DATA PROCESSOR AGREEMENT

Use of subcontractor

Data Processor Agreement concerning the instrument vendors processing and safeguarding personal data linked to service and maintenance on instruments

between

Oslo University Hospital HF

NO 993 467 049

Hereafter referred to as Main Data Processor

and

Instrument vendor

Hereafter referred to as Data Processor

in connection with the provision of service

via remote access on instruments

Contents

1 Introduction

This data processor agreement applies when the Data Processor Processes Personal Data on behalf of the Main Data Processor, Oslo University Hospital. The agreement is used for services established in the Network of the Data Controller when the contractual relationship is to be regulated directly between the Main Data Processor and the Data Processor in connection with instruments via remote access ,without Sykehuspartner HF being a contracting party.

The Data Processor and Main Data Processor, jointly referred to as “the Parties”, have entered into this Data Processing Agreement, henceforth called the "Agreement".

1.1 Footnotes

Where reference is made to documentation or information by footnotes with an electronic URL, the Main Data Processor and the Data Processor must ensure that he reads and understands them.

2 Objectives of the Agreement

The objective of this Agreement is to regulate the Data Processor`s connection with personal information on behalf of the Main Data Processor. The Agreement ensures that personal information is handled

- in accordance with the requirements laid down in personal data protection laws and regulations,
- according to this Data Processing Agreement, and
- according to instructions provided by the Main Data Processor.

The Processing of Personal Data covers only the processing necessary for the Data Processor to fulfil service via remote access on the instruments.

3 Definitions

The Data Processor Agreement shall be understood on the basis of the following definitions:

Personal Data Protection Laws and Regulations[1]:	The Personal Data Protection Laws and Regulations are to be understood as: a) Personal Data Act of 2018 implementing regulation (EU) 2016 679 of the European Parliament and of the Council of 27 April 2016 into Norwegian law b) The GDPR (General Data Protection Regulation); Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016. Unless otherwise specifically stated, any reference to the GDPR shall be understood as a reference to the implementation of the GDPR into Norwegian law; c) The Privacy and Electronic Communications Regulation; proposal for Regulation 2017/0003 of the European Parliament and of the Council (Regulation on Privacy and Electronic Communications), if and from when the regulation is adopted and implemented into Norwegian law; d) Any other applicable Norwegian acts and regulations that regulate the Data Processor’s Processing of Personal Data, as well as sectoral legislation.

[1] The term “Personal Data Protection Laws and Regulations” refers to all legislation relevant for personal data protection. This includes, but is not limited to: Statutory law and administrative law, as well as EU directives, regulations and decisions.

Personal data:	Any information relating to an identified or identifiable natural person ("the data subject"), cf. GDPR Art. 4 (1).
Processing:	Any operation or set of operations that are performed on personal data, whether or not by automated means, such as collection, registration, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission("Date"), dissemination or otherwise making available, alignment or combination, restriction, deletion or destruction, cf. GDPR Art. 4 (2).
Data controller:	Natural or legal person, which, alone or jointly with others, determines the purposes and means of the processing of Personal Data, cf. GDPR Art. 4 (7).
Data processor:	Natural or legal person, who processes Personal Data on behalf of the Main Data Processor, cf. GDPR Art. 4 (8).
Risk Assessment	A Risk Assessment specifies and describes what the Main Data Processor has ordered of specific operating services from the Data Processor, such as software or hardware, and what personal data is processed. ROS also contains all relevant information under the GDPR.
Service plan agreement	The service plan agreement regulates the commercial matters related to the deliveries of service from Data Processor, and regulates what can be ordered, what requirements can be set for the delivery and which pricing mechanisms can be used as a basis.
Third-party state or international organisation:	Transmission of Personal Data that is processed or to be processed after transfer to a third country or to an international organization which does not ensure an adequate level of protection without there being a basis for transfer, such as countries outside the EEA
Subcontractor:	Natural or legal person contracted by the Data Processor, intentionally or not, to perform the Processing of Personal Data.
Regional management system for information security:	Helse Sør-Øst's common management system for information security ensures that the region collectively complies with the current information security requirements for the collection, registration, storage, disclosure and closing of personal data, including coded/anonymised information. Moreover, the management system for information security applies regardless of how the information is collected technically and thus also encompasses the collection of personal data by means of technical medical equipment (TME) and other means of collecting information. This encompasses the use of personal data based on the Patient Medical Records Act, Health Register Act, Medical Research Act, Personal Data Act, etc., in which the Personal Data Act and Personal Data Regulations provide key guidelines for information security.
Breach of Personal Data Security or Breach:	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise Processed. Such a Breach of Personal Data Security is not dependent on a breach of the Personal Data Protection Regulations, cf. GDPR Art. 4 (12).

4 Data Processor's Processing of Personal Data

4.1 Grounds for processing

The Main Data Processor is responsible for specifying the grounds for processing.

Grounds for processing
☒ Statutory authority
☐ Consent
☒ Contract
☐ Other, specify:

4.2 Purpose and nature of the processing

The Data Processor may have access to Personal Data in connection with service via remote access to the instruments.

Purpose and nature of the processing
The purpose of the Processing is to perform according to the Annual Maintenance Plan (AMP) and during additional services as mentioned in the AMP under customer responsibilities. In connection with fulfilment of the Data Processor Agreement, the Data Processor may perform Processing in the form of access. Such Processing will only take place in accordance with the provisions of service on the instrument, and only in accordance with formal, documented instructions from the Data Processor. The Processing will, when needed, take place on the PC's connected to the instruments. The software is used to have management of instruments, and to handle and process analytical data generated on the instruments at the Main Data Processors sites.

The Data Processor shall not Process Personal Data to a greater extent than is necessary in order to fulfil the Data Processor Agreement. Other Processing may only take place in exceptional cases and for short periods of time, and only in accordance with formal, documented instructions from the Main Data Processor.

If the Data Processor is in doubt about whether the Processing of certain Personal Data is necessary, or within the scope of the Data Processor Agreement, the Main Data Processor shall be consulted immediately and before the start of any Processing.

Under no circumstances is the Data Processor entitled to process Personal Data or other data that belongs to the Main Data Processor for his own purposes, and beyond the purposes that are necessary in the service on the instruments.

If the Data Processor is required to perform more extensive Processing pursuant to laws or corresponding instructions from a public authority, the Data Processor is obligated to notify the Main Data Processor, and to ensure future confidentiality and security in accordance with the Data Processor Agreement.

4.3 Categories of Personal Data and data subjects

In connection with service on the instrument, the Data Processor can Process the following Personal Data:

Data on the instrument that contain case numbers, which is personal for a sample donor.

The Personal Data will refer to the following types of persons:
☐ Employee
☐ Supplier
☐ Patient
☐ Close family members
☐ Former employee
☐ Contracted consultants
☒ Other, specify: Sample donor, persons subjected to examination during the investigation of criminal law cases and civil law

4.4 Area of Processing

The Data Processor shall only Process Personal Data on the PC connected to the instrument, or otherwise as agreed between the Parties.

Any transmission shall satisfy the security requirements and protection requirements for the rights of the data subjects as stipulated in this Data Processor Agreement and in accordance with the Personal Data Protection Regulations.

Area for processing
Norway

4.5 Duration of the Processing

The Processing is not time-limited and lasts until the Data Processor Agreement is terminated.

5 Relationship between Main Data Processor and Data Processor

Only the Main Data Processor can accept the change of risk, and the Main Data Processor must therefore approve the use of services on the basis of performed and processed risk assessment before the data processing can start.

6 Role and responsibility of the Data Processor

The Data Processor has an independent responsibility for ensuring that the Processing of Personal Data is in accordance with

a) Personal Data Protection Laws and Regulations

b) Norms for Information Security[2]

c) regional[3] and internal[4] information security management system, and

d) this Data Processor Agreement

The Data processor shall assist the Main Data Processor in ensuring compliance with their obligations to maintain the security of Personal Data by

a) taking any technical or organizational action that is necessary to maintain security as stipulated in the Personal Data Protection Laws and Regulations, and comply with the conditions of this Data Processor Agreement;

b) ensuring that the Personal Data that is Processed is kept separate from the data of other parties;

[2] Norm for informasjonssikkerhet i helse- og omsorgssektoren
[3] Felles regionalt styringssystem for informasjonssikkerhet
[4] Sykehuspartner ISMS

c) being able to document the system and routines for the processing of Personal Data, including, but not limited to, descriptions of routines for authorization and usage, as well as technical and organisational security measures;

d) submitting, upon request, such documentation as mentioned above, in c), to the Main Data Processor, Data Protection Authority, Norwegian Board of Health Supervision, and other regulatory authorities;

e) the Data Processor shall inform the Main Data Processor immediately of any suspicion that the instructions conflict with the GDPR or personal data protection laws and regulations;

f) assisting the Main Data Processor with the assessment of privacy consequences in accordance with the Personal Data Protection Laws and Regulations if there is a likelihood of a particular data processing posing a high risk to the data subjects` rights and obligations;

g) keeping records of its own data processing activities in accordance with the Personal Data Protection Regulations.

7 Data Processor's information security requirements

7.1 General requirements

The Data Processor is obligated to process personal information in accordance with Personal Data Protection Laws and Regulations, this Agreement, the shared regional information security management system at the Southern and Eastern Norway Regional Health Authority (HSØ) and the Main Data Processor's management system, as well as to ensure that all Processing of Personal Data covered by this Data Processor Agreement is in accordance with the Main Data Processor`s stipulated acceptable risk level.

To achieve a level of safety that is appropriate in relation to the risk, the Data Processor shall carry out relevant technical or organisational measures, by, for example:

a) Ensure the ability to maintain the confidentiality, integrity, availability and robustness of the processing systems and services.
b) Ensure the ability to restore the availability of and access to Personal Data at the right time if a physical or technical event occurs.
c) Ensure that processes are in place for regular testing, analysis and evaluation of the effectiveness of the technical and organisational security measures for the processing.
d) Prevent that computer systems that process Personal Data are used by or provide access to Personal Data to persons who are not authorised, including access to reading, copying, modifying or deleting Personal Data without authorisation.
e) Ensure that there is an event log for all access to and use of the system in accordance with the Personal Data Protection Regulations, including requirements for the logging of remote access events.

7.2 Data Processor's measures

The Data Processor shall, following instructions from the Main Data Processor, prepare security objectives, strategy and organisation in accordance with Personal Data Protection Laws and Regulations.

The Data Processor is also required to follow up on these with a satisfactory internal control system and other planned and systematic measures, including documentable procedures for logging errors, nonconformities, notification of nonconformities and nonconformities management.

7.3 Technical security requirements

The following minimum technical security requirements shall be implemented by the Data Processor when relevant:

a) Only authorised employees shall have access to Personal Data, and access to services and data in the network shall be based on individual user codes and passwords given by Main Data Processor.

b) Personal Data shall be protected from negligent disclosure. Personal Data shall not be moved out of secure zones or from an approved storage site.

c) Security shall be maintained during remote operation. Remote access to the instruments is only given through Sykehuspartners remote access system.. Any equipment used in connection with remote access shall not be used by friends, family or other unauthorised parties.

d) Level 2 authentication shall be used if the access is through an unsecured network.

e) Communication shall be secured by encryption if it is transmitted over an unsecured network.

7.4 Access control requirements

The Data Processor shall have routines for access authorisation and management that ensure that only the employees of the Data Processor who have a genuine need for access to the system and the Personal Data have access. The access level shall be in accordance with a genuine need related to performance of service on instruments.

The Data Processor shall have a list of its personnel authorised to access to the data and services related to service on instruments. It shall be possible to present such a list to the Data Processor on request.

If the Main Data Processor object to the fact that one or more named persons have physical and/or electronic access to the system, their authorisation shall be revoked.

The Data Processor shall use a temporary password given by the Main Data Processor. The passwords will be blocked immediately, when access is no longer required.

7.5 Risk assessment in the event of changes to the data processing

Any modification of the Processing by a Data Processor that has or may be of importance to information security shall be risk assessed by the Main Data Processor before the modification is implemented, possibly with additional measures, as instructed by the Data Processor.

8 Notification and assistance in the event of non-conformity

The Data Processor shall, without undue delay, notify the Main Data Processor of a breach or possible breach of security, including accidental or unlawful destruction, loss, alteration,

unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise Processed, including as a minimum where there is a Breach of Personal Data Security. Immediately after the notification of a Breach of Personal Data Security, the Data Processor shall implement measures to control and correct the non-conformity and reduce any negative effects. If deemed necessary to clarify what has happened, the Data Processor shall cooperate with the Norwegian Data Protection Authority.

The Data Processor shall notify the Main Data Processor if an instruction infringes the Personal Data Protection Laws and Regulations.

The Main Data Processor`s Data Protection Officer shall also be notified immediately.

8.1 What to include in the notification

The Data Processor shall provide a notification of security breaches and non-conformity to the Main Data Processor, describing of the following:

a) Submitter`s org. number, address, postal code and location

b) The breach/non-conformity, including explanation of the cause, time period, the time when the breach/non-conformity was discovered, how many may be affected by the deviation, what kind of personal data was affected, etc.

c) Consequences for the persons concerned, and

d) Measures taken and planned to prevent the incident from occurring again

9 Processing liability / Liability for breaches and non-conformity

The Data Processor is only liable for damage caused by the Data Processor`s Processing, and only in cases where there is a failure to comply with the requirements especially directed towards data processors as stated in Personal Data Protection Laws and Regulations, or if the Data Processor has failed to comply with, or acted contrary to, the instructions of the Data Processor.

If the Main Data Processor has been involved in the Processing, the Data Processor has the right to reclaim the part of any compensation which corresponds to the Main Data Processor`s responsibility of the damage.

9.1 Material breach

In the event of a material breach, the Data Processor Agreement may be terminated with immediate effect.

The following shall always be regarded as a material breach:

a) Non-conformity or an information security failure that results in Personal Data going astray or being unlawfully disclosed to a third party, corrupted or otherwise damaged.
b) Failure to comply with security and information requirements, as well as express instructions given in accordance with this Data Processor Agreement.

c) Transmission of Personal data to a third party without an express agreement.
d) Failure to disclose defined non-conformity in the Data Processor's information security to the Main Data Processor.

10 Duty of confidentiality

The employees of the Data Processor and others who act on behalf of the Data Processor in connection with the processing of Personal Data in accordance with this Data Processor Agreement shall be subject to a duty of confidentiality.

This duty of confidentiality applies to all confidential data, the personal affairs of any individual, security-related and commercial affairs and information that may harm one of the Parties or that can be exploited by external parties.

The Data Processor shall ensure that anyone who processes Personal Data is familiar with the duty of confidentiality and has signed an adequate non-disclosure agreement. Employees who have access to Health Data shall be subject to a duty of confidentiality in accordance with the applicable regulations.

This duty of confidentiality remains in force after the termination of the Data Processor Agreement.

The Parties undertake to take the necessary precautions to ensure that materials and data are not disclosed to unauthorised individuals, and to submit documentation of such precautions on request.

11 Data Processor's use of Subcontractors

The Data Processor may not use Subcontractors to process Personal Data, including the transmission of Personal Data to such Subcontractors, unless the following conditions are fulfilled:

a) The Main Data Processor has approved the risk assessment
b) The Main Data Processor has in writing approved use of the Subcontractor
c) A separate, written subcontracting data processor agreement has been entered into with the Subcontractor, which includes requirements and obligations that correspond to those that follow from this Data Processor Agreement

The Data Processor is responsible for the subcontractors` execution of tasks being in the same way as if the Data Processor itself was executing these tasks. It is the responsibility of the Data Processor to ensure that Subcontractors are bound by the same contractual and statutory obligations as the Data Processor is subject to in accordance with this Data Processor Agreement, through separate, written data processor agreements.

The Data Processor shall ensure that any Subcontractor is informed about and actively undertake to observe the statutory duty of confidentiality.

The Main Data Processor and supervisory authorities are entitled to information on all Subcontractors, including the content of data processor agreements and information on technical and organisational measures implemented by the Subcontractor in order to comply with the Personal Data Protection Laws and Regulations.

12 Transmission

The Data processor shall not transmit Personal Data to third-party countries or international organisations unless this has been approved by the Main Data Processor.

12.1 Transmission to a third-party country or international organisations

Transmission to third-party countries and international organisations that have not been approved by the European Commission may only take place on the following conditions:

a) The transmission does not infringe the Personal Data Protection Laws and Regulations, and
b) a risk assessment has been conducted and approved in writing by the Main Data Processor before the transmission starts.

The Data Processor acknowledges that transmission to a third-party country outside of the EU/EEA is not a static concept related to the geographic location of the Processing, but a dynamic concept related to any data processing that is carried out in connection with this Data Processor Agreement.

Provided that the Main Data Processor has approved transmission to a third-party country outside of the EU/EEA in writing, the Data Processor must ensure that the transmission:

a) Takes place based on a decision on an adequate level of protection, by means, for example, of standard EU contracts, or

b) Will be encompassed by other forms of necessary guarantees, or

c) Will be encompassed by approved binding corporate rules.

13 Access, verification, audits, etc.

The Main Data Processor may at any given time request access to and verification of the Data Processor's processing of Personal Data, which encompass, but are not limited to, documentation to verify fulfilment of the requirements for information security and the internal control systems.

The right to access applies to all technical, organisational and administrative factors that are relevant to the security of the service, including, but not limited to:

a) Relevant documentation, including test documentation.

b) Interviews and meetings with the employees of the Data Processor for verification purposes.

c) Documentation related to security monitoring of network traffic and server activity.

The Main Data Processor 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. Audits and inspections can be carried out by the Main Data Processor or by a third party appointed by the Main Data Processor.

The Data Processor shall give the Norwegian Data Protection Authority and other relevant supervisory authorities the same access as mentioned above.

The Data Processor shall correct any non-conformity that is identified pursuant to the audit without undue delay, and shall report in writing on any corrective actions and implementation plans.

14 Duration and termination of Processing

The Data Processor Agreement takes effect from when it is signed and is applicable for as long as the Data Processor Processes or has access to Personal Data. The Data Processor Agreement may be revised as required for adaptation to mandatory statutory provisions and interpretations of the GDPR that necessitate such revision.

The Main Data Processor may choose to suspend further Processing at any given time, or request that the methods of Processing used by the Data Processor for the Personal Data are changed.

15 Termination

When the Data Processor Agreement expires, the Data Processor shall prepare for and contribute to the transmission (return) of all the Data that Data Processor Processes on behalf of the Main Data Processor. The Parties will agree in more detail on how the transmission will specifically take place.

After the Data has been transmitted to the Main Data Processor, and he has confirmed receipt of the data, the Data Processor shall delete all the data in his system. The requirement of deletion also applies to backup copies of Personal Data from the period of time after the ordinary Processing ended until the return has been completed.

The Data Processor shall give the Main Data Processor written confirmation that the information has been transmitted and deleted as stated above.

If the Data Processor has entered into an agreement with a Subcontractor, the Subcontractor's Processing shall end no later than at the same time as under this Data Processor Agreement, and the Data Processor shall ensure that the Subcontractor fulfils his obligations in the same manner as the Data Processor.

If, pursuant to a statutory obligation, further Processing of Personal Data is necessary after the Data Processor Agreement has expired, the Data Processor is obligated to perform such Processing of Personal Data free of charge.

16 Governing Law and venue

The agreement is subject to Norwegian law and the parties adopt the Oslo District Court as venue. This also applies after termination of the agreement.

17 Signatures

This Data Processor Agreement is signed in two copies; one for each party.

Place: _____, on __/__/____.

_____	_____
Main Data Processor (signature)	Data Processor (signature)
_____	_____
(in block letters)	(in block letters)
Position: _____	Position: _____