation of all technical, organizational and security measures that are necessary to ensure information security for the handling and processing of health data and personal information, and to plan this work adequately. All personal data covered by this Data Processing Agreement shall be processed with adequate levels of acceptable risk that have been established by the Data Controller.

The Data Processor shall:

1. establish and comply with all necessary technical and organizational measures with regard to confidentiality, integrity, availability and robustness in the handling of health data and personal information to ensure satisfactory information security according to the provisions of the Personal Data Act, including the requirements laid down in Article 32 of the General Data Protection Regulation and in current health care legislation (personal data protection legislation), the common regional HSØ management system and the enterprise's internal management system. This includes e.g. everything that can be considered a relevant and necessary measure to prevent accidental or illegal destruction or loss of data, unauthorised access to or the sharing or distribution of data as well as all other uses of health data and personal information that is not in accordance with this contract, and measures to restore availability and access to information if undesirable incidents occur;
2. Protect health information against negligent distribution. Technical measures shall be in place to prevent personal data from being moved out of secure zones or from approved storage sites
3. Ensure security for remote operation of the Data Controller's systems. Encrypted VPN connections shall be used with blocking of all simultaneous access to internet. Equipment used in connection with remote access must only be used by authorised persons
4. 2-level authentication is used if access to the Data Controller's systems goes via unsecured networks
5. Protect communication with encryption if it is sent via unsecured networks
6. Maintain good and suitable internal control systems;
7. Have routines in place for authorisation and control to ensure that only the Data Processor's employees who actually need access to the systems and information to carry out necessary assignments to execute the Service/Assignment Contract. The access level shall conform to the real needs related to executing the assignment;
8. Access control via access cards with personal identity codes or similar shall be used. Access into restricted areas, such as operational and server rooms, shall be based on real need. Access control with locked doors will be used for the following types of premises: data hall/server rooms, IT premises (operation/support), premises with ICT equipment (coupling matrices, switches/routers) etc.
9. Establish necessary systems and routines to protect information security and follow up on deviations, which shall include e.g. routines for deviation reporting, normal situation recovery, removing the cause of any deviation and hindering repeated incidents. Upon request, the Data Processor shall provide the Data Controller with access to relevant security documentation and systems that are used to handle and process health data and personal information;
10. Discover, register, report and close deviations related to information security, including logbooks and documenting any attempt at unauthorised access and other breaches of information security in the data processing systems. Such documentation shall be archived by the Data Processor;
11. if a deviation is found or suspected, notify the Data Controller and the Data Controller's data protection officer immediately. The notification should explain the cause of the deviation, the time and date of its discovery, the categories of and approximate number of data subjects who were affected, the categories of and approximate number of registrations of personal data that were affected, the name of the data protection officer and his or her contact information or another point of contact where more information can be collected, the assumed consequences of the deviations and which immediate measures were implemented or considered for dealing with the deviation. Every notification or enquiry to the Data Inspectorate shall be sent by the Data Controller;
12. document every deviation, including the actual facts related to the deviation, its effects and remedies that were implemented;
13. notify the Data Controller immediately about any unauthorised distribution of personal data;
14. register all authorised and unauthorised access to personal data. All queries must be recorded so one can track the individual users (i.e. Data Processor employees and subcontractors and the Data Controller). The logs should be archived until they are no longer needed, or as specified in the Service/Assignment Contract;
15. assist the Data Controller in ensuring compliance with the obligations stated in articles 32–34 of the General Data Protection Regulation, i.e.:
- processing security;
- notifying the inspectorate authority about a violation or breach of personal data security;
- informing the Data Subjects about the breach to personal data security;
16. in connection with security audits carried out by the Data Controller or a third party appointed by the Data Controller, submit Internal audit reports, Internal procedures, routines, security architecture, risk and vulnerability analyses with measures and other documents of significance for the audit;
17. notify the Data Controller about all conditions that imply a change to risk scenarios;
18. collecting the approval from the Data Controller before any change to processing can be executed by the Data Processor that has or could have a significance to information security.

Detailed requirements about the Data Processor's information security are stated in Appendix 2a (if relevant). See Appendix 2b – Risk Assessments.

In the event of a breach of this Agreement or the provisions of personal data protection legislation, the Data Controller can demand changes to processing procedures or instruct the Data Processor to cease further handling or processing of the information with immediate effect.

The Data Processor shall document its routines and all measures that are implemented to satisfy the requirements stated above. This documentation shall be made available to the Data Controller upon request.

# Use of subcontractors

The Data Controller permits the Data Processor to use subcontractors to satisfy its obligations to this Agreement. The Data Processor shall use subcontractors as described in Appendix 3 for the services referred to in the Agreement, and shall confirm that no other subcontractors will be used. The Data Processor cannot use other subcontractors than those who were agreed on when the Agreement was signed between the Data Controller and the Data Processor without completing the activities stated in letters [d] and [f].

The Data Processor shall:

1. ensure that the subcontractor accepts the same obligations the Data Processor agreed to in the Agreement and pursuant to current legislation;
2. ensure that the subcontractors only process personal data in accordance with this Agreement and not to any greater scope than that which is necessary to carry out the service the subcontractor was contracted to deliver;
3. keep an updated list over the identity and territorial locations of the subcontractors listed in **Appendix 3**. The updated list shall be available for the Data Controller;
4. execute a risk assessment in the use of subcontractors and their significance to the service before signing any agreement with a subcontractor and upon request from the Data Controller, share the results of the assessment with the Data Controller;
5. upon request from the Data Controller, submit a copy of any contract(s) that were entered into with subcontractors (with the exception of commercial conditions). Such agreements must be signed before the subcontractors begin processing health data and personal information;
6. inform the Data Controller in good time about any plans to use other subcontractors or replace a subcontractor. The Data Controller must be informed about such replacements in good time, so the Data Controller has the opportunity to oppose any such change. The Data Processor cannot use other subcontractors than those agreed to when the Agreement was signed and as stated in Appendix 3 without the following being done: 1) the Data Controller has approved the risk assessment, 2) the Data Controller has approved the use of the current/new subcontractor in writing. If a subcontractor is to be replaced, **Appendix 3** shall be updated and sent to the Data Controller's contact person to make him or her aware of this;
7. ensure that the Data Controller and the inspectorate authority have the same right to inspect documents and to audit the subcontractor's personal data processing routines that the Data Controller has towards the Data Processor according to Item 12 of the Agreement;
8. upon termination of the Agreement, ensure that the subcontractors fulfil their obligation to delete and properly dispose of or return the health data and personal information if requested – and all copies and security copies of the information that are described in Item 13 of the Agreement in the same manner as the Data Processor, as long as this does not conflict with other statutory provisions.

The Data Processor is responsible towards the Data Controller for all work done by subcontractors. The Data Processor is also responsible for subcontractor compliance with the provisions of this Agreement.

Access to health data and personal information by third parties requires a specific agreement beyond this Agreement between the parties for anyone other than the Data Processor's subcontractors.

# Transfer of personal data to other countries

The parties to this Agreement agree that no health data or personal information being processed for this Agreement shall leave Norway unless the Parties to this Agreement agree to do so. In addition, health data and personal information shall be placed on servers in Norway (see letter b of § 9 of the Archives Act). Any exception that involves transferring data to a foreign country must be approved explicitly by the Data Controller before processing can begin.

The Data Processor will confirm that no subcontractors will transfer health data and personal information for this Agreement to a foreign country, with the exception of transfers stated in Appendix 3. This also applies to remote access from abroad.

A subcontractor who wishes to transfer health data and personal information to any country outside of EU/EEA (so-called third countries) must be approved by the Data Controller, in advance and agreed upon in writing. When transferring health data and personal information to any country outside of EU/EEA (third countries), the Data Processor must only use EU-approved transfer mechanisms.

When transferring health data and personal information to any country regardless of whether it is inside EU/EEA or outside EU/EEA (third countries), the Data Processor shall provide all necessary documentation about security, risk and compliance related to the subcontractors so the Data Controller has all the information necessary to execute a special risk assessment. The Data Controller can refuse to consent to the transfer based on specified risks that were identified during the Data Controller's risk assessment.

# Duty of confidentiality

The Data Processor's employees and others who act on behalf of the Data Processor to process personal data according to this Agreement, the Service/Assignment Contract and Later Written Agreements between the Parties (henceforth called "Authorised Persons") are subject to secrecy and confidentiality pursuant to this Agreement and to current legislation. Persons Authorised to Process Person Data are obligated to treat this information as confidential. The same applies to subcontractors.

The Data Processor shall ensure that everyone who processes personal data for this Agreement is aware of this duty.

Employees and others who act on behalf of the Data Processor where the processing of personal data is concerned must sign a declaration of confidentiality. This provision also applies to subcontractors.

The Parties are also subject to confidentiality regarding confidential information related to each other's activities when these are related to the assignment.

The Parties are obligated to take adequate precautions to protect data, information, documents etc. from reaching unauthorised persons.

The confidentiality obligation shall continue to apply after the expiry of the Agreement.

# Inspection of documents, verification and revisions

The Data Controller shall be given access to and/or verification of the Data Processor's processing routines and personal data that belongs to the Data Controller, including access to and verification of documentation to verify fulfilment of the requirements for information security and the Data Processor's internal control systems.

The right to access and insight applies to all technical, organizational and administrative conditions undertaken by the Data Processor on behalf of the Data Controller that are relevant to processing security and any other statutory rights related to inspecting documents. If the Data Controller requests access, all generalised information from the audit will be made available to the other Data Controllers who use the same service from the Data Processor.

The Data Controller shall as far as possible notify the Data Processor in good time about the audit and/or inspection, normally a 30-day warning. Requests to audit documents require a 14-day warning. The Data Controller shall facilitate access and coordinate an audit between several Data Controllers if they are receiving the same services from the Data Processor. Audits and inspections can be carried out by the Data Controller or by a third party appointed by the Data Controller. The Data Processor will be paid for any documented extra costs that are required to complete the audit.

The Data Processor shall provide the Data Inspectorate and other relevant inspectorate authorities with access to the processing of health data and personal information according to relevant legislation.

The Data Processor shall correct any deviations that are found, without unnecessary delay. Deviations caused by the Data Processor or its subcontractors shall be corrected at no cost to the Data Controller. The Data Processor explain these corrective measures in writing and provide a plan for execution.

# Duration and termination

This Agreement is applicable upon its signing by both Parties and until the Agreement and all other agreements between the Parties that involve the Data Processor processing health data and personal information on behalf of the Data Controller has ended.

Upon termination of the Agreement, the Data Processor shall organize and assist in returning all information that the Data Processor received and processed on behalf of the Data Controller. The Parties shall agree on the details for how this transfer takes place.

After all the information are has been transferred to the Data Controller and confirmation of this has been received, the Data Processor shall irreversibly delete or properly destroy all information and all copies and security copies of the information in its systems, unless indisputable legislation requires the health data and personal information to be archived for a longer time.

If a divided infrastructure is used where direct deletion is not technically possible, the Data Processor shall ensure that the data cannot be accessed until the data has been overwritten on the system.

The Data Processor shall give the Data Controller written confirmation that the data was transferred and deleted as stated above.

# Altering the Agreement

If current laws change or if a final judgment is pronounced that requires a different interpretation of the law, or if changes are made to the services listed and described in Service/Assignment Contract that require modifications to this Agreement, the Parties shall cooperate to update the Agreement accordingly.

# Notification

Notifications, informing the other party or other types of communication between the Data Controller and the Data Processor shall be done in writing, or be confirmed in writing, to:

|  |  |
| --- | --- |
| Data Controller | Data Processor |
| Akershus universitetssykehus HFPostboks 1000, 1478 Lørenskog | **[Enterprise's name]**[Address] |
| Name: Øystein MælandRole: CEOE-mail: postmottak@ahus.no Cell phone no.:  | Name:Role:E-mail:Cell phone no.: |

# Choice of law and legal venue

This Agreement is subject to Norwegian law. The parties agree that the Oslo District Court shall be the legal venue for resolving any legal disputes.

This shall continue to apply after the expiry of the Agreement.

# Signatures

This Agreement is signed in two originals, of which each of the Parties keeps one.

Place and date:

[*enter city/location*], xx.xx.20xx

|  |  |
| --- | --- |
| Data Controller | Data Processor |
|  |  |
| Name: | Name: |

**APPENDIX 1 – OBJECTIVES OF PROCESSING, INFORMATION AND PROCESSING**

This table is to be updated as required.

[date/month/year]

1. **Objective and duration of processing**

The objectives and duration of processing health data and personal information: *[remember that all processing must be related to specific and expressly stated objectives – see the example below]*

|  |  |  |
| --- | --- | --- |
| Name of service | Objective of processing | Duration of processing |
| File transfer service | Transfer major data volumes | Until the purpose is achieved |
|  |  |  |
|  |  |  |

**B. Handling and processing health data and personal information**

Processing covered by the Agreement: *[list what the processing of health data and personal information includes – see the examples below]*

|  |  |
| --- | --- |
| Processing | Data processing activities |
| Collection |  |
| Registering |  |
| Organizing |  |
| Structuring |  |
| Archiving |  |
| Adaptation or changing |  |
| Recovery |  |
| Comparison |  |
| Deletion or destroying |  |
| Distributing/transferring |  |

**C. Types of data and information**

The following types of health data and personal information will be processed:

*[List what kind of health data and personal information is to be processed – see the examples below]*

|  |  |
| --- | --- |
| Personal information | Health data |
| NameNational ID no.Residence | Use of medicationDiagnostic dataData from the health registers |

**D. Categories of data subjects**

Data will be processed from the following categories of persons (data subjects):

*[List the categories of data subjects for whom health data and personal information is to be processed – see the examples below]*

|  |
| --- |
| Categories of data subjects |
| PatientsChildrenParentsAttorneys | Health personnelEmployeesEx-employeesEmployees of cooperating company | SuppliersKey personnel |

**APPENDIX 2 – Security Requirements**

*[list the detailed requirements for information security, as needed]*

|  |  |  |
| --- | --- | --- |
| No. | Subject | Requirement |
|  | Norm for information security in the health and care services sector | The Data Processor shall comply with relevant requirements in Norm for information security (see fact sheet 6b, and what requirements are given for the Data Processor) |
|  | Protecting data | The Data Processor shall have mechanisms for protecting data under transport, processing and storage to ensure integrity and confidentiality. |
|  | Authentication | When accessing data for professional needs, use personal user name and password. The Data Processor shall have an established password policy. |
|  | Denial-of-service |  |
|  | Logging and traceability |   |
|  | Redundancy and scaling |  |
|  | Test data |  |
|  | Erasure and return |  |
|  | Storage period |  |
|  | Backup and restore |  |
|  | Encryption when storing |  |
|  | Encryption in communication |  |
|  |  |  |
|  |  |  |
|  |  |  |

**APPENDIX 3 – SUBCONTRACTORS**

*[list the names of subcontractors which will be processing health data and personal information – see the examples below]*

This table is to be updated as required.

*[date/month/year]*

|  |  |  |
| --- | --- | --- |
| Name of subcontractor | Delivery type | Location |
| ABC | Data centre, hosting | Stockholm, Sweden |
| DEF | IT support services | Oslo, Norway |
| XYZ | Backup | Paris, France |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |