Data ethics and management plan

Research centre for digital mental health services (Forhelse) - a centre for research-based innovation (SFI)

Host Institution: Helse Bergen
Project leader: Tine Nordgreen
NFR-number: 309264
Financed by the Norwegian research council
Data ethics and management plan versjon 2 (17.10.2024)

Innhold

Overview

Purpose and scope

This data ethics and management plan is written with the purpose of giving a description of ethics related to data in Forhelse SFI, how the various work packages (WP) and sub-projects within the centre manages data and how we intend to share data in the project in a secure manner. The data ethics and management plan outline the steps necessary to share data in the centre and guides the research- health service and industry partners in how to handle data within the relevant legislation including data privacy/GDPR (General Data Protection Regulation). This plan adheres to the guidelines and recommendations from selected RRI projects in EU[1], as well as the overall RRI principals from Horizon Europe and Horizon 2020 as well as the RCN's strategy[2].

Background

In Forhelse SFI several of our sub-projects have, or will, collect research data. The data is varied and stems from several sources. Part of the research raw data will be sensitive personal data and requires an ethical approval. Where necessary there is a signed data management agreement in place.

Helse Bergen is the host institution for Forhelse SFI, and the centre has several research partners, including Oslo University Hospital, St. Olavs Hospital, and the Norwegian Centre for eHealth Research. In addition, Forhelse SFI has user partners in the form of, among other things, IT companies and health service partners such as municipalities and various parts of the specialist health service.

A premise in Forhelse SFI's general data ethics and management plan, is that all partners to the extent that they encounter personal data, must use their own local systems for internal control, data privacy, information security and routines for handling research data. Forhelse SFI does not offer a centralized service for this but lays down some guidelines and minimum requirements that all partners in the centre must meet.

The centre's management assumes that all partners comply with the relevant legislation including data privacy/GDPR (General Data Protection Regulation) for the processing of personal data linked to the various sub-projects.

Ethics

A clear perspective on ethics is important for the centre. We have described how we will handle ethics in our consortium agreement and will operationalize that in this document.

> From the consortium agreement:
>
> *5. Exploitation, communication, and data management.*
>
> *Plans for data management, including the use of portals, databases and archives will be described in detail in the first quarter of the centre, including a data ethics and data management plan with clear guidelines for practical data management. This will guide the consortium on how to*

[1] Responsible Research and Innovation (RRI) is a term used by the European Union's Framework Programmes to describe scientific research and technological development processes that take into account effects and potential impacts on the environment and society.

[2] See Strategy plans (forskningsradet.no)

safeguard and share any relevant data. The work process will support a responsible research- and innovation process, and the Responsible Research and Innovation framework from Horizon 2020 will guide this process. The centre (CMMH) will comply with general guidelines laid out in the General Data Protection Regulation (GDPR) and will confer with legal counsel from Haukeland University Hospital and from our technology transfer office in order to evaluate protective measures not covered by GDPR. Study participants will not be identifiable in any publications emanating from CMMH. All sensitive data will be stored according to Norwegian rules and regulations, and in accordance with the specifications in the approvals from the Regional Ethical Committee (REK). We will perform Data Protection Impact Assessment (DPIA) according to the Norwegian Data Protection Authorities guidelines when needed.

7. Research tasks and scientific methods
Ethical perspectives. There are several ethical issues to consider. As indicated in the description of the WPs, the project involves human data collection and processing of personal data (measures on mental health, demographics, activities). Clinical trials will be conducted in accordance with the principles stated in the Declaration of Helsinki. The clinical trials pose no threat of psychical injury, financial-, social- or legal harm to the participants. We will therefore comply with corresponding national guidelines to ensure the privacy of research subjects and the protection of data and the Health Research Act. Potential ethical aspects of the proposed research formed by the use and transfer of data from humans will be addressed by obtaining ethics approvals from the Regional Committees for Medical and Health Research Ethics and informed consent from all study participants. CMMH guarantees confidentiality and anonymous processing of data acting in accordance with the Guidelines for Research Ethics. All participants in the trials can withdraw their consent without negative effects. Furthermore, an Ethics and Data management plan will be delivered from work package (WP) 6 Management. This will guide the Project Consortium on how to safeguard the relevant ethical and data protection issues. In order to ensure considerations of ethical aspects in the innovation and exploitation phases, the project will be informed by the Responsible Research and Innovation framework as proposed in the framework program for research and innovation in Horizon 2020. A risk management plan will be developed during the first three months of CMMH. Risk management is a continuous process throughout the lifetime of the centre and addresses the planning of risk management, identification, analysis, monitoring and control. The Board will be presented the risk management plan at every meeting, where risks will be assessed and adjusted according to the experiences and results. At the centre (CMMH) the risks are related to collaboration between partners, collaboration between sectors, recruitment of participants to the effectiveness and cost-effectiveness trials, recruitment of participants to the HTA and implementation trials, change of healthcare policies, bankruptcy of business-partners.

In addition to the above it should be noted that participants who withdraw their consent have ethe right to get data deleted if not already used in analyses and/or published.

Practical ethical management

The centre management recommend that all partners familiarize themselves with the relevant guidelines for national research ethics committees (FEK) De nasjonale forskningsetiske komiteene | Forskningsetikk, see especially Retningslinjer og veiledere | Forskningsetikk including medicine and health sciences and general research ethics guidelines.

Guidelines for when one must conduct a DPIA can be found in this page:
https://www.datatilsynet.no/en/

We assume that processing of personal data in Forhelse SFI is only carried out when it is linked to purposes rooted in the centre, and that all involved partners in Forhelse SFI always process personal data in line with the guidelines in force. It is illegal to process and store personal data for other purposes than those included in the projects purpose, and as approved by REK/ other relevant bodies.

It is recommended that the templates attached at the end of the document be used by the partners in the centre.

Collection and/or reuse of existing data

Personal data in Forhelse SFI is collected and reused in various ways in the respective sub-projects. The centre's management assumes that the partners authorize the collection of personal data in the relevant legislation, and that the partners have a satisfactory system for information security management. Locally, collection and/or reuse should describe methods of collection, how data origin is to be documented, any limits for reuse of existing data, what type of data is collected, storage format and estimated data volume. A description of how data quality will be safeguarded during the project should also be prepared.

Consent

The work packages and sub-projects in Forhelse SFI will seek REK approval where it is deemed necessary. All REK approvals will then, in turn, have guidelines from their approval on the consent form that participants will sign. The REK application and approval will outline the purpose of data collection as well as the extent of data collecting. All consent forms give information about how to withdraw consent. REK approval also requires an assessment of possible negative effects on participants. REK approval gives clear directions on how to store data and secure the privacy of the participants. We refer you to “data storage” below to read more about how to store research data.

Data minimization

Our partners must ensure that the personal data that is shared is minimized according to GDPR standards of data minimizing, so that only data necessary to do project work is shared and processed.

Security routines when updating IT platforms

In Forhelse SFI, there are several suppliers of IT platforms that contribute to the development of digital healthcare services. It is assumed that each IT supplier takes care of IT security when platforms are updated and has routines to take care of this.

In addition, such suppliers must have routines for incident handling and processes for security updates of platforms and systems.

More details are provided in sections 8.1.2 and 8.2 in the appendix "data processing agreement".

Transfer of personal data for research purposes

In Forhelse SFI, there are several cases where personal data must be transferred between organizational units and data storage devices, for example from an IT-supplier to a research server at one of the research partners. We assume that when personal data is transferred between units, this is done in line with current legislation and measures are put in place to minimize the risk of data leaks and unnecessary storage of data in multiple locations.

Project partners who handle personal data must have a plan for how data can be recovered and how it can be shared securely in line with current legislation. The parties must have a conscious relationship with whether data can be reused for new purposes or not, and whether, in that case, new permissions must be obtained for new purposes. We recommend that a persistent identifier (DOI) is used for the datasets.

Data storage

In Forhelse SFI data will not be stored at one centralized location, but rather at safe locations at the site of different partners. The centre's management assumes that all partners comply with the relevant legislation including data privacy/GDPR (General Data Protection Regulation) for the storage of personal data linked to the various sub-projects. In addition, Forhelse SFI has some minimum requirements for how our partners and sub-projects handle personal data:

Digital locations

All the partners in the sub-projects who are responsible for storage and data security during the sub-projects must have routines for backing up data, how data should be restored in the event of accidental incidents, routines for who should have access to personal data and control of this access. Only approved storage facilities for research data can be used.

Physical location

Physical data include sound files, videos, participant lists and notes. All physical data are temporary and will be safely discarded when transcribed and moved to digital storage or when they are not necessary to carry out the study. Access to these physical data is monitored by local relevant management. Only approved storage facilities for research data can be used.

Competence building

The centre's management recommends that all partners in Forhelse SFI build expertise related to personal data protection and research, as well as develop and implement local routines for data management. We also refer to the section above in the data management plan "Practical ethical management".

Agreements

Current agreements

Consortium agreement

Forhelse SFI consortium agreement gives us a right and an obligation to share data within the project to secure the different partners ability to carry out their project work. The consortium agreement does not touch upon how data sharing will and should happen, nor does it outline what agreements might be required to do so.

Data management agreements

Data management agreements outline what data of a sensitive, personal and health nature are collected, who owns the data and who is responsible for storing the data. The subprojects in Forhelse SFI will have several data management agreements over the lifespan of the centre. All data management agreements are between the active participants of each subproject, and not for the consortium as a whole.

Data sharing agreement

A data sharing, or data access agreement, is made and will be used when sharing data with single researchers across organisations. The agreement presumes that a data request has been made, that a REK approval is present (where applicable) and that general GDPR guidelines are followed. The host institution, Helse Bergen, must have the right to receive and assess a copy of data processing agreements for the partners.

Beyond sharing – open access

The goal for data in Forhelse SFI is to share them as open access files. This is in line with what our funder, The Research council of Norway, expects and recommends. *"As open as possible and as closed as necessary".*

(Each research organisation is eligible to apply for refunds of open access publishing costs through STIM-OA from The Research Council of Norway, the STIM-OA program is extended to 2022).

Appendix

1. Template, data management agreement
2. Template data access agreement

Direktoratet for e-helse

Standard Data Processing Agreement for the Health and Care Services Sector

[for processing personal health data]

Pursuant to the Norwegian Personal Data Act and

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

between

[Name of organisation]

Organisation no.: 000 000 000

Controller

and

[Name of organisation]

Organisation no.: 000 000 000

Processor

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

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

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

Place and date:

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

For the Controller	For the Processor
Name: Insert	Name: Insert
Signature: _____	Signature: _____

Contents

1. About the agreement

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

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

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

Appendices to the agreement:

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

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

2. Definitions

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

3. Purpose of the Agreement

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

4. Scope

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

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

5. Purpose of the processing, data and processing activities

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

6. Framework for the processing of personal health data

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

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

7. The Controller’s obligations

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

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

8. The Processor's obligations

8.1. General

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

8.1.1 The Processor shall not:

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

8.1.2 The Processor shall:

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

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

8.2. Technical, organisational and security measures

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

At a minimum, the Processor shall:

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

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

c. have routines for internal control;

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

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

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

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

h. document any breach, including the factual circumstances linked to the breach, its impact and any remedial measures that have been implemented;

i. notify the Controller without undue delay in the event of the unauthorised disclosure of personal data;

j. register all authorised and unauthorised access to data. All look-ups that are performed shall be registered so that they can be traced to the individual user concerned (i.e. an employee of the Processor, a subcontractor or the Controller). The logs shall be retained until there is no longer considered to be any use for them or as stipulated by the Agreement or Service/assignment agreement;

k. assist the Controller with ensuring fulfilment of the obligations in Articles 32-34 of the General Data Protection Regulation, including but not limited to:
- security of processing;
- notification of a personal data breach to the supervisory authority;
- communication of a personal data breach to the data subject;

l. notify the Controller of circumstances related to the Processor's obligations under the Service/assignment agreement that entail or may be deemed to entail a weakness in information security;

m. obtain written approval from the Controller prior to the implementation of any change in the data processing by the Processor which is or could be of negative importance for information security when processing data in accordance with this Agreement.

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

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

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

9. Use of subcontractors

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

The Processor shall:

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

b. maintain an updated list of the identity and location of subcontractors specified in Appendix 4 and where they process personal data. The updated list shall be available to the Controller;

c. conduct a risk assessment concerning the use of subcontractors and the significance for the service before entering into an agreement with subcontractors and, at the request of the Controller, share the assessment with the Controller;

d. at the request of the Controller, present a copy of the agreement(s) that has/have been entered into with the subcontractors (with the exception of commercial conditions). Such agreements must be established before the subcontractors commence the processing of personal health data;

e. notify the Controller of any plans to use other subcontractors or substitute subcontractors. The Controller must be given sufficient advance notice of such substitutions in order to give the

Controller an opportunity to object to the change. In the event of the substitution of a subcontractor, Appendix 4 must be updated and sent to the Controller before a new subcontractor commences its work. The amendment must also be entered in Appendix 6;

f. ensure that the Controller and the supervisory authority have the same access and audit rights concerning the processing of personal data with respect to a subcontractor as the Controller has with respect to the Processor under Clause 12 of the Agreement;

g. in the event of the termination of the Agreement, ensure that subcontractors fulfil their obligation to return, erase or destroy in an appropriate manner all personal health data and any and all copies and back-up copies of the data as stipulated in Clause 13 of the Agreement.

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

10. Transfer of personal data to other countries

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

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

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

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

11. Obligations of secrecy

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

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

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

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

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

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

12. Audits

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

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

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

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

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

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

13. Duration and termination

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

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

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

After all the data has been transferred to the Controller and receipt of the data has been confirmed, the Processor shall irreversibly erase or destroy in an appropriate manner all the data and any copies and

back-ups of the data in its systems, unless other regulations require the personal health data to continue to be stored.

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

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

14. Amendments to the Agreement

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

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

15. Governing Law, disputes and venue

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

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

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

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

A. Purpose and duration of the processing

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

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

Name of service	Purpose of the processing	Duration of the processing

B. Processing of personal health data

The following processing is covered by the Agreement:

Processing	Processing activities

C. Types of data

The following personal health data are processed:

Personal data	Special categories of personal data: personal health data

D. Categories of data subjects

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

Categories of data subjects

APPENDIX 2 – DETAILED REQUIREMENTS CONCERNING INFORMATION SECURITY

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

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

No.	Topic	Requirement

APPENDIX 3 ADMINISTRATIVE PROVISIONS

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

Contact details

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

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

Other administrative provisions

The parties have agreed that:

Administrative provisions

APPENDIX 4 – SUBCONTRACTORS

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

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

The Processor uses the following subcontractors:

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

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

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

Change table:

Clause in the agreement	Replaced with

APPENDIX 6: AMENDMENTS AFTER THE AGREEMENT HAS BEEN ENTERED INTO

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

Catalogue of changes:

No.	Date	Change	Any appendices	Applies from

Direktoratet for e-helse

Standard databehandleravtale for helse- og omsorgssektoren

[for behandling av helse- og personopplysninger]

I henhold til personopplysningsloven og

EUs Personvernforordning (EU) 2016/679

mellom

[Virksomhetens navn]

Org.nr.: 000 000 000

Dataansvarlig

og

[Virksomhetens navn]

Org.nr.: 000 000 000

Databehandler

Denne databehandleravtalen er knyttet til følgende tjeneste/oppdragsavtale mellom partene:

Tjeneste/oppdragsavtalens tittel	Tjeneste/oppdragsavtalens dato	Tjeneste/oppdragsavtalens saksreferanse
Fyll ut	Fyll ut	Fyll ut

Databehandleravtalen undertegnes i to eksemplarer, ett til hver part.

Sted og dato:

[*sted*], xx.xx.20xx

For Dataansvarlig	For Databehandler
Navn: Fyll ut	Navn: Fyll ut
Underskrift: _____	Underskrift: _____

Innhold

1. Om avtalen

Denne databehandleravtalen med vedlegg (heretter omtalt som "Avtalen") regulerer rettigheter og plikter mellom Dataansvarlig og Databehandler (heretter omtalt som "partene") etter:

- Lov om behandling av personopplysninger av 15.juni 2018 nr. 38 (personopplysningsloven);
- Europaparlaments- og rådsforordning (EU) 2016/679 av 27.april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger (General Data Protection Regulation) (heretter omtalt som "personvernforordningen");
- Lov om helseregistre og behandling av helseregistre av 20.juni 2014 nr. 43 (helseregisterloven);
- Lov om behandling av helseopplysninger ved ytelse av helsehjelp av 20.juni 2014 nr. 42 (pasientjournalloven); og
- Enhver lov, forskrift eller annet regelverk som endrer eller erstatter ovennevnte regler.

Ved motstrid mellom Avtalens regulering og de rammer som følger av personvernregelverket eller relevant helselovgining, viker Avtalens regulering. I tilfelle konflikt mellom denne Avtalen og Tjeneste/oppdragsavtalen, skal denne Avtalen gjelde.

Vedlegg til avtalen:

- Vedlegg 1: Behandlingens formål, opplysninger og behandlinger
- Vedlegg 2: Detaljerte krav til informasjonssikkerhet
- Vedlegg 3: Administrative bestemmelser
- Vedlegg 4: Underleverandører
- Vedlegg 5: Endringer i den generelle avtaleteksten ved avtaleinngåelsen
- Vedlegg 6: Endringer etter avtaleinngåelsen

Endringer til den generelle avtaleteksten skal samles i vedlegg 5. Slike endringer erstatter den opprinnelige avtaleteksten.

2. Definisjoner

Begrepene "personopplysninger", "helseopplysninger", "behandling", "dataansvarlig", "databehandler", "brudd på personopplysningssikkerheten" og "helseopplysninger" skal forstås slik de er definert i personvernforordningen artikkel 4, helseregisterloven § 2 og pasientjournalloven § 2.

3. Avtalens formål

Formålet med Avtalen er å sikre de registrertes rettigheter og partenes etterlevelse av artikkel 28 nummer 3 i personvernforordningen.

4. Omfang

Denne Avtalen kommer til anvendelse på all behandling av helse- og personopplysninger som Databehandler foretar på vegne av Dataansvarlig på grunnlag av Tjeneste/oppdragsavtalen.

Denne Avtalen vil i tillegg gjelde for ytterligere behandling av helse- og personopplysninger basert på eventuelle skriftlige avtaler mellom partene som inngås i løpet av denne Avtalens varighet og som innebærer at Databehandler behandler helse- og personopplysninger på vegne av Dataansvarlig (heretter omtalt som "senere skriftlige avtaler mellom partene"). Slike tillegg skal fremgå av **Vedlegg 6**. Avtalens øvrige vedlegg skal oppdateres i samsvar med endringen.

5. Behandlingens formål, opplysninger og behandlinger

Formålet med og varigheten av behandling av helse- og personopplysninger, hvilke helse- og personopplysninger som behandles, kategorier av de registrerte og behandlingsaktiviteter er angitt i **Vedlegg 1.**

6. Rammene for behandling av helse- og personopplysninger

Dataansvarlig har til enhver tid full rådighet over de helse- og personopplysningene som Databehandler behandler etter denne Avtalen. Databehandler har ikke selvstendig råderett over helse- og personopplysningene, og kan ikke behandle disse til egne formål.

Dataansvarlig har, med mindre annet er avtalt eller følger av lov, rett til tilgang til og innsyn i helse- og personopplysningene som behandles hos Databehandleren.

7. Dataansvarliges plikter

Dataansvarlig skal etterleve de forpliktelser som følger av personvernregelverket, jf. personvernforordningen artikkel 24, relevant helselovgivning og annen særlovgivning, samt denne Avtalen.

Dataansvarlig er ansvarlig for at personvernprinsippene overholdes, jf. personvernforordningen artikkel 5, og skal blant annet sørge for at behandlingen av opplysninger er formålsbestemt og basert på et gyldig rettsgrunnlag.

8. Databehandlers plikter

8.1. Generelt

Databehandler forplikter seg til å behandle helse- og personopplysninger kun i samsvar med gjeldende regelverk, denne Avtalen, Tjeneste/oppdragsavtalen, Dataansvarliges dokumenterte instrukser og andre gjeldende avtaler mellom partene, samt "Norm for informasjonssikkerhet i helse- og omsorgssektoren". Databehandler skal ikke ved noen handling eller unnlatelse, sette Dataansvarlig i en slik situasjon at Dataansvarlig bryter gjeldende regelverk som angitt i Avtalen punkt 1.

8.1.1 Databehandler skal ikke:

d. behandle helse- og personopplysninger for andre formål eller i større grad eller på annen måte enn det som følger av denne Avtalen, Tjeneste/oppdragsavtale og eventuelle senere skriftlige avtaler mellom partene;
e. behandle helse- og personopplysninger utover det som er nødvendig for å oppfylle Databehandlers forpliktelser i henhold til de til enhver tid gjeldende avtaler;
f. utlevere, overlate, overføre eller innhente helse- og personopplysninger i noen form til eller fra tredjepart på eget initiativ, med mindre det er lovpålagt eller det på forhånd er avtalt med Dataansvarlig eller Dataansvarlig har godkjent dette skriftlig;

8.1.2 Databehandler skal:

j. ha løpende kontroll på alle kategorier av behandlingsaktiviteter utført på vegne av Dataansvarlig, jf. personvernforordningen artikkel 30 nr. 2, jf. også **Vedlegg 1**;
k. gi Dataansvarlig tilgang til og innsyn i helse- og personopplysninger som behandles hos Databehandleren på vegne av Dataansvarlig;
l. treffe alle rimelige tiltak for å bistå Dataansvarlig med å sikre at helse- og personopplysningene til enhver tid er korrekte og oppdaterte;
m. etablere rutiner for å slette opplysninger i henhold til instruks eller retningslinjer fastsatt av Dataansvarlig;
n. påse at samtlige personer som gis tilgang til personopplysninger som behandles på vegne av Dataansvarlig er kjent med denne Avtalen og gjeldende avtaler mellom partene, og er underlagt disse avtalenes bestemmelser;
o. gi Dataansvarlig nødvendig bistand slik at Dataansvarlig skal kunne oppfylle sine forpliktelser overfor de registrerte, herunder å svare på anmodninger fra den registrerte som vil utøve sine rettigheter fastsatt i personvernforordningen kapittel III;
p. uten ugrunnet opphold varsle den Dataansvarlige dersom Databehandler mener at en instruks er i strid med personvernforordningen eller andre bestemmelser om vern av personopplysninger;
q. bistå Dataansvarlig for å sikre overholdelse av forpliktelsene i personvernforordningen artiklene 35-36 som omhandler vurdering av personvernkonsekvenser og forhåndsdrøftinger med Datatilsynet;
r. Databehandler skal umiddelbart varsle Dataansvarlig hvis den mottar forespørsel fra en myndighet om å utlevere personopplysninger som er behandlet under Databehandleravtalen. Med mindre utleveringen er lovpålagt, skal Databehandler ikke etterkomme en slik forespørsel uten skriftlig forhåndsgodkjenning fra Dataansvarlig.

8.2. Tekniske, organisatoriske og sikkerhetsmessige tiltak

Databehandler plikter å treffe og gjennomføre alle tekniske, organisatoriske og sikkerhetsmessige tiltak slik at det til enhver tid er et sikkerhetsnivå som er egnet med hensyn til risikoen ved behandling av helse og personopplysninger.

Databehandleren skal, som minimum:

n. etablere og etterkomme nødvendige tekniske og organisatoriske tiltak med hensyn til vedvarende konfidensialitet, integritet, tilgjengelighet og robusthet ved behandling av helse- og personopplysninger for å sikre tilfredsstillende informasjonssikkerhet i henhold til

personvernregelverket, herunder kravene etter personvernforordningen artikkel 32, og gjeldende helselovgivning.

o. sikre at krav til innebygd personvern og personvern som standardinnstilling innfris i Databehandlers løsninger. Dette inkluderer å bygge inn funksjonalitet for å oppfylle personvernprinsipper samt funksjonalitet for å sikre den registrertes rettigheter, herunder retten til begrenset behandling;

p. ha rutiner for internkontroll;

q. ha rutiner for autorisasjon og styring som sikrer at bare de av Databehandlers medarbeidere som har tjenstlig behov for tilgang til systemer og opplysningene for å ivareta nødvendige oppgaver for gjennomføring av Tjeneste/oppdragsavtalen får slik tilgang. Tilgangsnivået skal være i henhold til tjenstlig behov knyttet til å gjennomføre oppdraget. Det skal etableres sterk autentisering for tilgang til helseopplysninger;

r. etablere nødvendige systemer og rutiner for å ivareta informasjonssikkerheten og følge opp avvik, som skal omfatte blant annet rutiner for avviksmelding, rutiner for backup, gjenoppretting av normalsituasjonen, fjerne årsaken til avviket og hindre gjentakelse. På forespørsel, skal Databehandler gi Dataansvarlig tilgang til relevant sikkerhetsdokumentasjon for behandling av helse- og personopplysninger;

s. avdekke, registrere, rapportere og lukke avvik knyttet til informasjonssikkerhet, herunder loggføre og dokumentere ethvert forsøk på ikke-autorisert tilgang og andre brudd på personopplysningssikkerheten i datasystemene. Slik dokumentasjon skal oppbevares hos Databehandler;

t. ved mistanke om eller konstatering av brudd på personopplysningssikkerheten, uten ugrunnet opphold varsle Dataansvarlig. I varselet opplyses avviket med forklaring om årsak, tidsrom og tidspunktet avviket ble oppdaget, kategoriene av og omtrentlig antall registrerte som er berørt, kategoriene av og omtrentlig antall registreringer av personopplysninger som er berørt, navnet på og kontaktopplysningene til personvernombudet eller et annet kontaktpunkt der mer informasjon kan innhentes, antatte konsekvenser av avviket og hvilke umiddelbare tiltak som er igangsatt eller vurderes igangsatt for å håndtere avviket. Dersom og i den grad det ikke er mulig å gi all informasjon samtidig, kan den gis trinnvis uten ytterligere ugrunnet opphold;

u. dokumentere ethvert avvik, herunder de faktiske forhold knyttet til avviket, dets virkninger og eventuelle iverksatte utbedringstiltak;

v. uten ugrunnet opphold varsle Dataansvarlig ved uautorisert utlevering av personopplysninger;

w. registrere all autorisert og uautorisert tilgang til opplysninger. Alle oppslag som gjøres skal registreres slik at de kan spores til den enkelte bruker (dvs. ansatte hos Databehandler, underleverandører og Dataansvarlig). Loggene skal oppbevares til det ikke lenger antas å være bruk for dem eller i henhold til det Avtalen eller Tjeneste/oppdragsavtalen spesifiserer;

x. bistå Dataansvarlig med å sikre overholdelse av forpliktelsene i personvernforordningen artiklene 32–34, herunder, men ikke begrenset til:
   - sikkerhet ved behandlingen;
   - melding til tilsynsmyndigheten om brudd på personopplysningssikkerheten;
   - underretning av den registrerte om brudd på personopplysningssikkerheten;

y. varsle Dataansvarlig om forhold relatert til Databehandlers forpliktelser under Tjeneste/oppdragsavtalen som medfører eller kan anses å medføre svekkelse av informasjonssikkerheten;

z. innhente skriftlig godkjenning av Dataansvarlig før gjennomføring av enhver endring av databehandlingen hos Databehandler som har eller kan ha negativ betydning for informasjonssikkerheten ved behandlingen etter denne Avtalen.

Nærmere krav til informasjonssikkerhet er angitt i **Vedlegg 2**.

Ved brudd på denne Avtalen eller på bestemmelsene i personvernregelverket, helselovgivningen eller annen relevant lovgivning kan Dataansvarlig kreve endringer i behandlingsmåten eller pålegge Databehandler å stoppe den videre behandlingen av opplysningene med øyeblikkelig virkning.

Databehandler skal dokumentere sine rutiner og alle tiltak truffet for å oppfylle kravene angitt ovenfor. Denne dokumentasjonen skal på forespørsel gjøres tilgjengelig for Dataansvarlig.

9. Bruk av underleverandør

Dataansvarlig tillater at Databehandler benytter underleverandører for oppfyllelse av forpliktelsene under Avtalen. Databehandler benytter kun de underleverandører som er angitt i **Vedlegg 4** for de der angitte tjenester.

Databehandler skal:

h. sikre at underleverandøren påtar seg tilsvarende forpliktelser som Databehandler selv er underlagt etter Avtalen og gjeldende lovgivning;

i. holde en oppdatert liste over identiteten til og stedlig plassering av underleverandører som angitt i Vedlegg 4 og hvor disse behandler personopplysninger. Oppdatert liste skal være tilgjengelig for Dataansvarlig;

j. gjennomføre en risikovurdering av bruk av underleverandør og betydningen for tjenesten før det inngås avtale med underleverandør og på Dataansvarliges forespørsel, dele vurderingen med Dataansvarlig;

k. på Dataansvarliges forespørsel, legge frem kopi av avtalen(e) som er inngått med underleverandørene (med unntak av merkantile betingelser). Slike avtaler skal senest være inngått før underleverandørene starter med behandling av helse- og personopplysninger;

l. underrette Dataansvarlig om eventuelle planer om å benytte andre underleverandører eller skifte ut underleverandører. Slike bytter skal varsles Dataansvarlig i god tid slik at denne gis mulighet til å motsette seg endringen. Ved bytte av underleverandør skal Vedlegg 4 oppdateres og oversendes Dataansvarlig før ny underleverandør starter opp. Endringen føres også opp i Vedlegg 6;

m. sikre at Dataansvarlig og tilsynsmyndighetene har samme rett til innsyn og kontroll med behandling av personopplysninger hos en underleverandør som Dataansvarlig har overfor Databehandler etter Avtalens punkt 12;

n. ved opphør av Avtalen, sikre at underleverandører oppfyller plikten til å tilbakeføre, slette eller forsvarlig destruere alle helse- og personopplysningene og alle eventuelle kopier og sikkerhetskopier av opplysningene, slik som det framgår av Avtalens punkt 13.

Databehandler er til enhver tid fullt ut ansvarlig overfor Dataansvarlig for alt arbeid som utføres av underleverandører og for underleverandørenes etterlevelse av bestemmelsene i denne Avtalen.

10. Overføring av personopplysninger til utlandet

Partene i denne Avtalen er enige om at ingen av helse- og personopplysningene som behandles under denne Avtalen skal føres ut av Norge, med mindre det er særskilt avtalt mellom partene. I tillegg skal arkivverdige dokumenter med helse- og personopplysninger være plassert på servere i Norge (jf. arkivloven § 9 bokstav b), og eventuelle unntak fra dette skal godkjennes eksplisitt av Dataansvarlig før denne behandlingen starter.

Databehandler bekrefter at ingen av underleverandørene overfører helse- og personopplysninger som omfattes av denne Avtalen til utlandet, med unntak for slike overføringer som er angitt i **Vedlegg 4.** Dette omfatter også fjerntilgang fra utlandet.

Bruk av underleverandører som overfører helse- og personopplysninger til land utenfor EU/EØS (tredjeland) skal avtales skriftlig med Dataansvarlig på forhånd. Ved overføring av helse- og personopplysninger til land utenfor EU/EØS (tredjeland) skal Databehandler benytte godkjente EU-overføringsmekanismer.

Ved overføring til utlandet, uavhengig av om det er innenfor EU/EØS eller utenfor EU/EØS (tredjeland), skal Databehandler gi nødvendig dokumentasjon om sikkerhet, risiko og etterlevelsesnivå knyttet til aktuelle underleverandører slik at Dataansvarlig får nødvendig informasjon for å kunne gjennomføre en særskilt risikovurdering. Dataansvarlig kan nekte samtykke til den aktuelle overføringen basert på spesifikke risikoer som fremkommer av Dataansvarliges egen risikovurdering.

11. Taushetsplikt

Databehandlers ansatte og andre som opptrer på Databehandlers vegne i forbindelse med behandling av helse- og personopplysninger i henhold til denne Avtalen, Tjeneste/oppdragsavtale og senere skriftlige avtaler mellom partene, skal underlegges taushetsplikt etter denne Avtalen og gjeldende regelverk. Personer som er autorisert til å behandle helse- og personopplysningene forplikter seg til å behandle opplysningene fortrolig. Det samme gjelder eventuelle underleverandører.

Ansatte og andre som opptrer på Databehandlers vegne i forbindelse med behandling av helse- og personopplysninger skal ha undertegnet taushetserklæring. Bestemmelsen gjelder tilsvarende for underleverandører.

Databehandler skal påse at alle som behandler personopplysninger under Avtalen er kjent med taushetsplikten.

Partene har i tillegg taushetsplikt om konfidensiell informasjon knyttet til hverandres virksomhet, som er formidlet i forbindelse med oppdraget.

Partene plikter å ta de forholdsregler som er nødvendige for å sikre at materiale eller opplysninger ikke blir gjort kjent for andre i strid med dette punktet.

Taushetsplikten gjelder også etter Avtalens opphør.

12. Revisjon

Databehandler skal på forespørsel gjøre tilgjengelig for den Dataansvarlige, all informasjon som er nødvendig for å påvise at Databehandlers forpliktelser fastsatt i personvernforordningen artikkel 28 og denne Avtalen er oppfylt.

Databehandler skal muliggjøre og bidra ved inspeksjoner og revisjoner som gjennomføres av eller på oppdrag fra Dataansvarlig. Databehandler skal framlegge interne revisjonsrapporter, interne prosedyrer, rutiner, sikkerhetsarkitektur, risiko og sårbarhetsanalyser med tiltak og andre dokumenter av betydning for revisjonen;

Databehandler skal også muliggjøre og bidra ved inspeksjoner fra aktuelle tilsynsmyndigheter. Den Dataansvarliges tilsyn med eventuelle underleverandører skal skje gjennom Databehandleren med mindre annet er særskilt avtalt.

Nærmere rutiner for gjennomføring av revisjoner kan avtales i **Vedlegg 3**.

Dersom en revisjon avdekker avvik fra forpliktelsene i gjeldende personvernregler eller Avtalen, skal Databehandler uten ugrunnet opphold utbedre avviket. Dataansvarlig kan kreve at Databehandleren midlertidig stopper hele eller deler av behandlingsaktivitetene frem til utbedringen er godkjent av Dataansvarlig.

Hver av Partene dekker sine egne kostnader forbundet med inspeksjoner fra aktuelle tilsynsmyndigheter og inntil én årlig revisjon initiert av Dataansvarlig. Hvis en revisjon avdekker vesentlige brudd på forpliktelsene etter gjeldende personvernregler eller Avtalen, skal Databehandleren likevel dekke Dataansvarliges rimelige kostnader forbundet med revisjonen.

13. Varighet og opphør

Databehandleravtalen gjelder fra den er signert av begge Parter og gjelder så lenge Databehandler behandler Personopplysninger på vegne av Behandlingsansvarlig.

I denne perioden gjelder Avtalen med mindre andre bestemmelser som regulerer Databehandlers behandling av Personopplysninger på vegne av Behandlingsansvarlig avtales mellom Partene.

Ved opphør av Avtalen skal Databehandler tilrettelegge for og medvirke til tilbakeføring av alle helse- og personopplysninger som Databehandler har mottatt og behandlet på vegne av Dataansvarlig. Partene avtaler nærmere hvordan overføring konkret skal skje.

Etter at alle opplysningene er overført til Dataansvarlig og bekreftet mottatt av denne, skal Databehandler irreversibelt slette eller forsvarlig destruere alle opplysningene og alle eventuelle kopier og sikkerhetskopier av opplysningene i sine systemer, med mindre annet regelverk krever at helse- og personopplysningene fortsatt lagres.

Benyttes delt infrastruktur der direkte sletting ikke er teknisk mulig skal Databehandler sørge for at data gjøres utilgjengelig inntil disse dataene er overskrevet av systemet.

Databehandler skal gi Dataansvarlig skriftlig bekreftelse på at opplysningene er overført og slettet som angitt over.

14. Endring av avtale

I tilfelle endringer i det rettslige rammeverket eller endringer i tjenester i Tjeneste/oppdragsavtalen som krever endringer av denne Avtalen, skal partene samarbeide for å oppdatere Avtalen tilsvarende.

Endringer etter avtaleinngåelsen listes opp i **Vedlegg 6.** Databehandler er ansvarlig for at det føres en slik endringskatalog og at denne holdes oppdatert.

15. Lovvalg, tvister og verneting

Avtalen er underlagt norsk rett. Tvister løses i samsvar med Tjeneste/oppdragsavtalens bestemmelser, herunder eventuelle bestemmelser om verneting.

VEDLEGG 1 – BEHANDLINGENS FORMÅL, OPPLYSNINGER OG BEHANDLINGER

[Versjon nr. XX, *dato/måned/år*]

Tabellene oppdateres ved endringer. Alle endringer skal føres opp i endringskatalogen i **Vedlegg 6.**

B. Formålet med og varigheten av behandlingen(e)

(Dersom databehandleravtalen knytter seg til flere tjenesteavtaler, må det spesifiseres hvilken avtale det gjelder.)

Formålet med og varigheten av behandling av helse- og personopplysninger er:

Navn på tjeneste	Formålet med behandlingen	Varigheten av behandlingen

B. Behandling av helse- og personopplysninger

Følgende behandlinger omfattes av Avtalen:

Behandling	Behandlingsaktiviteter

C. Typer av opplysninger

Følgende helse- og personopplysninger behandles:

Personopplysninger	Særlige kategorier av personopplysninger: helseopplysninger

D. Kategorier av registrerte

Følgende kategorier av personer behandles det opplysninger om (registrerte):

Kategorier av registrerte

VEDLEGG 2 – DETALJERTE KRAV TIL INFORMASJONSSIKKERHET

[Versjon nr. XX, *dato/måned/år*]

Følgende krav til informasjonssikkerhet er avtalt i tillegg til bestemmelsene i Avtalen:

Nr.	Tema	Krav

VEDLEGG 3 ADMINISTRATIVE BESTEMMELSER

[Versjon nr. XX, *dato/måned/år*]

Kontaktopplysninger

Meddelelser, underretting, varsel eller annen kommunikasjon mellom Dataansvarlig og Databehandler skal gis skriftlig, eller bekreftes skriftlig til:

Dataansvarlig	Databehandler
[Virksomhetens navn] [Adresse]	**[Virksomhetens navn]** [Adresse]
Navn: Rolle: E-post: Telefonnummer:	Navn: Rolle: E-post: Telefonnummer:

Øvrige administrative bestemmelser

Partene har avtalt at:

Administrative bestemmelser

VEDLEGG 4 – UNDERLEVERANDØRER

[Versjon nr. XX, *dato/måned/år*]

Tabellen oppdateres ved endringer. Alle endringer skal føres opp i endringskatalogen i **Vedlegg 6.**

Databehandler benytter følgende underleverandører:

Navn	Org.nr	Adresse	Leveransetype (behandling)	Behandlingssted

VEDLEGG 5: ENDRINGER I DEN GENERELLE AVTALETEKSTEN VED AVTALEINNGÅELSEN

Partene har avtalt følgende endringer i den generelle avtaleteksten:

Endringstabell:

Punkt i avtalen	Erstattes med

VEDLEGG 6: ENDRINGER ETTER AVTALEINNGÅELSEN

[Versjon nr. XX, *dato/måned/år*]

Katalog over endringer:

Nr.	Dato	Endring	Ev. vedlegg	Gjelder fra

Direktoratet for e-helse

Standard Data Processing Agreement - subcontractor of Helse Vest IKT AS

for processing personal health data

Pursuant to the Norwegian Personal Data Act and

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

between

Helse Vest IKT AS

Organisation no.: 987 601 787

(the data processor)

and

[Name of organisation]

Organisation no.: 000 000 000

subcontractor

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

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

Place and date:

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

For the Processor	**For the Subcontractor**
Name: Insert	Name: Insert
Signature: _____	Signature: _____

Background and further information about the parties

Background

This agreement (the Standard Data Processor Agreement – subcontractor of Helse Vest IKT AS) governs Helse Vest IKT AS' use of subcontractors when processing medical and personal data on behalf of the Data Controller, cf. Article 28 paragraph 2 of the GDPR.

The Data Controller has signed an agreement with the Data Processor/Helse Vest IKT AS which allows the Data Processor/Helse Vest IKT AS to enter into agreements with subcontractors in conjunction with developing and operating IT as a service for the Data Controller. The agreement entitles the Data Controller to request that the Data Processor present the agreement entered into between Helse Vest IKT AS and the Subcontractor before it is signed.

Parties

Data Controller: The enterprise/health trust that has entered into a data processor agreement with Helse Vest IKT AS. (Details of the Data Controllers who use the system covered by this agreement can be found in the configuration database/system list maintained by the Data Processor).

Data Processor: Helse Vest IKT AS.

Subcontractor: [Company]

If the Subcontractor uses other subcontractors, this is covered by Clause 9 and by Annex 4.

The purpose of the system/solution

The purpose of the system/solution is: [Enter a general description of what the system is and does and of what the agreement covers. You can often find this in the system description in Assyst.)]

NB!
Text in square brackets highlighted in yellow must be replaced by the relevant information for the specific agreement. Remove text highlighted in blue.

Contents

1. About the agreement

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

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

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

Appendices to the agreement:

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

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

2. Definitions

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

3. Purpose of the Agreement

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

4. Scope

This Agreement shall apply to all processing of personal health data which the Subcontractor carries out according to the Data Processor`s instructions on behalf of the Controller and in accordance with the Service/assignment agreement.

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

5. Purpose of the processing, data and processing activities

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

6. Framework for the processing of personal health data

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

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

7. The Controller's obligations

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

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

8. The Subcontractor's obligations

8.1. General

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

8.1.1 The Subcontractor shall not:

g. process personal health data for any purposes or to any greater extent or in any other manner than as specified in this Agreement, the Service/assignment agreement and any subsequent written agreements between the parties;

h. process personal health data over and above that which is necessary in order to fulfil the Subcontractor's obligations in accordance with the agreements applicable at any one time;

i. disclose, hand over, transfer or obtain personal health data in any form to or from a third party at the Subcontractor's own initiative, unless there is a statutory obligation or prior agreement with the Controller or with the written consent of the Controller;

8.1.2 The Subcontractor shall:

s. maintain ongoing control over all categories of processing activities that are carried out on behalf of the Controller, cf. Article 30 (2) of the General Data Protection Regulation, 2, cf. also **Appendix 1**;

t. grant the Controller access to personal health data which are processed by the Subcontractor on behalf of the Controller;

u. take all reasonable measures to assist the Controller with ensuring that the personal health data are accurate and updated at all times;

v. establish routines to erase data in accordance with instructions and guidelines stipulated by the Controller;

w. ensure that all persons who are granted access to personal data processed on behalf of the Controller are familiar with this Agreement and applicable agreements between the parties, and are subject to the provisions of these agreements;

x. provide the Controller with the necessary assistance to enable the Controller to fulfil its obligations with respect to the data subjects, including responding to requests from the data subjects that will exercise their rights as set out in Chapter III of the General Data Protection Regulation;

y. notify the Controller without undue delay if the Subcontractor believes that any instructions are in breach of the General Data Protection Regulation or other provisions concerning the protection of personal data;

z. assist the Controller in ensuring compliance with the obligations of Articles 35-36 of the General Data Protection Regulation, which concern the assessment of data protection consequences and advance discussions with the Norwegian Data Protection Authority.

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

8.2. Technical, organisational and security measures

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

At a minimum, the Subcontractor shall:

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

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

cc. have routines for internal control;

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

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

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

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

hh. document any breach, including the factual circumstances linked to the breach, its impact and any remedial measures that have been implemented;

ii. notify the Controller without undue delay in the event of the unauthorised disclosure of personal data;

jj. register all authorised and unauthorised access to data. All look-ups that are performed shall be registered so that they can be traced to the individual user concerned (i.e. an employee of the Subcontractor, a subcontractor or the Controller). The logs shall be retained until there is no longer considered to be any use for them or as stipulated by the Agreement or Service/assignment agreement;

kk. assist the Controller with ensuring fulfilment of the obligations in Articles 32-34 of the General Data Protection Regulation, including but not limited to:
- security of processing;
- notification of a personal data breach to the supervisory authority;
- communication of a personal data breach to the data subject;

ll. notify the Controller of circumstances related to the Subcontractor's obligations under the Service/assignment agreement that entail or may be deemed to entail a weakness in information security;

mm. obtain written approval from the Controller prior to the implementation of any change in the data processing by the Subcontractor which is or could be of negative importance for information security when processing data in accordance with this Agreement.

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

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

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

9. Use of subcontractors

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

The Subcontractor shall:

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

p. maintain an updated list of the identity and location of subcontractors specified in Appendix 4 and where they process personal data. The updated list shall be available to the Controller;

q. conduct a risk assessment concerning the use of subcontractors and the significance for the service before entering into an agreement with subcontractors and, at the request of the Controller, share the assessment with the Controller;

r. at the request of the Controller, present a copy of the agreement(s) that has/have been entered into with the subcontractors (with the exception of commercial conditions). Such agreements must be established before the subcontractors commence the processing of personal health data;

s. notify the Controller of any plans to use other subcontractors or substitute subcontractors. The Controller must be given sufficient advance notice of such substitutions in order to give the Controller an opportunity to object to the change. In the event of the substitution of a subcontractor, Appendix 4 must be updated and sent to the Controller before a new subcontractor commences its work. The amendment must also be entered in Appendix 6;

t. ensure that the Controller and the supervisory authority have the same access and audit rights concerning the processing of personal data with respect to a subcontractor as the Controller has with respect to the Subcontractor under Clause 12 of the Agreement;

u. in the event of the termination of the Agreement, ensure that subcontractors fulfil their obligation to return, erase or destroy in an appropriate manner all personal health data and any and all copies and back-up copies of the data as stipulated in Clause 13 of the Agreement.

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

10. Transfer of personal data to other countries

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

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

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

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

11. Obligations of secrecy

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

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

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

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

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

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

12. Audits

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

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

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

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

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

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

13. Duration and termination

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

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

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

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

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

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

14. Amendments to the Agreement

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

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

15. Governing Law, disputes and venue

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

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

[day/month/year] *Insert today`s date.*

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

C. Purpose and duration of the processing

NB! Remove this text box, which is only for your information.

Why does the subcontractor process the data? Why do we need external assistance with our operations?

If the purpose is not clear from the service agreement, it should be clear to the customer(s)/data Controller, so consider asking them.

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

Remember that <u>each</u> processing activity must be linked to a specific and explicitly stated purpose – see the example below. Complete/delete as appropriate.

Date (from/to)	Name of service	Purpose of the processing	Duration of the processing
[day/month/year-]	[Support with error correction]	[Provide support with error correction – to restore and stabilise service]	[Until the purpose has been achieved]
[day/month/year-]	[System maintenance]	[Operation and management]	[For the duration of the agreement]
[day/month/year-]	[File transfer]	[Transferring large quantities of data to…]	[For the duration of the agreement]
[day/month/year-]	[File storage]	[Storage of files and databases to …]	[For the duration of the agreement]
[day/month/year-]	[Complete]	[Complete]	[Complete]

B. Processing of personal health data

Article 4 (2) of the General Data Protection Regulation states that processing means: "any operation or set of operations which is performed on personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction"

NB! Remove this text box, which is only for your information.

How does the subcontractor process the data? Which specific tasks and actions does this subcontractor perform in relation to stored personal data?

This may be set out in the agreement with the subcontractor, and it should be known to the public administration and most likely the customers/Data Controllers for the solution.

The following processing is covered by the Agreement:

See examples below.

Processing	Processing activities	System location and place where

		processing takes place
[Access to stored personal data for rectification]	[Highly relevant – suggested text: The Supplier needs access to stored personal data to detect and rectify errors.]	[Suggested text: The database is stored on Helse Vest IKT's servers. To allow it to carry out its processing activities, the Supplier will be given access to the database via VPN (Bomgar remote access), which it can order from Helse Vest IKT]
[Access to stored personal data for support updates]	[Highly relevant – suggested text: The Supplier needs access to stored personal data for updates]	[Complete]
[Access to stored personal data for configuration]	[Highly relevant – suggested text: The Supplier needs access to stored personal data for configuration purposes. TheSupplier may carry out changes to the configuration at the request of the Data Processor or the Data Controller.]	[Complete]
[Innsamling]	[Complete if relevant]	[Complete]
[Collection]	[Complete if relevant]	[Complete]
[Recording]	[Complete if relevant]	[Complete]
[Organisation]	[Complete if relevant]	[Complete]
[Structuring]	[Complete if relevant]	[Complete]
[Storage]	[Complete if relevant]	[Complete]
[Adaptation or alteration]	[Complete if relevant]	[Complete]
[Retrieval]	[Complete if relevant]	[Complete]
[Alignment]	[Complete if relevant]	[Complete]
[Erasure or destruction]	[Complete if relevant]	[Complete]
[Disclosure/Transfer]	[Complete if relevant]	[Complete]
[Otherwise making available]	[Complete]	[Complete]

[Other relevant processing activities]	[Complete]	[Complete]

C. Types of data

NB! Remove this text box, which is only for your information.

The key here is "what information is stored about the data subjects?". Which information is stored in the system that the subcontractor may have access to/be able to modify?

The following personal health data are processed:

List the medical and personal data covered – see examples below. Enter what is relevant.

Personal data
[Name]
[Surname]
[National identity number]
[Address]
[Mobil or telephone number]
[E-mail]
[Next of kin]
[Position held]
[Salary details]
[Details of leave taken]
[Details of inclusive working life and HR]
[Expertise (education, courses, work experience, certificates/authorisations, etc.)]
[Other information – provide details]

Medical information
[Use of medication]
[Diagnostic information]
[Data from health care databases]
[Treatment location]
[GP]
[Other information – provide details]

D. Categories of data subjects

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

List the categories of data subjects that are covered – see examples below. The key here is "about whom?". Whose personal data is stored in the system? Complete/delete as appropriate.

Categories of data subjects		
Patients	[Employees of Helse Vest IKT]	[Employees of the Supplier]
Children	[Former employees of Helse Vest IKT]	[Employees at partner firms]
Parents	[Employees of health trusts]	[Complete]
[Next of kin]	[Former employees of health trusts]	
Public officials		

APPENDIX 2 – DETAILED REQUIREMENTS CONCERNING INFORMATION SECURITY

[day/month/year] Insert today`s date

No.	Topic	Requirement
1	Code of Conduct for information security in the health and care services sector	The Subcontractor shall comply with the relevant provisions of the Code of Conduct on information security, including the Appendix "Overall summary of the requirements of the Code".
2	Data security	The Subcontractor shall have mechanisms in place to ensure the integrity and confidentiality of data during transport, processing and storage. The mechanisms are specified below in sections 4, 5 and 6. *[Mechanisms = measures such as encryption, logging. The service agreement shall describe the measures taken. If not mentioned in the service agreement, they must be included in the data processor agreement.]*
3	Authentication	Personal user names and passwords shall be used to access data when needed for work purposes. The Data Subcontractor shall have established a password policy.
4	Logging and tracing	If the database is stored on Helse Vest IKT's servers, all access must be via VPN (Bomgar remote access). All processing activity is logged and is traceable. *[You can find more information about Bomgar remote access here: https://helse-vest-ikt.no/brukarstotte/for-leverandorar#fjernaksess]* If the database is stored by/transferred to the Subcontractor, the Subcontractor shall ensure that all access and attempted access to the data can be documented. Logs shall be secured against modification, and shall be available on request.
5	Availability, redundancy and scalability	The Subcontractor shall ensure that the availability of the service meets the requirements of the contract/SLA, which includes protecting against denial-of-service attacks, software, network and hardware errors, and other events that might reduce availability.
6	Test data	All testing shall be agreed with Helse Vest IKT. When using personal data for testing, this shall always be done in accordance with the basic data minimisation principles set out in Clause 1.(c) of Article 5 of the General

		Data Protection Regulation. Only adequate and relevant personal data shall be used, and only to the extent necessary for the purposes for which they are being processed/the test.
7	Erasure and return	Subcontractors shall have procedures in place that they can provide if requested by the Data Processor on behalf of the Data Controller.
8	Storage time	Subcontractors shall ensure that data are erased in accordance with the agreement's stipulations on storage time, and that data are available until the agreed deletion time.
9	[Backup and restore]	[Complete if relevant]
10	[Storage encryption]	[Complete if relevant]
11	[Encryption for communication]	[Complete if relevant] *E.g. https with (transport layer security) TLS version.*
12	[Other]	[Complete]

APPENDIX 3 ADMINISTRATIVE PROVISIONS

[day/month/year] Insert today`s date

Contact details [Can be removed if handled elsewhere]

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

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

Other administrative provisions

The parties have agreed that:

Administrative provisions

APPENDIX 4 – SUBCONTRACTORS

[day/month/year] Insert today`s date

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

Here you should list which subcontractors are used by the Subcontractor – see examples below – only complete if the subcontractor uses other subcontractors.

The Subcontractor uses the following subcontractors:

See examples below.

Name	Organisation no.	Address	Service type (processing)	Place of processing
ABC			Data centre, hosting	Stockholm, Sweden
DEF			IT support service	Oslo, Norway
XYZ			Backup	Paris, France

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

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

Change table:

Clause in the agreement	Replaced with

APPENDIX 6: AMENDMENTS AFTER THE AGREEMENT HAS BEEN ENTERED INTO

[day/month/year] Insert today`s date

Catalogue of changes:

No.	Date	Change	Any appendices	Applies from

Standard «underdatabehandleravtale»

for behandling av helse- og personopplysninger

i henhold til personopplysningsloven og

EUs Personvernforordning (EU) 2016/679

mellom

Helse Vest IKT AS

Org.nr.: 987 601 787

(databehandler)

og

[Virksomhetens navn]

Org.nr.: 000 000 000

Underleverandør

Denne underdatabehandleravtalen er knyttet til følgende tjeneste/oppdragsavtale mellom partene: […….].

Underdatabehandleravtalen undertegnes i to eksemplarer, ett til hver part.

Sted og dato:

[*sted*], xx.xx.20xx

For Databehandler	**For Underleverandør**
Navn: Fyll ut	Navn: Fyll ut
Underskrift: _____	Underskrift: _____

Nærmere om bakgrunn og partene

Bakgrunn

Denne avtalen regulerer Helse Vest IKT AS bruk av underleverandører ved behandling av helse – og personopplysninger som skjer på vegne av Dataansvarlig virksomhet, jf. personvernforordningen art 28 nr. 2.

Dataansvarlig har inngått avtale med Databehandler/Helse Vest IKT AS som innebærer at Helse Vest IKT AS kan inngå avtaler med underleverandører i forbindelse med utvikling og drift av IT som en tjeneste til Dataansvarlig. Av den avtalen fremkommer det at Dataansvarlig på forespørsel skal kunne be Databehandler om å få seg forelagt avtalen som inngås mellom Helse Vest IKT AS og underleverandøren før signering.

Parter

Dataansvarlig: Virksomheter/helseforetak som har inngått Underleverandøravtale med Helse Vest IKT AS. (Hvilke dataansvarlige virksomheter som bruker løsningen som omfattes av denne avtalen fremkommer av Systemlisten som vedlikeholdes av Helse Vest IKT AS).

Databehandler: Helse Vest IKT AS.

Underleverandør): [Selskap]

Dersom Underleverandøren benytter andre underleverandører, er dette omtalt i punkt 9 og Vedlegg 4.

Kort beskrivelse av formålet med systemet/løsningen:

Formålet med systemet/løsningen er: [**Sett inn en generell beskrivelse av hva systemet er og gjør og hva avtalen omfatter**: Dette finnes gjerne i systembeskrivelsesattributten i Assyst.]

NB!

Tekst i klammeparentes markert med gul mark-up må fjernes og erstattes med det som gjelder for den aktuelle avtalen. Hjelpetekst markert med blå mark-up fjernes.

Innhold

1. Om avtalen

Denne databehandleravtalen med vedlegg (heretter omtalt som "Avtalen") regulerer rettigheter og plikter mellom Databehandler og Underleverandør (heretter omtalt som "partene") etter:

- Lov om behandling av personopplysninger av 15.juni 2018 nr. 38 (personopplysningsloven);
- Europaparlaments- og rådsforordning (EU) 2016/679 av 27.april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger (General Data Protection Regulation) (heretter omtalt som "personvernforordningen");
- Lov om helseregistre og behandling av helseregistre av 20.juni 2014 nr. 43 (helseregisterloven);
- Lov om behandling av helseopplysninger ved ytelse av helsehjelp av 20.juni 2014 nr. 42 (pasientjournalloven); og
- Enhver lov, forskrift eller annet regelverk som endrer eller erstatter ovennevnte regler.

Ved motstrid mellom Avtalens regulering og de rammer som følger av personvernregelverket eller relevant helselovgining, viker Avtalens regulering. I tilfelle konflikt mellom denne Avtalen og Tjeneste/oppdragsavtalen, skal denne Avtalen gjelde.

Vedlegg til avtalen:

- Vedlegg 1: Behandlingens formål, opplysninger og behandlinger
- Vedlegg 2: Detaljerte krav til informasjonssikkerhet
- Vedlegg 3: Administrative bestemmelser
- Vedlegg 4: Underleverandører
- Vedlegg 5: Endringer i den generelle avtaleteksten ved avtaleinngåelsen
- Vedlegg 6: Endringer etter avtaleinngåelsen

Endringer til den generelle avtaleteksten skal samles i vedlegg 5. Slike endringer erstatter den opprinnelige avtaleteksten.

2. Definisjoner

Begrepene "personopplysninger", "helseopplysninger", "behandling", "dataansvarlig", "databehandler", "brudd på personopplysningssikkerheten" og "helseopplysninger" skal forstås slik de er definert i personvernforordningen artikkel 4, helseregisterloven § 2 og pasientjournalloven § 2.

3. Avtalens formål

Formålet med Avtalen er å sikre de registrertes rettigheter og partenes etterlevelse av artikkel 28 nummer 3 i personvernforordningen.

4. Omfang

Denne Avtalen kommer til anvendelse på all behandling av helse- og personopplysninger som Underleverandør utfører på grunnlag av Tjeneste- /oppdragsavtalen og etter Databehandlers instrukser på vegne av Dataansvarlig.

Denne Avtalen vil i tillegg gjelde for ytterligere behandling av helse- og personopplysninger basert på eventuelle skriftlige avtaler mellom partene som inngås i løpet av denne Avtalens varighet og som innebærer at Underleverandør behandler helse- og personopplysninger etter Databehandlers instrukser som skjer på vegne av Dataansvarlig (heretter omtalt som "senere skriftlige avtaler mellom partene"). Slike tillegg skal fremgå av **Vedlegg 6**. Avtalens øvrige vedlegg skal oppdateres i samsvar med endringen.

5. Behandlingens formål, opplysninger og behandlinger

Formålet med og varigheten av behandling av helse- og personopplysninger, hvilke helse- og personopplysninger som behandles, kategorier av de registrerte og behandlingsaktiviteter er angitt i **Vedlegg 1.**

6. Rammene for behandling av helse- og personopplysninger

Dataansvarlig har til enhver tid full rådighet over de helse- og personopplysningene som Underleverandør behandler etter denne Avtalen. Underleverandør har ikke selvstendig råderett over helse- og personopplysningene, og kan ikke behandle disse til egne formål.

Dataansvarlig har, med mindre annet er avtalt eller følger av lov, rett til tilgang til og innsyn i helse- og personopplysningene som behandles hos Underleverandøren.

7. Dataansvarliges plikter

Dataansvarlig skal etterleve de forpliktelser som følger av personvernregelverket, jf. personvernforordningen artikkel 24, relevant helselovgivning og annen særlovgivning, samt denne Avtalen.

Dataansvarlig er ansvarlig for at personvernprinsippene overholdes, jf. personvernforordningen artikkel 5, og skal blant annet sørge for at behandlingen av opplysninger er formålsbestemt og basert på et gyldig rettsgrunnlag.

8. Underleverandørs plikter

8.1. Generelt

Underleverandør forplikter seg til å behandle helse- og personopplysninger kun i samsvar med gjeldende regelverk, denne Avtalen, Tjeneste/oppdragsavtalen, Dataansvarliges dokumenterte instrukser og andre gjeldende avtaler mellom partene, samt "Norm for informasjonssikkerhet i helse- og omsorgssektoren".

Underleverandør skal ikke ved noen handling eller unnlatelse, sette Dataansvarlig i en slik situasjon at Dataansvarlig bryter gjeldende regelverk som angitt i Avtalen punkt 1.

8.1.1 Underleverandør skal ikke:

j. behandle helse- og personopplysninger for andre formål eller i større grad eller på annen måte enn det som følger av denne Avtalen, Tjeneste/oppdragsavtale og eventuelle senere skriftlige avtaler mellom partene;

k. behandle helse- og personopplysninger utover det som er nødvendig for å oppfylle Underleverandørs forpliktelser i henhold til de til enhver tid gjeldende avtaler;

l. utlevere, overlate, overføre eller innhente helse- og personopplysninger i noen form til eller fra tredjepart på eget initiativ, med mindre det er lovpålagt eller det på forhånd er avtalt med Dataansvarlig eller Dataansvarlig har godkjent dette skriftlig;

8.1.2 Underleverandør skal:

ø. ha løpende kontroll på alle kategorier av behandlingsaktiviteter utført på vegne av Dataansvarlig, jf. personvernforordningen artikkel 30 nr. 2, jf. også **Vedlegg 1**;

å. gi Dataansvarlig tilgang til og innsyn i helse- og personopplysninger som behandles hos Underleverandøren på vegne av Dataansvarlig;

aa. treffe alle rimelige tiltak for å bistå Dataansvarlig med å sikre at helse- og personopplysningene til enhver tid er korrekte og oppdaterte;

bb. etablere rutiner for å slette opplysninger i henhold til instruks eller retningslinjer fastsatt av Dataansvarlig;

cc. påse at samtlige personer som gis tilgang til personopplysninger som behandles på vegne av Dataansvarlig er kjent med denne Avtalen og gjeldende avtaler mellom partene, og er underlagt disse avtalenes bestemmelser;

dd. gi Dataansvarlig nødvendig bistand slik at Dataansvarlig skal kunne oppfylle sine forpliktelser overfor de registrerte, herunder å svare på anmodninger fra den registrerte som vil utøve sine rettigheter fastsatt i personvernforordningen kapittel III;

ee. uten ugrunnet opphold varsle den Dataansvarlige dersom Underleverandør mener at en instruks er i strid med personvernforordningen eller andre bestemmelser om vern av personopplysninger;

ff. bistå Dataansvarlig for å sikre overholdelse av forpliktelsene i personvernforordningen artiklene 35-36 som omhandler vurdering av personvernkonsekvenser og forhåndsdrøftinger med Datatilsynet;

gg. Underleverandør skal umiddelbart varsle Dataansvarlig hvis den mottar forespørsel fra en myndighet om å utlevere personopplysninger som er behandlet under Databehandleravtalen. Med mindre utleveringen er lovpålagt, skal Underleverandør ikke etterkomme en slik forespørsel uten skriftlig forhåndsgodkjenning fra Dataansvarlig.

8.2. Tekniske, organisatoriske og sikkerhetsmessige tiltak

Underleverandør plikter å treffe og gjennomføre alle tekniske, organisatoriske og sikkerhetsmessige tiltak slik at det til enhver tid er et sikkerhetsnivå som er egnet med hensyn til risikoen ved behandling av helse og personopplysninger.

Underleverandøren skal, som minimum:

kk. etablere og etterkomme nødvendige tekniske og organisatoriske tiltak med hensyn til vedvarende konfidensialitet, integritet, tilgjengelighet og robusthet ved behandling av helse- og personopplysninger for å sikre tilfredsstillende informasjonssikkerhet i henhold til personvernregelverket, herunder kravene etter personvernforordningen artikkel 32, og gjeldende helselovgivning.

ll. sikre at krav til innebygd personvern og personvern som standardinnstilling innfris i Underleverandørs løsninger. Dette inkluderer å bygge inn funksjonalitet for å oppfylle personvernprinsipper samt funksjonalitet for å sikre den registrertes rettigheter, herunder retten til begrenset behandling;

mm. ha rutiner for internkontroll;

nn. ha rutiner for autorisasjon og styring som sikrer at bare de av Underleverandørs medarbeidere som har tjenstlig behov for tilgang til systemer og opplysningene for å ivareta nødvendige oppgaver for gjennomføring av Tjeneste/oppdragsavtalen får slik tilgang. Tilgangsnivået skal være i henhold til tjenstlig behov knyttet til å gjennomføre oppdraget. Det skal etableres sterk autentisering for tilgang til helseopplysninger;

oo. etablere nødvendige systemer og rutiner for å ivareta informasjonssikkerheten og følge opp avvik, som skal omfatte blant annet rutiner for avviksmelding, rutiner for backup, gjenoppretting av normalsituasjonen, fjerne årsaken til avviket og hindre gjentakelse. På forespørsel, skal Underleverandør gi Dataansvarlig tilgang til relevant sikkerhetsdokumentasjon for behandling av helse- og personopplysninger;

pp. avdekke, registrere, rapportere og lukke avvik knyttet til informasjonssikkerhet, herunder loggføre og dokumentere ethvert forsøk på ikke-autorisert tilgang og andre brudd på personopplysningssikkerheten i datasystemene. Slik dokumentasjon skal oppbevares hos Underleverandør;

qq. ved mistanke om eller konstatering av brudd på personopplysningssikkerheten, uten ugrunnet opphold varsle Dataansvarlig. I varselet opplyses avviket med forklaring om årsak, tidsrom og tidspunktet avviket ble oppdaget, kategoriene av og omtrentlig antall registrerte som er berørt, kategoriene av og omtrentlig antall registreringer av personopplysninger som er berørt, navnet på og kontaktopplysningene til personvernombudet eller et annet kontaktpunkt der mer informasjon kan innhentes, antatte konsekvenser av avviket og hvilke umiddelbare tiltak som er igangsatt eller vurderes igangsatt for å håndtere avviket. Dersom og i den grad det ikke er mulig å gi all informasjon samtidig, kan den gis trinnvis uten ytterligere ugrunnet opphold;

rr. dokumentere ethvert avvik, herunder de faktiske forhold knyttet til avviket, dets virkninger og eventuelle iverksatte utbedringstiltak;

ss. uten ugrunnet opphold varsle Dataansvarlig ved uautorisert utlevering av personopplysninger;

tt. registrere all autorisert og uautorisert tilgang til opplysninger. Alle oppslag som gjøres skal registreres slik at de kan spores til den enkelte bruker (dvs. ansatte hos Underleverandør, andre underleverandører og Dataansvarlig). Loggene skal oppbevares til det ikke lenger antas å være bruk for dem eller i henhold til det Avtalen eller Tjeneste/oppdragsavtalen spesifiserer;

uu. bistå Dataansvarlig med å sikre overholdelse av forpliktelsene i personvernforordningen artiklene 32–34, herunder, men ikke begrenset til:
- sikkerhet ved behandlingen;
- melding til tilsynsmyndigheten om brudd på personopplysningssikkerheten;
- underretning av den registrerte om brudd på personopplysningssikkerheten;

vv. varsle Dataansvarlig om forhold relatert til Underleverandørs forpliktelser under Tjeneste/oppdragsavtalen som medfører eller kan anses å medføre svekkelse av informasjonssikkerheten;

ww. innhente skriftlig godkjenning av Dataansvarlig før gjennomføring av enhver endring av databehandlingen hos Underleverandør som har eller kan ha negativ betydning for informasjonssikkerheten ved behandlingen etter denne Avtalen.

Nærmere krav til informasjonssikkerhet er angitt i **Vedlegg 2**.

Ved brudd på denne Avtalen eller på bestemmelsene i personvernregelverket, helselovgivningen eller annen relevant lovgivning kan Dataansvarlig kreve endringer i behandlingsmåten eller pålegge Underleverandør å stoppe den videre behandlingen av opplysningene med øyeblikkelig virkning.

Underleverandør skal dokumentere sine rutiner og alle tiltak truffet for å oppfylle kravene angitt ovenfor. Denne dokumentasjonen skal på forespørsel gjøres tilgjengelig for Dataansvarlig.

9. Bruk av underleverandør

Dataansvarlig tillater at Underleverandør benytter underleverandører for oppfyllelse av forpliktelsene under Avtalen. Underleverandør benytter kun de underleverandører som er angitt i **Vedlegg 4** for de der angitte tjenester.

Underleverandør skal:

v. sikre at underleverandøren påtar seg tilsvarende forpliktelser som Underleverandør selv er underlagt etter Avtalen og gjeldende lovgivning;

w. holde en oppdatert liste over identiteten til og stedlig plassering av underleverandører som angitt i Vedlegg 4 og hvor disse behandler personopplysninger. Oppdatert liste skal være tilgjengelig for Dataansvarlig;

x. gjennomføre en risikovurdering av bruk av underleverandør og betydningen for tjenesten før det inngås avtale med underleverandør og på Dataansvarliges forespørsel, dele vurderingen med Dataansvarlig;

y. på Dataansvarliges forespørsel, legge frem kopi av avtalen(e) som er inngått med underleverandørene (med unntak av merkantile betingelser). Slike avtaler skal senest være inngått før underleverandørene starter med behandling av helse- og personopplysninger;

z. underrette Dataansvarlig om eventuelle planer om å benytte andre underleverandører eller skifte ut underleverandører. Slike bytter skal varsles Dataansvarlig i god tid slik at denne gis mulighet til å motsette seg endringen. Ved bytte av underleverandør skal Vedlegg 4 oppdateres og oversendes Dataansvarlig før ny underleverandør starter opp. Endringen føres også opp i Vedlegg 6;

æ. sikre at Dataansvarlig og tilsynsmyndighetene har samme rett til innsyn og kontroll med behandling av personopplysninger hos en underleverandør som Dataansvarlig har overfor Underleverandør etter Avtalens punkt 12;

ø. ved opphør av Avtalen, sikre at underleverandører oppfyller plikten til å tilbakeføre, slette eller forsvarlig destruere alle helse- og personopplysningene og alle eventuelle kopier og sikkerhetskopier av opplysningene, slik som det framgår av Avtalens punkt 13.

Underleverandør er til enhver tid fullt ut ansvarlig overfor Dataansvarlig for alt arbeid som utføres av underleverandører og for underleverandørenes etterlevelse av bestemmelsene i denne Avtalen.

10. Overføring av personopplysninger til utlandet

Partene i denne Avtalen er enige om at ingen av helse- og personopplysningene som behandles under denne Avtalen skal føres ut av Norge, med mindre det er særskilt avtalt mellom partene. I tillegg skal arkivverdige dokumenter med helse- og personopplysninger være plassert på servere i Norge (jf. arkivloven § 9 bokstav b), og eventuelle unntak fra dette skal godkjennes eksplisitt av Dataansvarlig før denne behandlingen starter.

Underleverandør bekrefter at ingen av underleverandørene overfører helse- og personopplysninger som omfattes av denne Avtalen til utlandet, med unntak for slike overføringer som er angitt i **Vedlegg 4.** Dette omfatter også fjerntilgang fra utlandet.

Bruk av underleverandører som overfører helse- og personopplysninger til land utenfor EU/EØS (tredjeland) skal avtales skriftlig med Dataansvarlig på forhånd. Ved overføring av helse- og personopplysninger til land utenfor EU/EØS (tredjeland) skal Underleverandør benytte godkjente EU-overføringsmekanismer.

Ved overføring til utlandet, uavhengig av om det er innenfor EU/EØS eller utenfor EU/EØS (tredjeland), skal Underleverandør gi nødvendig dokumentasjon om sikkerhet, risiko og etterlevelsesnivå knyttet til aktuelle underleverandører slik at Dataansvarlig får nødvendig informasjon for å kunne gjennomføre en særskilt risikovurdering. Dataansvarlig kan nekte samtykke til den aktuelle overføringen basert på spesifikke risikoer som fremkommer av Dataansvarliges egen risikovurdering.

11. Taushetsplikt

Underleverandørs ansatte og andre som opptrer på Underleverandørs vegne i forbindelse med behandling av helse- og personopplysninger i henhold til denne Avtalen, Tjeneste/oppdragsavtale og senere skriftlige avtaler mellom partene, skal underlegges taushetsplikt etter denne Avtalen og gjeldende regelverk. Personer som er autorisert til å behandle helse- og personopplysningene forplikter seg til å behandle opplysningene fortrolig. Det samme gjelder eventuelle underleverandører.

Ansatte og andre som opptrer på Underleverandørs vegne i forbindelse med behandling av helse- og personopplysninger skal ha undertegnet taushetserklæring. Bestemmelsen gjelder tilsvarende for underleverandører.

Underleverandør skal påse at alle som behandler personopplysninger under Avtalen er kjent med taushetsplikten.

Partene har i tillegg taushetsplikt om konfidensiell informasjon knyttet til hverandres virksomhet, som er formidlet i forbindelse med oppdraget.

Partene plikter å ta de forholdsregler som er nødvendige for å sikre at materiale eller opplysninger ikke blir gjort kjent for andre i strid med dette punktet.

Taushetsplikten gjelder også etter Avtalens opphør.

12. Revisjon

Underleverandør skal på forespørsel gjøre tilgjengelig for den Dataansvarlige, all informasjon som er nødvendig for å påvise at Underleverandørs forpliktelser fastsatt i personvernforordningen artikkel 28 og denne Avtalen er oppfylt.

Underleverandør skal muliggjøre og bidra ved inspeksjoner og revisjoner som gjennomføres av eller på oppdrag fra Dataansvarlig. Underleverandør skal framlegge interne revisjonsrapporter, interne prosedyrer, rutiner, sikkerhetsarkitektur, risiko og sårbarhetsanalyser med tiltak og andre dokumenter av betydning for revisjonen;

Underleverandør skal også muliggjøre og bidra ved inspeksjoner fra aktuelle tilsynsmyndigheter. Den Dataansvarliges tilsyn med eventuelle underleverandører skal skje gjennom Underleverandøren med mindre annet er særskilt avtalt.

Nærmere rutiner for gjennomføring av revisjoner kan avtales i **Vedlegg 3**.

Dersom en revisjon avdekker avvik fra forpliktelsene i gjeldende personvernregler eller Avtalen, skal Underleverandør uten ugrunnet opphold utbedre avviket. Dataansvarlig kan kreve at Underleverandøren midlertidig stopper hele eller deler av behandlingsaktivitetene frem til utbedringen er godkjent av Dataansvarlig.

Hver av Partene dekker sine egne kostnader forbundet med inspeksjoner fra aktuelle tilsynsmyndigheter og inntil én årlig revisjon initiert av Dataansvarlig. Hvis en revisjon avdekker vesentlige brudd på forpliktelsene etter gjeldende personvernregler eller Avtalen, skal Underleverandøren likevel dekke Dataansvarliges rimelige kostnader forbundet med revisjonen.

13. Varighet og opphør

Underleverandøravtalen gjelder fra den er signert av begge Parter og gjelder så lenge Underleverandør behandler Personopplysninger på vegne av Dataansvarlig.

I denne perioden gjelder Avtalen med mindre andre bestemmelser som regulerer Underleverandørs behandling av Personopplysninger på vegne av Dataansvarlig avtales mellom Partene.

Ved opphør av Avtalen skal Underleverandør tilrettelegge for og medvirke til tilbakeføring av alle helse- og personopplysninger som Underleverandør har mottatt og behandlet på vegne av Dataansvarlig. Partene avtaler nærmere hvordan overføring konkret skal skje.

Etter at alle opplysningene er overført til Dataansvarlig og bekreftet mottatt av denne, skal Underleverandør irreversibelt slette eller forsvarlig destruere alle opplysningene og alle eventuelle kopier og sikkerhetskopier av opplysningene i sine systemer, med mindre annet regelverk krever at helse- og personopplysningene fortsatt lagres.

Benyttes delt infrastruktur der direkte sletting ikke er teknisk mulig skal Underleverandør sørge for at data gjøres utilgjengelig inntil disse dataene er overskrevet av systemet.

Underleverandør skal gi Dataansvarlig skriftlig bekreftelse på at opplysningene er overført og slettet som angitt over.

14. Endring av avtale

I tilfelle endringer i det rettslige rammeverket eller endringer i tjenester i Tjeneste/oppdragsavtalen som krever endringer av denne Avtalen, skal partene samarbeide for å oppdatere Avtalen tilsvarende.

Endringer etter avtaleinngåelsen listes opp i **Vedlegg 6.** Underleverandør er ansvarlig for at det føres en slik endringskatalog og at denne holdes oppdatert.

15. Lovvalg, tvister og verneting

Avtalen er underlagt norsk rett. Tvister løses i samsvar med Tjeneste/oppdragsavtalens bestemmelser, herunder eventuelle bestemmelser om verneting.

VEDLEGG 1 – BEHANDLINGENS FORMÅL, OPPLYSNINGER OG BEHANDLINGER

[*dato/måned/år*] *Sett inn dagens dato.*

Tabellene oppdateres ved endringer. Alle endringer skal føres opp i endringskatalogen i **Vedlegg 6.**

A. Formålet med og varigheten av behandlingen

OBS! Fjern denne boksen med veiledningstekst.

Hvorfor gjør underleverandøren denne databehandlingen? Hvorfor trenger vi ekstern bistand i driften?

Formålet må komme tydelig frem.

Dersom formålet ikke klart fremkommer av driftsavtalen skal dette være klart for kunden(e)/de dataansvarlige for systemet, så spør gjerne der.

Formålet med og varigheten av behandling av helse- og personopplysninger er:

Husk at hver behandling må være knyttet til spesifikke og uttrykkelig angitt formål – se eksempel nedenfor. Fjern det som ikke er aktuelt.

Dato (fra/til)	Navn på tjeneste	Formålet med behandlingen	Varigheten av behandlingen
[dato/måned/år-]	[Bistand ved feilretting]	[Bistå ved feilretting – for å gjenopprette og stabilisere drift]	[I avtaleperioden]
[dato/måned/år-]	[Vedlikehold av system]	[For å kunne opprettholde drift og forvaltning]	[I avtaleperioden]
[dato/måned/år-]	[Filoverføring]	[Overføre større datamengder for å…]	[Til formålet er oppnådd]
[dato/måned/år-]	[Fillagring]	[Lagring av filer for å…]	[I avtaleperioden]
[dato/måned/år-]	[Fyll ut]	[Fyll ut]	[Fyll ut]

B. Behandling av helse- og personopplysninger

Det følger av personvernforordningen art 4 nr.2 at med «behandling» menes**:** «*enhver operasjon eller rekke av operasjoner som gjøres med personopplysninger, enten automatisert eller ikke, f.eks. innsamling, registrering, organisering, strukturering, lagring, tilpasning eller endring, gjenfinning, konsultering, bruk, utlevering ved overføring, spredning eller alle andre former for tilgjengeliggjøring, sammenstilling eller samkjøring, begrensning, sletting eller tilintetgjøring*»

OBS- Fjern denne boksen med veiledningstekst.

Hvordan gjennomfører underleverandøren denne databehandlingen? Hva er det denne underleverandøren konkret utfører av oppgaver og handlinger knyttet til lagrede personopplysninger?

Dette kan fremkomme av avtalene med underleverandøren, bør være kjent for forvaltningen og gjerne også for kundene/ de dataansvarlige av løsningen.

Følgende behandlinger av personopplysninger omfattes av Avtalen:

Se eksempler nedenfor – stryk det som ikke passer.

Databehandling	Nærmere beskrivelse av databehandlingsaktiviteter	Lokasjon av system og sted for databehandlingsaktivitet
[Tilgang til lagrede personopplysninger for feilretting]	[Særlig relevant – forslag til tekst: Leverandøren har behov for tilgang til lagrede personopplysninger for feilsøking og feilretting]	[Forslag til tekst: Databasen ligger hos Helse Vest IKT. Leverandør gis tilgang via VPN (Bomgar-løsningen), på bestilling fra Helse Vest IKT, for å utføre denne behandlingsaktiviteten]
[Tilgang til lagrede personopplysninger for support oppdatering]	[Særlig relevant – forslag til tekst: Leverandøren har behov for tilgang til lagrede personopplysninger for oppdatering]	[Fyll ut]
[Tilgang til lagrede personopplysninger for konfigurasjon]	[Særlig relevant – forslag til tekst: Leverandøren har behov for tilgang til lagrede personopplysninger for konfigurasjon. Leverandøren kan utføre konfigurasjonsendringer på oppdrag fra databehandler eller dataansvarlig]	[Fyll ut]
[Innsamling]	[Fyll ut hvis relevant]	[Fyll ut]
[Registrering]	[Fyll ut hvis relevant]	[Fyll ut]
[Organisering]	[Fyll ut hvis relevant]	[Fyll ut]
[Strukturering]	[Fyll ut hvis relevant]	[Fyll ut]
Lagring]	[Fyll ut hvis relevant]	[Fyll ut]
[Tilpasning eller endring]	[Fyll ut hvis relevant]	[Fyll ut]
[Gjenfinning]	[Fyll ut hvis relevant]	[Fyll ut]
[Sammenstilling]	[Fyll ut hvis relevant]	[Fyll ut]
[Sletting eller tilintetgjøring]	[Fyll ut hvis relevant]	[Fyll ut]
[Utlevering/Overføring]	[Fyll ut hvis relevant]	[Fyll ut]
[Andre former for tilgjengeliggjøring]	[Fyll ut hvis relevant]	[Fyll ut]
[Andre relevante behandlinger]	[Fyll ut]	[Fyll ut]

C. Typer av opplysninger

OBS- Fjern denne boksen med veiledningstekst.

Stikkordet her er «hva er lagret om de registrerte». Hvilke opplysninger ligger lagret i løsningen som underleverandøren eventuelt kan få tilgang til/komme i inngrep med.

«De registrerte» er Ikke begrenset til kun å gjelde pasienter, men også f.eks. ansatte, konsulenter eller andre personer Helse Vest behandler opplysninger om.

Følgende helse- og personopplysninger behandles:

Her listes opp hvilke helse- og personopplysninger som omfattes – se eksempler nedenfor – fyll ut/stryk det som passer.

Personopplysninger
[Navn]
[Etternavn]
[Fødselsnummer]
[Bosted]
[Mobilnummer/telefonnummer]
[E-post]
[Pårørende]
[Stillingsinformasjon]
[Oversikt over lønn]
[Oversikt over permisjoner]
[Oversikt over IA og -personaloppfølging]
[Kompetanse (utdanning, kurs, arbeidserfaring, sertifikat/autorisasjoner mm)]
[Andre opplysninger – fyll ut]

Helseopplysninger
[Legemiddelbruk]
[Diagnoseopplysninger]
[Opplysninger fra helseregistre]
[Behandlingssted]
[Fastlege]
[Andre opplysninger – fyll ut]

D. Kategorier av registrerte

Følgende kategorier av personer behandles det opplysninger om (registrerte):

Her listes opp hvilke kategorier av registrerte som omfattes – se eksempler nedenfor. Stikkordet her er «om hvem». Hvilke personer ligger det data om i løsningen. Fyll ut/stryk det som ikke passer.

Kategorier av registrerte		
[Pasienter] [Barn] [Foreldre] [Pårørende] [Fullmektiger/verge/formyndige]	[Ansatte i Helse Vest IKT] [Tidligere ansatte i Helse Vest IKT] [Ansatte i helseforetak] [Tidligere ansatte i helseforetak]	[Ansatte hos leverandør] [Ansatte i samarbeidende firma] [Andre opplysninger – fyll ut]

VEDLEGG 2 – DETALJERTE KRAV TIL INFORMASJONSSIKKERHET FOR DATABEHANDLER OG UNDERLEVERANDØRER (ANNEN DATABEHANDLER)

[*dato/måned/år*] *Sett inn dagens dato.*

Nr.	Tema	Krav
1.	Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren	Underleverandør skal følge relevante krav i Norm for informasjonssikkerhet og personvern, inkludert vedlegget «Oversikt over Normens krav».
2.	Sikring av data	Underleverandør skal ha mekanismer for data under transport, prosessering og lagring for å ivareta integritet og konfidensialitet. Mekanismene spesifiseres i pt. 4, 5 og 6 under. *[Mekanismer = tiltak som f.eks. kryptering, logging. Det skal stå beskrevet i driftsavtalen hvilke tiltak som er gjort. Hvis det ikke står i driftsavtalen må det stå i databehandleravtalen.]*
3.	Autentisering	Ved tilgang til data ved tjenstlig behov skal det benyttes personlige brukernavn med passord. Underleverandør skal ha etablert passordpolicy.
4.	Logging og sporbarhet	Dersom løsning ligger hos Helse Vest IKT er kravet at all tilgang skal gå igjennom VPN (Bomgar-løsningen). All behandingsaktivitet blir logget og er sporbar. *[Mer om Bomgar-løsningen finnes her: https://helse-vest-ikt.no/brukarstotte/for-leverandorar#fjernaksess]* Dersom løsning ligger hos/overføres Underleverandør skal Underleverandør skal sikre at all tilgang til og forsøk på tilgang til data kan dokumenteres. Logger skal sikres mot endring, og skal kunne forevises på etterspørsel.
5.	Tilgjengelighet, redundans og skalering	Underleverandør skal sikre at tjenesten er tilgjengelig iht. krav i kontrakt/SLA, inkludert beskyttelse mot tjenestenektangrep, programvare-, nettverks- og maskinvarefeil, og andre hendelser som kan gi redusert tilgjengelighet.

6.	Testdata	All testing skal avtales med Helse Vest IKT. Ved bruk av personopplysninger ved test skal det alltid tas utgangspunkt i bl.a. det grunnleggende personvernprinsippet i personvernforordningen art 5 b) «dataminimering». Det skal kun brukes adekvate og relevante personopplysninger og det skal begrenset til det som er nødvendig for formålet for behandlingen/testen.
7.	Sletting og tilbakelevering	Underleverandør skal ha rutiner som skal kunne vises på forespørsel fra databehandler på vegne av Dataansvarlig.
8.	Lagringstid	Underleverandør skal sørge for at data slettes iht. avtalens krav om lagringstid, og at data er tilgjengelige inntil avtalt tidspunkt for sletting.
9.	[Backup og restore]	[Fyll ut hvis relevant]
10.	[Kryptering ved lagring]	[Fyll ut hvis relevant]
11.	[Kryptering i kommunikasjon]	[Fyll ut hvis relevant] *F.eks https med TLS-versjon (transport layer security)*
12.	[Annet]	[Fyll ut hvis relevant]

VEDLEGG 3 ADMINISTRATIVE BESTEMMELSER

[dato/måned/år] Sett inn dagens dato.

Kontaktopplysninger [Kan fjernes dersom det håndteres andre steder]

Meddelelser, underretting, varsel eller annen kommunikasjon mellom Databehandler og Underleverandør skal gis skriftlig, eller bekreftes skriftlig til:

Databehandler	Underleverandør
[Virksomhetens navn] [Adresse]	**[Virksomhetens navn]** [Adresse]
Navn: Rolle: E-post: Telefonnummer:	Navn: Rolle: E-post: Telefonnummer:

Øvrige administrative bestemmelser

Partene har avtalt at:

Administrative bestemmelser

VEDLEGG 4 – UNDERLEVERANDØRER

[dato/måned/år] Sett inn dagens dato.

Tabellen oppdateres ved endringer. Alle endringer skal føres opp i endringskatalogen i **Vedlegg 6.**

Her listes opp hvilke underleverandører som benyttes av Databehandlers underleverandør – se eksempler nedenfor- fylles kun ut når underleverandøren benytter andre underleverandører.

Se eksempler under:

Databehandler benytter følgende underleverandører:

Navn	Org.nr	Adresse	Leveransetype (behandling)	Behandlingssted
ABC			[Datasenter, hosting]	Stockholm, Sweden
DEF			[IT-supporttjenester]	Oslo, Norway
XYZ			[Backup]	Paris, France

VEDLEGG 5: ENDRINGER I DEN GENERELLE AVTALETEKSTEN VED AVTALEINNGÅELSEN

Partene har avtalt følgende endringer i den generelle avtaleteksten:

Endringstabell:

Punkt i avtalen	Erstattes med

VEDLEGG 6: ENDRINGER ETTER AVTALEINNGÅELSEN

[dato/måned/år] Sett inn dagens dato.

Katalog over endringer:

Nr.	Dato	Endring	Ev. vedlegg	Gjelder fra

M-02-3

Databehandleravtale – databehandler/underleverandør av Helse Vest IKT AS

mellom

Helse Vest IKT AS, org.nr. 987 601 787
(databehandler)

og

[Leverandør] (underleverandør til databehandler), org. nr. [... ... ...]

[System:……]

i henhold til personvernforordningen art 28 nr. 2 og nr.4 vedrørende bruk av databehandlere/underleverandører av Helse Vest IKT AS

NB!

Tekst i klammeparentes markert med gul mark-up må fjernes og erstattes med det som gjelder for den aktuelle avtalen. Hjelpetekst markert med blå mark-up fjernes.

1. Avtalens hensikt og formål

Denne avtalen (databehandleravtalen) regulerer Helse Vest IKT AS bruk av underleverandører ved behandling av helse –og personopplysninger som skjer på vegne av Behandlingsansvarlig, heretter kalt Dataansvarlig, jf. personvernforordningen art 28 nr. 2.

Formålet med denne avtalen er å regulere underleverandørens behandling av personopplysninger på vegne av Dataansvarlig. Videre skal den regulere partenes rettigheter og plikter ved behandling av personopplysninger, jf. personvernforordningen art 28 nr.3.

Formålet med systemet/løsningen er: [Sett inn en generell beskrivelse av hva systemet er og gjør og hva avtalen omfatter. Dette finnes gjerne i systembeskrivelsesattributten i Assyst.]

Databehandleravtalen skal sikre at personopplysninger, som definert i gjeldende personvernregelverk ikke brukes urettmessig og at konfidensialitet, integritet, tilgjengelighet og robusthet ivaretas. Avtalen skal videre sikre at partene ivaretar vern av den registrertes rettigheter i henhold til personvernregelverket.

Underleverandøren skal oppfylle de plikter som fremgår av denne databehandleravtalen samt å følge de instrukser Databehandler gir på vegne av Dataansvarlig.

2. Bakgrunn og nærmere om partene

Dataansvarlig har inngått avtale med Databehandleren/Helse Vest IKT AS som innebærer at Databehandler/Helse Vest IKT AS kan inngå avtaler med underleverandører i forbindelse med utvikling og drift av IT som en tjeneste til Dataansvarlig.

Av denne avtalen fremkommer det at Dataansvarlig skal på forespørsel kunne be Databehandler om å få seg forelagt avtalen som inngås mellom Helse Vest IKT AS og underleverandøren før signering.

Dataansvarlig: Virksomheter/helseforetak som har inngått databehandleravtale med Helse Vest IKT AS. (Hvilke Dataansvarlige som bruker løsningen som omtales av denne avtalen fremkommer av konfigurasjonsdatabasen/Systemlisten som vedlikeholdes av Databehandler).

Databehandler: Helse Vest IKT AS.

Annen databehandler (Heretter kalt Underleverandør): [Selskap]

Dersom Underleverandøren benytter andre underleverandører er dette omtalt i punkt 8 og Vedlegg 3.

3. Forholdet til andre avtaler

Denne avtalen supplerer andre avtaler som er inngått mellom databehandler og underleverandør.

Når det gjelder informasjonssikkerhet og personvern ved databehandling av person- og helseopplysninger skal bestemmelsene i denne databehandleravtalen ha forrang fremfor bestemmelser i andre avtaler, med mindre alternative bestemmelser gir et sterkere vern av opplysningene enn bestemmelsene her.

4. Beskrivelse av behandling av personopplysninger

Leverandøren utøver service, vedlikehold og/eller drift på følgende informasjonssystem [Sett inn navn på løsning/system]. I forbindelse med oppdraget kan leverandøren kun behandle personopplysninger i henhold til vedlegg 1 til denne avtalen.

I vedlegg 1 er formålet med og varigheten av behandlingen nærmere beskrevet. Videre beskrives selve behandlingen som utføres, hvilke helse- og personopplysninger som skal behandles, kategorier av de registrerte og behandlingens art. Eventuelt senere endringer skal fremgå av vedlegg 1.

5. Omfang for behandling av helse- og personopplysninger

Dataansvarlig har til enhver tid full rådighet over de helse- og personopplysningene som Databehandler og Underleverandør har anledning til å behandle etter denne Avtalen. Databehandler og Underleverandør har ikke selvstendig råderett over helse- og personopplysningene, og kan ikke behandle disse til egne formål.

Dataansvarlig har, med mindre annet er avtalt eller følger av lov, rett til tilgang til og innsyn i helse- og personopplysningene som behandles hos Databehandleren og Underleverandør.

6. Dataansvarliges plikter

Dataansvarlig skal etterleve de forpliktelser som fremkommer av personopplysningsloven, personvernforordningen, relevant helselovgivning og annen særlovgivning, samt denne avtalen.

7. Underleverandørens plikter

7.1. Generelt

Underleverandøren forplikter seg til å behandle helse- og personopplysninger kun i samsvar med all relevant lov og regelverk, denne Avtalen, Tjeneste/oppdragsavtalen, Dataansvarliges dokumenterte instruksjoner og andre gjeldende avtaler mellom partene, samt «Norm for informasjonssikkerhet og personvern i helse og omsorgstjenesten» "Normen". Underleverandør skal ikke ved noen handling eller unnlatelse, sette Dataansvarlig i en slik situasjon at Dataansvarlig bryter noen bestemmelse i gjeldende lov og regelverk.

Underleverandør skal ikke:

a. behandle helse- og personopplysninger for andre formål eller i større grad enn det som følger av denne Avtalen med vedlegg;
b. behandle helse- og personopplysninger utover det som er nødvendig for å oppfylle Dataansvarliges og databehandlers forpliktelser i henhold til de til enhver tid gjeldende avtaler omtalt i punkt 4;
c. utlevere, overlate eller overføre helse- og personopplysninger i noen form på eget initiativ med mindre det er avtalt på forhånd med Dataansvarlig eller Dataansvarlig har godkjent dette skriftlig;
d. samle inn fra eller overføre helse- og personopplysninger til en tredjepart;
e. behandle helse- og personopplysninger de får tilgang eller adgang til gjennom oppdraget fra Dataansvarlig på annen måte enn hva som er angitt i denne Avtalen med vedlegg.
f. gjøre kjent personopplysninger for noen tredjepart hvis dette ikke er godkjent av Dataansvarlig eller loven krever det. Hvis en offentlig myndighet eller tilsynsmyndighet krever tilgang til personopplysninger, skal Underleverandør varsle Dataansvarlig før utleveringen med mindre dette er forbudt ved lov. Underleverandør krever at alt ens personell som er autorisert for å behandle Dataansvarliges personopplysninger, forplikter seg til konfidensialitet og ikke behandler Dataansvarliges personopplysninger for noe annet formål, unntatt på instruksjon fra Databehandler eller dersom gjeldende lov krever det.

Underleverandør skal:

a. ha løpende kontroll på alle kategorier av behandlingsaktiviteter utført på vegne av Dataansvarlig;

b. gi Dataansvarlig tilgang til og innsyn i helse- og personopplysninger som behandles hos Underleverandør;

c. føre og vedlikeholde en oversikt over alle opplysninger og behandlinger eller dersom det er relevant, protokoll over sine egne behandlingsaktiviteter i henhold til personvernforordningen artikkel 30;

d. treffe alle rimelige tiltak for å sikre at helse- og personopplysningene til enhver tid er korrekte og oppdaterte;

e. følge etablerte rutiner for å slette informasjon når den ikke lenger er nødvendig ut fra formålet med behandlingen og slette informasjon i henhold til fastsatte rutiner og retningslinjer fra den Dataansvarlige;

f. ha rutiner for og teknisk mulighet til å begrense behandlingen av den registrertes helse- og personopplysninger dersom den registrerte ønsker det med hjemmel i gjeldende lovgivning;

g. påse at samtlige personer som av underleverandør gis tilgang til personopplysninger som behandles på vegne av Dataansvarlig er kjent med denne Avtalen og gjeldende avtaler mellom partene, og er underlagt disse avtalenes bestemmelser;

h. sikre at krav til innebygd personvern og personvern som standardinnstilling innfris i Underleverandørs løsninger. Dette inkluderer å bygge inn funksjonalitet for å oppfylle personvernprinsipper samt funksjonalitet for å sikre den registrertes rettigheter;

i. gi Dataansvarlig nødvendig bistand slik at Dataansvarlig skal kunne oppfylle sine forpliktelser overfor de registrerte;

j. samarbeide med og bistå Dataansvarlig ved oppfyllelse av de registrertes rettigheter knyttet til tilgang til opplysninger, herunder å svare på anmodninger fra den registrerte med henblikk på å utøve sine rettigheter fastsatt i personvernforordningen kapittel III;

k. omgående underrette den Dataansvarlige dersom Underleverandør mener at en instruks er i strid med personvernforordningen eller andre bestemmelser om vern av personopplysninger;

l. bistå Dataansvarlig for å sikre overholdelse av forpliktelsene i personvernforordningen artiklene 35-36 som omhandler vurdering av personvernkonsekvenser og forhåndsdrøftinger med Datatilsynet.

7.2 Tekniske, organisatoriske og sikkerhetsmessige tiltak

Underleverandøren plikter å treffe og gjennomføre alle nødvendige og adekvate planlagte og systematiske tekniske, organisatoriske og sikkerhetsmessige tiltak slik at det til enhver tid er tilfredsstillende informasjonssikkerhet ved behandling av helse- og personopplysninger.

Underleverandøren skal:

a. etablere og etterkomme nødvendige tekniske og organisatoriske tiltak med hensyn til vedvarende konfidensialitet, integritet, tilgjengelighet og robusthet ved behandling av helse- og personopplysninger for å sikre tilfredsstillende informasjonssikkerhet i henhold til personopplysningslovgivningens bestemmelser, herunder kravene etter personvernforordningen artikkel 32, og gjeldende helselovgivning. Dette omfatter blant annet, alt etter hva som er relevant, nødvendige tiltak for å forhindre tilfeldig eller ulovlig ødeleggelse eller tap av data, ikke-autorisert tilgang til eller spredning av data så vel som enhver annen bruk av helse- og personopplysninger som ikke er i overensstemmelse med denne Avtalen, og tiltak for å gjenopprette tilgjengelighet og tilgang til opplysningene ved hendelser;

b. ha gode og hensiktsmessige internkontrollrutiner;

c. ha rutiner for autorisasjon og styring som sikrer at bare de av Underleverandørs medarbeidere som har reelt behov for tilgang til systemer og opplysningene for å ivareta nødvendige oppgaver for gjennomføring av Tjeneste/oppdragsavtalen får slik tilgang. Tilgangsnivået skal være i henhold til reelt behov knyttet til å gjennomføre oppdraget;

d. etablere nødvendige systemer og rutiner for å ivareta informasjonssikkerheten og følge opp avvik, som skal omfatte blant annet rutiner for avviksmelding, gjenoppretting av normalsituasjonen, fjerne årsaken til avviket og hindre gjentakelse. På forespørsel, skal Underleverandør gi Databehandler og Dataansvarlig tilgang til relevant sikkerhetsdokumentasjon og systemene som benyttes for behandling av helse- og personopplysninger;

e. avdekke, registrere, rapportere og lukke avvik knyttet til informasjonssikkerhet, herunder loggføre og dokumentere ethvert forsøk på ikke-autorisert tilgang og andre brudd på opplysningssikkerheten i datasystemene. Slik dokumentasjon skal oppbevares hos Underleverandør;

f. ved mistanke om eller konstatering av avvik, omgående varsle Databehandler og Dataansvarlig. I varselet opplyses avviket med forklaring om årsak, tidsrom og tidspunktet avviket ble oppdaget, kategoriene av og omtrentlig antall registrerte som er berørt, kategoriene av og omtrentlig antall registreringer av personopplysninger som er berørt, navnet på og kontaktopplysningene til personvernombudet eller et annet kontaktpunkt der mer informasjon kan innhentes, antatte konsekvenser av avviket og hvilke umiddelbare tiltak som er igangsatt eller vurderes igangsatt for å håndtere avviket;

g. dokumentere ethvert avvik, herunder de faktiske forhold knyttet til avviket, dets virkninger og eventuelle iverksatte utbedringstiltak;

h. omgående varsle Databehandler og Dataansvarlig ved uautorisert utlevering av personopplysninger;

i. registrere all autorisert og uautorisert tilgang til informasjon. Alle oppslag som gjøres skal registreres slik at de kan spores til den enkelte bruker (dvs. ansatte hos Databehandler, underleverandører og Dataansvarlig). Loggene skal oppbevares til det ikke lenger antas å være bruk for dem eller i henhold til det Tjeneste/oppdragsavtalen spesifiserer;

j. bistå Dataansvarlig med å sikre overholdelse av forpliktelsene i personvernforordningen artiklene 32–34, dvs.:
   - sikkerhet ved behandlingen;
   - melding til tilsynsmyndigheten om brudd på personopplysningssikkerheten;
   - underretning av den registrerte om brudd på personopplysningssikkerheten;

k. i forbindelse med sikkerhetsrevisjon som utføres av Dataansvarlig eller en tredjepart utpekt av Dataansvarlig, framlegge interne revisjonsrapporter, interne prosedyrer, rutiner, sikkerhetsarkitektur, risiko og sårbarhetsanalyser med tiltak og andre dokumenter av betydning for revisjonen;

l. varsle Dataansvarlig og Databehandler om alle forhold som medfører endring i risikobildet;

m. innhente godkjenning av Dataansvarlig før gjennomføring av enhver endring av databehandlingen hos Underleverandør som har eller kan ha betydning for informasjonssikkerheten.

Nærmere krav til Underleverandørs informasjonssikkerhet er angitt i **Vedlegg 2** (hvis relevant).

Ved brudd på denne Avtalen eller på bestemmelsene i personopplysningslovgivningen, helselovgivningen eller annen relevant lovgivning kan Dataansvarlig kreve endringer i behandlingsmåten eller pålegge Underleverandør å stoppe den videre behandlingen av opplysningene med øyeblikkelig virkning.

Underleverandør skal dokumentere sine rutiner og alle tiltak truffet for å oppfylle kravene angitt ovenfor. Denne dokumentasjonen skal på forespørsel gjøres tilgjengelig for Dataansvarlig.

8. Underleverandørens bruk av annen databehandler

Dersom Underleverandøren benytter annen databehandler eller andre som normalt ikke er ansatt hos Underleverandøren, må det inngås avtale med denne virksomheten (annen databehandler) hvor de pålegges de samme plikter som er angitt i denne Databehandleravtalen.

Enhver som utfører oppdrag på vegne av Underleverandøren som omfatter behandling av personopplysninger skal være kjent med de forpliktelser som fremgår av denne Databehandleravtalen og alle rettslige forpliktelser, og skal etterleve disse.

Underleverandøren plikter å føre oversikt over sine underleverandører/andre databehandlere (se vedlegg 3) og skriftlig informere Databehandleren om eventuelle påtenkte endringer vedrørende supplering eller bytte av underleverandør før endringen gjennomføres. Dette må varsles i god tid slik at Dataansvarlig gis mulighet til å motsette seg endringen.

9. Overføring av personopplysninger til utlandet

Ingen helse- og personopplysninger som behandles under denne databehandleravtalen skal føres ut av Norge, med mindre det er særskilt avtalt med de Dataansvarlige. I tillegg skal helse- og personopplysninger være plassert på servere i Norge (jf. arkivloven § 9 bokstav b). Eventuelle unntak som innebærer overføring til utlandet skal godkjennes eksplisitt av Dataansvarlig før behandlingen starter.

Databehandler bekrefter at ingen av underleverandørene overfører helse- og personopplysninger som omfattes av denne Avtalen til utlandet, med unntak for slike overføringer/databehandleringer som er angitt i Vedlegg 1 B for underleverandørene i Vedlegg 3. Dette omfatter også fjerntilgang fra utlandet.

Bruk av underleverandører som overfører helse- og personopplysninger til land utenfor EU/EØS (tredjeland) skal avtales skriftlig med Dataansvarlig på forhånd. Ved overføring av helse- og personopplysninger til land utenfor EU/EØS (tredjeland) skal Databehandler benytte godkjente EU-overføringsmekanismer.

Ved overføring til utlandet, uavhengig av om det er innenfor EU/EØS eller utenfor EU/EØS (tredjeland), skal Databehandler gi nødvendig dokumentasjon om sikkerhet, risiko og etterlevelsesnivå knyttet til aktuelle underleverandører slik at Dataansvarlig får nødvendig informasjon for å kunne gjennomføre en særskilt risikovurdering. Dataansvarlig kan nekte samtykke til den aktuelle overføringen basert på spesifikke risikoer som fremkommer av Dataansvarliges egen risikovurdering.

10. Taushetsplikt

Underleverandøren har taushetsplikt vedrørende dokumentasjon og personopplysninger som Underleverandøren får tilgang til under Databehandleravtalen. Underleverandøren skal påse at alt personell er kjent med og forpliktet av taushetsplikten under denne Databehandleravtalen.

Denne bestemmelsen gjelder også etter opphør av Databehandleravtalen.

11. Innsyn, verifikasjon og revisjon

Dataansvarlig kan til enhver tid kreve innsyn i og verifikasjon av Underleverandørs behandling av personopplysninger tilhørende Dataansvarlig, herunder innsyn i og verifikasjon av dokumentasjon for oppfyllelse av kravene til informasjonssikkerhet og Underleverandørs system for internkontroll.

Retten til innsyn gjelder alle tekniske, organisatoriske og administrative forhold som er relevante for sikkerheten ved behandlingen som utføres av Underleverandør på vegne av Dataansvarlig, og øvrige innsynsrettigheter nedfelt i lov. Hvis Dataansvarlig ber om innsyn skal generell informasjon fra revisjonen gjøres tilgjengelig for andre Dataansvarlige som benytter samme tjeneste hos Underleverandør.

Dataansvarlig skal så vidt mulig gi Underleverandør varsel i rimelig tid ved krav om innsyn og kontroll, vanligvis minst 30 dagers varsel. For krav om dokumentinnsyn bør det gis minst 14 dagers varsel. Dataansvarlig skal medvirke til at innsyn og kontroll kan koordineres mellom flere Dataansvarlige som får levert tjenester fra Databehandler. Innsyn og kontroll kan gjennomføres av Dataansvarlig eller tredjepart som Dataansvarlig utpeker. Underleverandør kan kreve dekket dokumenterte merkostnader som påløper ved slike revisjoner.

Underleverandør skal gi Datatilsynet og annen relevant tilsynsmyndighet tilgang og innsyn i behandlingen av helse- og personopplysninger slik det følger av relevant lovgivning.

Underleverandør skal uten ugrunnet opphold korrigere eventuelle avvik. Avvik som skyldes Underleverandøren eller dennes underleverandører skal korrigeres uten kostnad for Dataansvarlig. Underleverandøren skal skriftlig redegjøre for korrektive tiltak og plan for gjennomføring.

12. Varighet og opphør

Denne Databehandleravtalen gjelder så lenge Underleverandøren behandler personopplysninger på vegne av Dataansvarlig. Denne avtalen skal signeres før underleverandør begynner å behandle personopplysninger.

Ved brudd på denne Databehandleravtalen eller gjeldende personvernregelverk, kan Dataansvarlig kreve at Underleverandøren stanser videre behandling av personopplysninger med umiddelbar virkning.

Ved opphør av Databehandleravtalen plikter Underleverandøren (og dennes godkjente underleverandører, jf. punkt 8) å returnere samtlige dokumenter og elektroniske data som Underleverandøren måtte ha i sin besittelse i egenskap av Underleverandør.

Som et alternativ til tilbakelevering kan Dataansvarlig bestemme at alle eller deler av opplysningene som omfattes av Databehandleravtalen skal ugjenkallelig slettes av Underleverandøren etter mottak av skriftlig instruks fra den Dataansvarlige. Underleverandøren har ingen rett til å beholde kopier av opplysninger i noe som helst format.

Underleverandøren må fremlegge skriftlig dokumentasjon på at sletting og/eller destruksjon har funnet sted i henhold til Databehandleravtalen innen rimelig tid etter opphør av denne, og må bekrefte at Underleverandøren ikke har beholdt noen kopi, utskrift eller annen gjengivelse av noen som helst del av materialet, uansett bruk av medium.

Underleverandøren plikter å sjekke og dokumentere at ovennevnte krav også er overholdt av eventuelle godkjente underleverandører.

13. Avtalebrudd(mislighold) og erstatning for økonomiske utlegg

Avtalebrudd foreligger dersom en part ikke oppfyller sine forpliktelser etter avtalen, og dette ikke skyldes forhold som den andre parten har ansvaret eller risikoen for. Den som vil påberope seg avtalebrudd må

meddele dette til den annen part med skriftlig begrunnelse, uten ugrunnet opphold etter at det aktuelle forholdet ble kjent.

Dersom en part i vesentlig grad misligholder sine forpliktelser etter avtalen kan den andre parten heve avtalen. Den som ønsker å heve skal i skriftlig varsel sette en rimelig frist for retting av forholdet. Av varselet skal det fremgå at avtalen vil bli hevet dersom forholdet ikke er rettet innen fristen.

Overtredelse av taushetsplikt vil alltid anses som vesentlig mislighold.

Dersom avtalebrudd på en eller flere av bestemmelsene i denne avtalen fører til økonomisk tap i form av økte utgifter eller reduserte inntekter, kan den skadelidte parten kreve at motparten dekker tapet.

14. Rettsvalg og verneting

Dette er nærmere regulert i gjeldende regelverk, herunder fortrinnsvis partenes tjeneste- eller leverandøravtale, subsidiært lovbestemt bakgrunnsrett dersom annet ikke er direkte avtalt mellom partene.

Riktig verneting er Bergen tingrett med mindre annet fremgår av Tjenesteavtalen mellom partene.

15. Undertegning

Denne avtalen undertegnes i to eksemplarer og partene beholder ett hver.

_____	_____
Sted og dato	Sted og dato
_____	_____
Helse Vest IKT AS Ole Jørgen Kirkeluten	[Navn på Underleverandør] [Navn]
Administrerende direktør	[Stilling]

VEDLEGG 1 – BEHANDLINGENS FORMÅL, OPPLYSNINGER OG BEHANDLINGER

Tabellene oppdateres fortløpende og dateres.

[*dato/måned/år*] *Sett inn dagens dato.*

B. Formålet med og varigheten av behandlingen

Formålet med og varigheten av behandling av helse- og personopplysninger er:

Husk at hver behandling må være knyttet til spesifikke og uttrykkelig angitt formål – se eksempel nedenfor. Fjern det som ikke er aktuelt.

OBS- Fjern denne boksen med veiledningstekst.

Hvorfor gjør underleverandøren denne databehandlingen? Hvorfor trenger vi ekstern bistand i driften?

Formålet må komme tydelig frem.

Dersom formålet ikke klart fremkommer av driftsavtalen skal dette være klart for kunden(e)/de dataansvarlige for systemet, så spør gjerne der.

Dato (fra/til)	Navn på tjeneste	Formålet med behandlingen	Varigheten av behandlingen
[dato/måned/år-]	[Bistand ved feilretting]	[Bistå ved feilretting – for å gjenopprette og stabilisere drift]	[I avtaleperioden]
[dato/måned/år-]	[Vedlikehold av system]	[For å kunne opprettholde drift og forvaltning]	[I avtaleperioden]
[dato/måned/år-]	[Filoverføring]	[Overføre større datamengder for å…]	[Til formålet er oppnådd]
[dato/måned/år-]	[Fillagring]	[Lagring av filer for å…]	[I avtaleperioden]
[dato/måned/år-]	[Fyll ut]	[Fyll ut]	[Fyll ut]

B. Behandling av helse- og personopplysninger

Det følger av personvernforordningen art 4 nr.2 at med «behandling» menes**:** «*enhver operasjon eller rekke av operasjoner som gjøres med personopplysninger, enten automatisert eller ikke, f.eks. innsamling, registrering, organisering, strukturering, lagring, tilpasning eller endring, gjenfinning, konsultering, bruk, utlevering ved overføring, spredning eller alle andre former for tilgjengeliggjøring, sammenstilling eller samkjøring, begrensning, sletting eller tilintetgjøring*»

Følgende behandlinger av personopplysninger omfattes av Avtalen:

Se eksempler nedenfor – stryk det som ikke passer.

OBS- Fjern denne boksen med veiledningstekst.

Hvordan gjennomfører underleverandøren denne databehandlingen? Hva er det denne underleverandøren konkret utfører av oppgaver og handlinger knyttet til lagrede personopplysninger?

Dette kan fremkomme av avtalene med underleverandøren, bør være kjent for forvaltningen og gjerne også for kundene/ de dataansvarlige av løsningen.

Databehandling	Nærmere beskrivelse av databehandlingsaktiviteter	Lokasjon av system og sted for databehandlingsaktivitet
[Tilgang til lagrede personopplysninger for feilretting]	[Særlig relevant – forslag til tekst: Leverandøren har behov for tilgang til lagrede personopplysninger for feilsøking og feilretting]	[Forslag til tekst: Databasen ligger hos Helse Vest IKT. Leverandør gis tilgang via VPN (Bomgar-løsningen), på bestilling fra Helse Vest IKT, for å utføre denne behandlingsaktiviteten]
[Tilgang til lagrede personopplysninger for support oppdatering]	[Særlig relevant – forslag til tekst: Leverandøren har behov for tilgang til lagrede personopplysninger for oppdatering]	[Fyll ut]
[Tilgang til lagrede personopplysninger for konfigurasjon]	[Særlig relevant – forslag til tekst: Leverandøren har behov for tilgang til lagrede personopplysninger for konfigurasjon. Leverandøren kan utføre konfigurasjonsendringer på oppdrag fra databehandler eller dataansvarlig]	[Fyll ut]
[Innsamling]	[Fyll ut hvis relevant]	[Fyll ut]
[Registrering]	[Fyll ut hvis relevant]	[Fyll ut]
[Organisering]	[Fyll ut hvis relevant]	[Fyll ut]
[Strukturering]	[Fyll ut hvis relevant]	[Fyll ut]
Lagring]	[Fyll ut hvis relevant]	[Fyll ut]
[Tilpasning eller endring]	[Fyll ut hvis relevant]	[Fyll ut]
[Gjenfinning]	[Fyll ut hvis relevant]	[Fyll ut]
[Sammenstilling]	[Fyll ut hvis relevant]	[Fyll ut]
[Sletting eller tilintetgjøring]	[Fyll ut hvis relevant]	[Fyll ut]
[Utlevering/Overføring]	[Fyll ut hvis relevant]	[Fyll ut]
[Andre former for tilgjengeliggjøring]	[Fyll ut hvis relevant]	[Fyll ut]
[Andre relevante behandlinger]	[Fyll ut]	[Fyll ut]

C. Typer av opplysninger

OBS- Fjern denne boksen med veiledningstekst.

Stikkordet her er «hva er lagret om de registrerte». Hvilke opplysninger ligger lagret i løsningen som underleverandøren eventuelt kan få tilgang til/komme i inngrep med.

«De registrerte» er Ikke begrenset til kun å gjelde pasienter, men også f.eks. ansatte, konsulenter eller andre personer Helse Vest behandler opplysninger om.

Følgende helse- og personopplysninger behandles:

Her listes opp hvilke helse- og personopplysninger som omfattes – se eksempler nedenfor – fyll ut/stryk det som passer.

Personopplysninger
[Navn]
[Etternavn]
[Fødselsnummer]
[Bosted]
[Mobilnummer/telefonnummer]
[E-post]
[Pårørende]
[Stillingsinformasjon]
[Oversikt over lønn]
[Oversikt over permisjoner]
[Oversikt over IA og -personaloppfølging]
[Kompetanse (utdanning, kurs, arbeidserfaring, sertifikat/autorisasjoner mm)]
[Andre opplysninger – fyll ut]

Helseopplysninger
[Legemiddelbruk]
[Diagnoseopplysninger]
[Opplysninger fra helseregistre]
[Behandlingssted]
[Fastlege]

[Andre opplysninger – fyll ut]

D. Kategorier av registrerte

Følgende kategorier av personer behandles det opplysninger om (registrerte):

Her listes opp hvilke kategorier av registrerte som omfattes – se eksempler nedenfor. Stikkordet her er «om hvem». Hvilke personer ligger det data om i løsningen. Fyll ut/stryk det som ikke passer.

Kategorier av registrerte		
[Pasienter] [Barn] [Foreldre] [Pårørende] [Fullmektiger/verge/formyndige]	[Ansatte i Helse Vest IKT] [Tidligere ansatte i Helse Vest IKT] [Ansatte i helseforetak] [Tidligere ansatte i helseforetak]	[Ansatte hos leverandør] [Ansatte i samarbeidende firma] [Andre opplysninger – fyll ut]

VEDLEGG 2 – DETALJERTE KRAV TIL INFORMASJONSSIKKERHET FOR DATABEHANDLER OG UNDERLEVERANDØRER (ANNEN DATABEHANDLER)

Krav til informasjonssikkerhet er lik for Databehandler og Underleverandør (annen Databehandler).

Her listes opp detaljerte krav til informasjonssikkerhet.

[*dato/måned/år*] *Sett inn dagens dato.*

Nr.	Tema	Krav
13.	Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren	Databehandler og Underleverandør skal følge relevante krav i Norm for informasjonssikkerhet og personvern, inkludert vedlegget «Oversikt over Normens krav».
14.	Sikring av data	Databehandler og Underleverandør skal ha mekanismer for data under transport, prosessering og lagring for å ivareta integritet og konfidensialitet. Mekanismene spesifiseres i pt. 4, 5 og 6 under. *[Mekanismer = tiltak som f.eks. kryptering, logging. Det skal stå beskrevet i driftsavtalen hvilke tiltak som er gjort. Hvis det ikke står i driftsavtalen må det stå i databehandleravtalen.]*
15.	Autentisering	Ved tilgang til data ved tjenstlig behov skal det benyttes personlige brukernavn med passord. Databehandler og Underleverandør skal ha etablert passordpolicy.
16.	Logging og sporbarhet	Dersom løsning ligger hos Helse Vest IKT er kravet at all tilgang skal gå igjennom VPN (Bomgar-løsningen). All behandingsaktivitet blir logget og er sporbar. *[Mer om Bomgar-løsningen finnes her: https://helse-vest-ikt.no/brukarstotte/for-leverandorar#fjernaksess]* Dersom løsning ligger hos/overføres Underleverandør skal Underleverandør skal sikre at all tilgang til og forsøk på tilgang til data kan dokumenteres. Logger skal sikres mot endring, og skal kunne forevises på etterspørsel.
17.	Tilgjengelighet, redundans og skalering	Underleverandør skal sikre at tjenesten er tilgjengelig iht. krav i kontrakt/SLA, inkludert beskyttelse mot tjenestenektangrep, programvare-, nettverks- og maskinvarefeil, og andre hendelser som kan gi redusert tilgjengelighet.

18.	Testdata	All testing skal avtales med Helse Vest IKT. Ved bruk av personopplysninger ved test skal det alltid tas utgangspunkt i bl.a. det grunnleggende personvernprinsippet i personvernforordningen art 5 b) «dataminimering». Det skal kun brukes adekvate og relevante personopplysninger og det skal begrenset til det som er nødvendig for formålet for behandlingen/testen.
19.	Sletting og tilbakelevering	Underleverandør skal ha rutiner som skal kunne vises på forespørsel fra databehandler på vegne av Dataansvarlig.
20.	Lagringstid	Underleverandør skal sørge for at data slettes iht. avtalens krav om lagringstid, og at data er tilgjengelige inntil avtalt tidspunkt for sletting.
21.	[Backup og restore]	[Fyll ut hvis relevant]
22.	[Kryptering ved lagring]	[Fyll ut hvis relevant]
23.	[Kryptering i kommunikasjon]	[Fyll ut hvis relevant] *F.eks https med TLS-versjon (transport layer security)*
24.	[Annet]	[Fyll ut hvis relevant]

VEDLEGG 3 – UNDERLEVERANDØRER

Tabellene oppdateres fortløpende.

Her listes opp hvilke underleverandører som benyttes av Databehandlers underleverandør – se eksempler nedenfor- fylles kun ut når underleverandøren benytter andre underleverandører.

[*dato/måned/år*] *Sett inn dagens dato.*

Navn på underleverandør	Leveranseområde	Stedlig plassering
[ABC]	[Datasenter, hosting]	[Stockholm, Sverige]
[DEF]	[IT-supporttjenester]	[Oslo, Norge]
[XYZ]	[Backup]	[Paris, Frankrike]

Versjon 3.0

Endringslogg:

*Kap.2 Dataansvarlig skal *på forespørsel kunne be* Databehandler om å få seg forelagt avtalen som inngås mellom Helse Vest IKT AS og underleverandøren før signering.

*Behandlings/Dataansvarlig er blitt erstattet med Dataansvarlig.

*Lagt til flere forslag til opplysninger i Vedlegg 1 Tabell C og D

*Lagt til standardtekster i Vedlegg 2

Versjon 3.1

Endringslogg:

*Kap.4 Endret tekst ettersom det ikke lenger skal henvises til tjenesteavtalen

*Kap.14 Endret tekst ettersom det ikke lenger skal henvises til tjenesteavtalen