SUBCONTRACTING PROCESSOR AGREEMENT

between

SYKEHUSPARTNER HF

Org.no 914 637 651

hereinafter referred to as "*the Data Processor*"

and

[NAME OF SUPPLIER]

Organisation number [XXX XXX XXX]

hereinafter referred to as "*the Subcontracting Data Processor*",

in connection with the provision of services in accordance with the Master Agreement in force at any given time

on behalf of

[data controller(s)],

hereinafter referred to as "*the Data Controller*"

Contents

1 Introduction and purpose

This data processor agreement, hereinafter referred to as "the Subcontracting Data Processor Agreement", applies when the Subcontracting Data Processor Processes Personal Data on behalf of the Data Processor.

The Data Processor and Subcontracting Data Processor are jointly referred to as "the Parties".

The purpose of this Subcontracting Data Processor Agreement is to regulate the Subcontracting Data Processor's Processing of Personal Data on behalf of the Data Processor in connection with [name of the commercial agreement(s) that applies to the service(s) to which this Data Processor Agreement applies], hereinafter referred to as "the Master Agreement".

The Subcontracting Data Processor Agreement shall ensure that Personal Data is processed:

- in accordance with the requirements that apply at any given time in the Personal Data Protection Regulations,
- in accordance with this Subcontracting Data Processor Agreement, and
- in accordance with formal, documented instructions from the Data Processor.

The Subcontracting Data Processor's processing of Personal Data shall be limited to Processing that is necessary for the Subcontracting Data Processor's fulfilment of the Master Agreement with the Data Processor.

The Subcontracting Data Processor Agreement may be revised as required for adaptation to mandatory legislation, interpretations of the GDPR and the Personal Data Protection Regulations. Any changes to this Subcontracting Data Processor Agreement shall be agreed on and documented in writing.

1.1 Document hierarchy

The Parties agree that if there is a conflict, or a conflict arises between the Master Agreement and this Subcontracting Data Processor Agreement, then the provisions of this Subcontracting Data Processor Agreement shall take precedence.

1.2 Footnotes

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

If the electronic URL does not work, or if the Subcontracting Data Processor cannot otherwise retrieve the information to which reference is made, it is the responsibility of the Subcontracting Data Processor to request such information and have it sent.

1.3 Definitions

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

Personal Data Protection Regulations:	The Personal Data Protection 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 regulaltion 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.
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).
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).

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). In Helse Sør-Øst, the term Data Controller is used instead of process controller, even in those cases where the term process controller is used in the Personal Data Protection Regulations.
Data processor:	Natural or legal person, who processes Personal Data on behalf of the Data Controller, cf. GDPR Art. 4 (8).
Health data:	Any information related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status, cf. GDPR Art. 4 (15), as well as genetic and biometric data, cf. same article (13) and (14).
Master agreement:	The Master Agreement governs the commercial matters related to the deliveries from the Subcontracting Data Processor, and it governs, among other things, the requirements applicable to the delivery and what the delivery will cost.
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.
Subcontractor:	Natural or legal person contracted by the Subcontracting Data Processor, intentionally or

	not, to perform the Processing of Personal Data.
Third-party state or international organisation:	States that are not EU/EEA members.

2 Appendices

The following appendices shall be enclosed with the Subcontracting Data Processor Agreement by the Subcontracting Data Processor:

Appendix 1	Relevant technical and organisational measures implemented by the Subcontracting Data Processor, cf. Section 5.1
Appendix 2	List of relevant subcontracting data processors / Subcontractors, cf. Section 9

3 Subcontracting Data Processor's Processing of Personal Data

3.1 Grounds for processing

The Data Controller is responsible for specifying the grounds for processing.

Grounds for processing

□ Statutory authority

□ Consent

□ Contract

□ Other, specify:

3.2 Purpose and nature of the processing

The Subcontracting Data Processor will have access to Personal Data in connection with [the service that is to be provided, such as support, operations management, etc.] of [the system to which the service applies] in accordance with the Master Agreement.

Purpose and nature of the processing
The purpose of the Processing is to [describe the purpose]. In connection with fulfilment of the Master Agreement, the Subcontracting Data Processor may perform Processing in the form of [access, organisation, structuring, adaptation, retrieval, conversion, storage, relocation, consultation and destruction]. Such Processing will only take place in accordance with the provisions of the Subcontracting Data Processor Agreement and Master Agreement, and only in accordance with formal, documented instructions from the Data Processor. The Processing will primarily take place in [system X / through support in the supplier's systems etc.]. [NOTE: Describe the relevant processing activities. Insert the Processing that takes place in the Data Processor's and/or Data Controller's computer systems. Give preferably an explanation/specification of the system.]

The Subcontracting Data Processor shall not Process Personal Data to a greater extent than is necessary in order to fulfil the Master 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 Data Processor.

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

Under no circumstances is the Subcontracting Data Processor entitled to process Personal Data or other data that belongs to the Data Controller for his own purposes, and beyond the purposes that are stated in the Subcontracting Data Processor Agreement or Master Agreement.

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

3.3 Categories of Personal Data and data subjects

In connection with the fulfilment of the Master Agreement, the Subcontracting Data Processor will Process the following Personal Data:

The Master Agreement necessitates the Processing of the following Personal Data:

name, telephone number, e-mail address, etc. [communication data, documents and text, financial information, special categories of information, behavioural data, photos, etc.].

The Personal Data will refer to the following types of persons:

□ Employee

□ Supplier

□ Patient

□ Close family members

□ Former employee

□ Contracted consultants

□ Other, specify:

3.4 Area of Processing

The Subcontracting Data Processor shall only Process Personal Data within the geographic area as stipulated in the Master Agreement, 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 Subcontracting Data Processor Agreement and in accordance with the Personal Data Protection Regulations.

Area for processing
Norway: YES/NO EU/EEA country, which: Third-party countries that have been approved by the European Commission: Other countries:

3.5 Duration of the Processing

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

4 Role and responsibility of the Subcontracting Data Processor

The Subcontracting Data Processor has an independent responsibility for ensuring that the Processing of Personal Data is in accordance with the Code of Conduct[1] and the regional[2] management systems for information security.

If a decision is made to make amendments to the Regional Management Systems for Information Security that are of importance to the Processing in accordance with this Subcontracting Data Processor Agreement, the Subcontracting Data Processor shall be notified of this.

4.1 Assistance to the Data Processor

The Subcontracting Data Processor is obligated, without compensation or other remuneration, to:

a) Process Personal Data only in accordance with instructions from the Data Processor, and only in accordance with the purpose of the Master Agreement. The Subcontracting Data Processor shall immediately send any instructions received directly from the Data Controller to the Data Processor for an assessment.

b) Ensure that the Personal Data that is Processed is kept separate from the data of other parties.

c) Take any action that is necessary to maintain security, taking into consideration the Processing that is carried out on behalf of the Data Processor, and to regularly and on its own initiative carry out an analysis and perform testing of such proportionate security measures, including an assessment of their effectiveness.

d) Assist the Data Processor and Data Controller in ensuring compliance with their obligations to maintain the security of Personal Data and assess the privacy consequences, while taking into consideration the nature of the Processing and the information that is available to the Subcontracting Data Processor.

e) Assist the Data Processor and Data Controller, whenever possible, while taking into consideration the nature of the Processing, in fulfilling their obligation to fulfil requests that data subjects submit with a view to exercising their rights. If such a request from a data subject is submitted directly to the Subcontracting Data Processor, the request shall be sent to the Data Processor as stipulated in the notification rules in Section 6 of the Subcontracting Data Processor Agreement.

f) Assist the Data Processor and Data Controller in resolving non-conformity situations in cooperation with the Data Processor, if the non-conformity necessitates this, in accordance with the process for non-conformity as stipulated in this Subcontracting Data Processor Agreement.

[1] The Code of Conduct for information security in the health and care sector (https://ehelse.no/normen/normen-for-informasjonssikkerhet-og-personvern-i-helse-og-omsorgssektoren)

[2] Common regional management system for information security (https://www.helse-sorost.no/informasjonssikkerhet-og-personvern/ledelsessystem-for-informasjonssikkerhet#øvrig-sikkerhetsdokumentasjon-fra-sykehuspartner-hf)

g) In accordance with instructions from the Data Processor, delete or return all Personal Data and delete any existing copies, unless there is a statutory duty to continue storage of the data.
h) Immediately notify the Data Processor if the instructions infringes the Personal Data Protection Regulations.
i) Ensure that anyone who Processes Personal Data has committed themselves to confidentiality or are bound by a special statutory duty of non-disclosure, and that only such authorised persons with a genuine need for access pursuant to the Master Agreement, have or are granted access to Personal Data.
j) Be able to document the system and routines for the processing of Personal Data and keep records of its own data processing activities in accordance with the Personal Data Protection Regulations.

5 Subcontracting Data Processor's information security requirements

5.1 General requirements

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

a) Pseudonymising and encrypting Personal Data, including the encryption of data communications that contain sensitive personal data, as well as health and personal data in accordance with the applicable regulations if such data is, for example, to be transmitted to an external network.
b) Ensure the ability to maintain the confidentiality, integrity, availability and robustness of the processing systems and services.
c) Ensure the ability to restore the availability of and access to Personal Data at the right time if a physical or technical event occurs.
d) 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.
e) 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.
f) 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.

5.2 Subcontracting Data Processor's measures

The Subcontracting Data Processor is obligated to follow up the measures mentioned in Section 5.1 with a satisfactory internal control system and other planned and systematic measures, including documentable procedures for logging errors, non-conformity, notification of non-conformity and non-conformity processing.

5.3 Technical security requirements

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

a) Access to services and data in the network shall be based on individual user codes and passwords.
b) Only authorised employees shall have access to Personal Data.
c) All access to Personal Data shall be logged.
d) Personal Data shall be protected from negligent disclosure. There shall be technical measures in place to prevent that Personal Data can be moved out of secure zones or from an approved storage site.
e) Security shall be maintained during remote operation. An encrypted VPN connection shall be used, and simultaneous Internet access shall be blocked. Any equipment used in connection with remote access shall not be used by friends, family or other unauthorised parties.
f) Level 2 authentication shall be used if the access is through an unsecured network.
g) Communication shall be secured by encryption if it is transmitted over an unsecured network.

5.4 Access control requirements

The Subcontracting Data Processor shall have routines for access authorisation and management that ensure that only the employees of the Subcontracting 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 the Master Agreement.

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

If the Data Processor or Data Controller 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 Subcontracting Data Processor shall implement routines and the technical ability to delete, restrict or transmit to other parties a data subject’s data if the data subject is entitled to this pursuant to the Personal Data Protection Regulations and in accordance with the special legislation.

The Subcontracting Data Processor shall use a temporary password or similar device. It shall be possible to change/block the passwords immediately, including when access is no longer required.

5.5 Physical security requirements

The Subcontracting Data Processor shall have an access control system with access cards and personal codes or a similar device.

Access to restricted areas, such as an operations centre or server room, shall be based on a genuine need.

Access control by the means of locked doors shall be used for the following types of premises: data centres or server rooms, IT premises (operations/support), premises with IT-related equipment (switching matrices, switches/routers), and similar premises.

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

Any modification of the Processing by a Subcontracting Data Processor that has or may be of importance to information security shall be risk assessed and approved by the Data Processor and

Data Controller before the modification is implemented, possibly with additional measures, as instructed by the Data Processor.

6 Notification and assistance in the event of non-conformity

The Subcontracting Data Processor shall notify the Data Processor of the following without undue delay:

a) An instruction from the Data Processor or Data Controller that infringes the Personal Data Protection Regulations.
b) An order to disclose Personal Data from a public authority, except when such notification is prohibited.
c) A breach or possible breach of security that can lead to the 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.
d) Inquiries from a data subject allowing the Data Processor to respond, and without the Subcontracting Data Processor responding himself without having received explicit permission to handle the inquiry himself.

The Subcontracting Data Processor is obligated to provide adequate assistance to the Data Processor and Data Controller after any notification to the Norwegian Data Protection Authority regarding the Breach of Personal Data Security or to the data subject in connection with inquiries.

Any notification or inquiry to the Norwegian Data Protection Authority shall be communicated through the Data Processor. When necessary in order to clarify the scope of the Breach of Personal Data Security, the Subcontracting Data Processor shall assist the Data Processor in its cooperation with the Norwegian Data Protection Authority.

Immediately after the notification of a Breach of Personal Data Security, the Subcontracting Data Processor shall provide a more detailed description of the following to the Data Processor:

a) All relevant circumstances related to the Breach that the Subcontracting Data Processor has knowledge of, including what the Breach involves, categories of Personal Data and data subjects concerned, and an approximate number of data subjects and Personal Data records concerned. Circumstances related to the non-conformity that the Subcontracting Data Processor does not become aware of until after such notification, shall be reported to the Data Processor as soon as the Subcontracting Data Processor becomes aware of such.
b) What measures have been implemented, or for which implementation has been proposed, to mitigate the consequences and limit the scope of the Breach of Personal Data Security as well as submitting a plan for implementing the measures. With consent from the Data Processor, the Subcontracting Data Processor shall implement the measures as described in the plan. The Data Processor is entitled to make changes in the plan at all times. The Subcontracting Data Processor is not obliged to submit a written plan if corrective measures must be implemented immediately based on the nature of the Breach and the circumstances in general for example in situations where further Breache of Personal Data Security may be avoided. However, the Subcontracting Data Processor has a responsibility to notify the Data Processor as soon as the Subcontracting Data Processor is aware of the Breach of Personal

Data Security and is aware that corrective measures must be implemented without submitting an action plan.

In addition, the Subcontracting Data Processor shall assist the Data Processor in assessing the privacy consequences of such a Breach of Personal Data Security.

The Subcontracting Data Processor is obligated to notify the Data Processor if it becomes aware of the fact that it does not comply with, or suspect that it will be difficult to comply with the Personal Data Protection Regulations or this Subcontracting Data Processor Agreement, regardless of the cause. In such a case, the Data Processor may suspend further Processing of Personal Data by the Subcontracting Data Processor.

The Data Processor's data protection officer shall be notified at the same time.

7 Liability for breaches and non-conformity

For regulation of liability in the event of breaches and non-conformity, reference is made to the Master Agreement.

7.1 Material breach

In the event of a material breach, the Subcontracting 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 Subcontracting Data Processor Agreement.
c) Transmission of Personal data or Health data to a third party without an express agreement.
d) Failure to disclose defined non-conformity in the Subcontracting Data Processor's information security to the Data Processor.

8 Duty of confidentiality

The employees of the Subcontracting Data Processor and others who act on behalf of the Subcontracting Data Processor in connection with the processing of Personal Data in accordance with this Subcontracting 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 Subcontracting 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 Subcontracting 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.

9 Subcontracting Data Processor's use of Subcontractors

The Subcontracting 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 Data Processor has approved the risk assessment and received acceptance from the Data Controller.
b) The Data Processor has in writing approved use of the Subcontractor and received acceptance from the Data Controller.
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 Subcontracting Data Processor Agreement.

The Subcontracting Data Processor is responsible for the performance of tasks by Subcontractors as if the Subcontracting Data Processor had performed the tasks himself.

It is the responsibility of the Subcontracting Data Processor to ensure that Subcontractors are bound by the same contractual and statutory obligations as the Subcontracting Data Processor is subject to in accordance with this Subcontracting Data Processor Agreement, through separate, written data processor agreements.

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

The Data Processor, Data Controller 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 Regulations.

The Data Processor is entitled to three (3) months' notice if the Subcontracting Data Processor desires to replace a Subcontractor. The Data Processor and Data Controller are entitled to oppose the Subcontracting Data Processor's use or replacement of a Subcontractor when there is a legitimate reason for doing so, and it shall give the Subcontracting Data Processor notice in writing within 30 days after having received information on the replacement of a Subcontractor.

If the Subcontracting Data Processor does not demonstrate that the Data Processor's or Data Controller's opposition is unfounded, and maintains its replacement of the Subcontractor, the Data Processor or Data Controller is entitled to terminate the Master Agreement with the Subcontracting Data Processor with immediate effect.

10 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 Regulations and
b) A risk assessment has been conducted and approved in writing by the Data Processor with acceptance from the Data Controller before the transmission starts.

The Subcontracting 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 Subcontracting Data Processor Agreement. For the avoidance of doubt, it is considered a transfer to third countries outside the EU/EEA if the Personal Data can be accessed by personal outside the area even if the data is stored within the EU/EEA.

Provided that the Data Processor has approved and received acceptance from the Data Controller for transmission to a third-party country outside of the EU/EEA in writing, the Subcontracting 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.

11 Access, verification, audits, etc.

The Data Processor and/or Data Controller may at any given time request access to and verification of the Subcontracting Data Processor’s processing of Personal Data.

The Subcontracting Data Processor is obligated to give the Data Processor and Data Controller adequate access to, and documentation of, any information that is necessary to demonstrate compliance with the obligations stipulated in the Subcontracting Data Processor Agreement and to be able to conduct security audits. Such security audits encompass, but are not limited to, a local inspection and evaluation of the systems, organisation and security measures, as well as the use of Subcontractors.

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 Subcontracting Data Processor for verification purposes.
c) Documentation related to security monitoring of network traffic and server activity.

The Data Processor and Data Controller are entitled to appoint an independent auditor to conduct security audits of the Subcontracting Data Processor's compliance with this Subcontracting Data Processor Agreement, the Master Agreement and the Personal Data Protection Regulations. The auditor shall be subject to confidentiality obligations, and the Subcontracting Data Processor may not oppose the Data Processor's or Data Controller's choice of an auditor without a legitimate reason. The Subcontracting Data Processor is entitled, whenever possible, to one (1) week's notice of such a security audit.

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

The Subcontracting 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.

The Data Processor and Data Controller are not responsible for the Subcontracting Data Processor's costs in connection with security audits.

12 Duration and termination of Processing

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

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

13 Termination

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

After the Personal Data has been transmitted to the Data Processor, and he has confirmed receipt of the data, the Subcontracting 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 Subcontracting Data Processor shall give the Data Processor written confirmation that the information has been transmitted and deleted as stated above.

All access to the Data Processor's systems shall be blocked for the Subcontracting Data Processor and his personnel upon conclusion of the Processing. The Subcontracting Data Processor is obligated to assist the Data Processor in this connection.

If the Subcontracting 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 Subcontracting Data Processor Agreement, and the Subcontracting Data Processor shall ensure that the Subcontractor fulfils his obligations under this section 13 in the same manner as the Subcontracting Data Processor.

The Subcontracting Data Processor is not entitled to compensation for costs related to the transmission and deletion of Personal Data in accordance with this section 13.

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

14 Choice of law and legal venue

The Subcontracting Data Processor Agreement is governed by Norwegian law, and the Parties accept the Oslo District Court as their court of venue. This also applies after the conclusion of the Master Agreement.

15 Contact persons

The following contact persons have been appointed in connection with this agreement:

for the Data Processor:

Name: Position:

E-mail: Phone number:

for the Subcontracting Data Processor:

Name: Position:

E-mail: Phone number:

16 Signatures

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

Place: __________, on __/__/____. Place: __________, on __/__/____.

______________________ ________________________

Data Processor (signature) Subcontracting Data Processor (signature)

______________________ ________________________

(in block letters) (in block letters)

Position: _________________ Position: _________________