Direktoratet for e-helse

Version: December 2020

GUIDE - Standard Data Processing Agreement

The standard data processing agreement with guide has been prepared by the Norwegian Directorate of eHealth on assignment from the Ministry of Health and Care Services.

The purpose of this guide is to provide further information regarding the substantive content of the agreement, as well as provide practical guidance on how the appendices to the agreement should be used and filled in.

Chapter 1 of the guide provides information about the background, purpose and scope of the standard agreement and how this is structured.

Chapter 2 provides remarks to each of the clauses in the standard agreement. The chapter is structured in such a manner that each section is linked to the corresponding clause in the agreement.

Chapter 3 provides remarks to the appendices to the standard agreement, as well as examples for how these are to be filled in.

For a more detailed description of more general issues, for example, when there is a processor assignment that requires an agreement, delegation of responsibilities and clarification of roles in such an assignment, reference is made to the guide from the Norwegian Data Protection Authority.

Contents

25

1 About the standard agreement

1.1 Background

In its letter of allocation for 2020, the Norwegian Ministry of Health and Care Services commissioned the Directorate of eHealth to:

- *Prepare a standard data processing agreement with a guide that the sector can use when entering into such agreements*

This standard agreement is based on the Template for Data Processing Agreement published at ehelse.no on 5 November 2018. No significant material amendments were made to the previous agreement template. Some structural amendments were made to ensure that the actual text of the agreement shall remain unchanged, see section 1.3 below. Furthermore, the focus of the agreement is now more on the processing of personal health data, see section 1.2.2. There were also some linguistic amendments to the text of the agreement.

It is an objective that a standard data processing agreement for the sector will both assist in ensuring compliance with the data protection regulations and simplify contract management for the individual establishments.

1.2 Use of the standard agreement

1.2.1 Purpose of the agreement

The standard agreement shall contribute to ensuring that personal health data are processed in accordance with the regulations when using processors in the healthcare and care services sector.

The regulations do not stipulate any requirements for structure or format when establishing a Data Processing Agreement. There is thus the freedom to draw up the type of agreement one may wish to have, provided that the requirements in the regulations are complied with. In this standard agreement, the relevant requirements in the data protection regulations relating to the content of a Data Processing Agreement are included in the text. Therefore, use of the standard agreement will ensure there is greater certainty that the agreement which is entered into covers the necessary requirements.

It is the desire of the Norwegian Directorate of eHealth that establishments in the healthcare and care services sector use this standard agreement when entering into a Data Processing Agreement that covers personal health data (see section 1.2.2 Scope). The widespread use of a standardised agreement in the sector will simplify both the conclusion of agreements and subsequent contract management for both controllers and processors as the agreement structure and content become uniform and more familiar.

1.2.2 Scope – when should the standard agreement be used?

- Personal health data

The standard agreement has been drawn up with a view to processing personal health data. This is reflected in the agreement's use of terms, scope and regulatory references. It is therefore recommended that the standard agreement is primarily used when the processor will process personal health data on behalf of the controller.

The requirements that apply when processing personal health data are essentially the same as those that apply for other personal data. However, personal health data constitutes "special categories of personal data", which entails that the requirements are stricter in terms of both requirements for clarity and degree of detail and requirements for information security measures.

When the processor assignment does not include personal health data, but exclusively concerns the processing of "ordinary" personal data, it may be more appropriate to use a different starting point for the agreement, for example, from the Norwegian Data Protection Authority or the Norwegian Digitalisation Agency.

The Norwegian Data Protection Authority has prepared guidance material which provides a practical introduction to when a Data Processing Agreement must be entered into and the requirements for the content of such an agreement. The Norwegian Data Protection Authority also makes reference to the standard data processing agreement adopted by the Danish Data Protection Authority. That agreement has been submitted to the European Data Protection Board (EDPB) and can also be used in Norway.

- The Norwegian Data Protection Authority's guide – "How to create a Data Processing Agreement"
- Standard Data Processing Agreement (Danish/English)

The Norwegian Digitalisation Agency has prepared a Data Processing Agreement that is primarily intended for relatively basic processor assignments and which is well-suited for use together with the Norwegian State's standard agreements (SSA). They have also created a checklist that can be used to verify that a provider's standard data processing agreement satisfies Norwegian requirements.

- Data Processing Agreement and checklist

Scope of the processor assignment

The standard agreement can be used both in extensive processor assignments (multiple processing assignments/large volume of data) and in assignments that are more simple in nature. The basic requirements for the processing will be the same, however the complexity of the assignment will be reflected in the appendices to the agreement. There must be a proportionality assessment to ensure that the scope of the agreement is adapted to the assignment. The more extensive the processor assignment, the greater the requirements for the description of this in the appendices to the agreement.

Relationship to the Service/assignment agreement

The standard agreement may be used irrespective of the type of agreement that constitutes the basis for the services/assignments that involve the processing of personal data on behalf of the controller. This may be, for example, the Norwegian State's standard agreements (SSA), Data Management Association Norway's contract standards (PS2000), terms of use, etc. The extent to which the processing of data is referred to in the Service/assignment agreement will vary. In any event, the relevant factors relating to the actual processor assignment will be specified in the Data Processing Agreement. Requirements for such contractual provisions are stipulated in Article 28, 3. If the processing of data is described in a different manner (contrary) in the Service/assignment agreement and in the Data Processing Agreement, the description in the Data Processing Agreement shall apply.

"Battle of Forms" - Who decides which agreement format shall be used?

There is no requirement to use a specific format or requirement for the particular structure of a Data Processing Agreement. Several establishments have prepared their own agreement templates that they wish to use for processor assignments when they are either the controller or processor. The structure of the agreement is of little importance and the decisive factor is that the material content covers the requirements in the regulations. For individual establishments, it will be both easier and provide greater assurance that the requirements are covered if a form of agreement is used that they are well-acquainted with. Issues relating to which agreement template to use are often referred to as "Battle of Forms".

It is generally the controller who decides which form of agreement is to be used. It is the controller who specifies the data processing assignment and who determines the framework for this.

However, in some instances this starting point is not practically feasible. For example, when concerning providers that offer commercial, standardised services which involve the processing of personal data, it may not be very appropriate to have to deal with a large number of different agreement formats from different customers (controllers). In such instances, the provider's (processor's) agreement template or standard terms will normally have to be used as a basis.

Even if this type of standardised Data Processing Agreement has been drawn up by the provider, it is the customer, as controller, who is responsible for ensuring compliance with the regulatory requirements. The customer must therefore ensure that the agreement covers the conditions it needs to cover, or possibly attempt to include the necessary amendments and assess whether the Data Processing Agreement is acceptable before it is entered into. The Norwegian Digitalisation Agency's checklist[1] for Data Processing Agreements could be a starting point for the assessment in such an instance. When concerning major providers and international stakeholders it will often be the case that there will be limited or no ability to influence the content of their standard data processing agreement/terms and conditions for the processing of personal data. If this is the case, the

[1] https://www.anskaffelser.no/sites/anskaffelser2/files/sjekkliste_databehandleravtale_2020.docx
Note that this has not been updated in connection with Schrems II, see section 3.10.2 below.

customer must consider whether the agreement entails an acceptable level of risk for it to be entered into, or whether they should refrain from doing so.

1.3 Structure of the standard agreement

The text of the agreement

The standard agreement is structured with a general text that must always be used. No amendments should be inserted in the actual text of the agreement. If there is a need to make amendments or adjustments to the actual text of the agreement, these must be described in Appendix 5 - Amendments to the general text of the agreement upon entering into the agreement. This ensures that the structure of the agreement is uniform and clear and also corresponds with how the Norwegian State's standard agreements (SSA) are structured.

The appendices

- Appendix 1: The specific assignment, including the associated processing of data, must be specified in Appendix 1.
- Appendix 2: The standard agreement describes the basic requirements for the processor's information security. This must be elaborated on and specified as required in Appendix 2.
- Appendix 3: Administrative provisions such as contact details, specific audit routines, regular meetings and reporting, etc., are inserted in Appendix 3.
- Appendix 4: If the processor uses a subcontractor to process the data in question, this must be stated in Appendix 4.
- Appendix 5: No amendments should be made to the actual text of the agreement. If, when the agreement is entered into, there is a need for amendments or additions to the general contractual provisions, these must be made in Appendix 5.
- Appendix 6: Amendments after the agreement has been entered into are collated in Appendix 6.

2 Remarks to the individual clauses in the standard agreement

Front page

The contracting parties must be identified on the front page of the agreement by the names and organisation numbers of the establishments.

The Data Processing Agreement will be linked to another contractual arrangement between the parties that involves the processing of personal health data. Such an agreement may be different in nature, and may be an assignment agreement, a service agreement, terms of use etc. It is important that the connection to the overarching agreement is clearly stated, and includes the title, date and any case reference. This is particularly to ensure that the contractual arrangements are viewed in a holistic context on the agreement date, and is also intended to simplify the follow-up of the agreement over time.

The agreement must be signed by an authorised representative of the establishment. This will be the establishment's senior manager or someone from the establishment who has been delegated this authority.

2.1 About the agreement

This clause sets out the legal framework for the Data Processing Agreement. Conditions that conflict with this framework must not be agreed to and any such contractual provisions shall be waived.

The appendices to the agreement are included in the agreement as a whole. Agreed amendments that are inserted in the amendment appendices (Appendix 5 and Appendix 6) take precedence over the text of the agreement. The other appendices provide supplementary descriptions/addendums to the agreement.

2.2 Definitions

The terms used in the Agreement are to be understood as they are defined in relevant legislation.

Since the agreement has been specifically structured with a view to processing personal health data, in the Norwegian version of the agreement the term "dataansvarlig" is used throughout the agreement instead of "behandlingsansvarlig". The terms are synonyms and are to be understood as "controller" is defined in Article 4 (7) of the General Data Protection Regulation 7. This is stipulated in Section 2 of the Patient Records Act.

2.3 Purpose of the Agreement

Pursuant to Article 28 (3) of the General Data Protection Regulation, a processor’s processing of data on behalf of the controller shall be governed by a contract. The agreement shall ensure that the regulations are complied with and that the data subject's rights are safeguarded.

2.4 Scope

The first paragraph states that the Data Processing Agreement regulates the processing of data by the processor on behalf of the controller as a result of the service/assignment agreement. The Data Processing Agreement takes precedence with regard to matters that are specifically related to the processing of personal data if there should be any conflict between the agreements.

The intention of the second paragraph is to highlight that the Data Processing Agreement can be expanded to include more/new processor arrangements between the same parties. This may, for example, be the case when an operations service provider will operate new solutions for the same customer. A new agreement will then be entered into between the parties, which will possibly take the form of an amendment agreement to the original operating agreement for the operation of the new solution and this will be a "subsequent written agreement between the parties".

In these instances, it is not necessary to enter into a completely new Data Processing Agreement. The parties may instead agree to amend the Data Processing Agreement they have already entered into (see section 14), by incorporating the operation of the new solution into the appendices to the Data Processing Agreement. There may be other purposes, other processing and other types of data etc. related to the new processor arrangement between the parties and the appendices must be amended in line with the new processing activities.

2.5 Purpose of the processing, data and processing activities

This clause refers to Appendix 1 of the agreement, which shall further specify the purpose and duration of the processing activity(ies), what processing and types of data are covered and the categories of people that are registered.

Further references and examples are provided below in section 3.1 concerning Appendix 1.

2.6 The framework for the processing of personal health data

This clause reflects the overarching principle in a processor arrangement: The processor only processes the data on behalf of the controller and only as the controller has stipulated.

2.7 The Controller’s obligations

The controller is responsible for compliance with the regulations. This also involves ensuring that there is a valid basis for the processing of data that the processor is instructed to carry out.

For further information regarding the controller's obligations, see the Norwegian Data Protection Authority‘s website.

2.8 The Processor’s obligations

The processor shall only process personal health data in accordance with instructions from the controller. Each of the clauses must be specified and elaborated on insofar is necessary and relevant in the appendices to the agreement.

2.8.1 General

Clause 8.1 of the agreement further regulates the manner in which the processor may process data on behalf of the controller. The clause has been divided into two parts, each of which stipulates more specific requirements for what the processor is obligated to do and to refrain from doing. In general, the processor pledges to process personal data in accordance with applicable regulations, the controller's instructions, and requirements in the Code of conduct for information security and data protection in the healthcare and care services sector.

2.8.2 Technical, organisational and security measures

The controller and processor have an independent duty to implement *“appropriate technical and organisational measures to ensure a level of security appropriate to the risk”,* cf. Article 32 of the General Data Protection Regulation. Among other things, this encompasses, insofar as is relevant, necessary measures to prevent the random or unlawful erasure or loss of data, unauthorised access to or distribution of data, and any other use of personal health data which is not in accordance with the Data Processing Agreement, and measures to restore accessibility and access to the data in the event of incidents.

Security measures must be introduced based on a risk assessment which, among other things, needs to take into account the type of data processed.

The text of the agreement also lists some mandatory minimum requirements for security measures that are based on requirements in the General Personal Data Regulation. For example, there are requirements for internal control systems, logging and routines for detecting and processing non-conformities.

The requirements for technical and organisational security measures should be further described and detailed in Appendix 2 – Detailed requirements concerning information security. See chapter 3.2 of the guide for guidance on how to fill in this appendix.

2.9 Use of subcontractors

The processor is permitted to use subcontractors (sub-processor) when executing the processor assignment, provided that these subcontractors are known to and accepted by the controller. The processor's use of subcontractors must therefore be specified in appendix 4 at all times.

The explicit approval of the controller is not required when changing or using a new subcontractor, however the controller must be notified of any such changes in order for the controller to be able to consider the change and possibly oppose this.

2.10 Transfer of personal data to other countries

Establishments which transfer personal data to other countries shall ensure that the level of protection stipulated in the Personal Data Act is not undermined in connection with the transfer. All EU/EEA countries have transposed the General Data Protection Regulation and thereby ensured that personal data are processed responsibly. The European Commission has also recognised that some third countries provide an adequate level of protection for personal data. Personal data may therefore be freely transferred to these states (list updated by the European Commission). This assumes that the other conditions of the Personal Data Act are met.

If providers or services established outside the EU/EEA are to be used, there is a requirement to assess the level of security in the country in question. The purpose of this is to ensure that the data are subject to the same level of protection as it would receive in the EU/EEA. When the establishment transfers personal data to states outside the EU/EEA, known as “third countries”, it must use one of the grounds for transfer stipulated in the Regulation. Grounds for transfer may include the EU’s standard agreements for the transfer of personal data or a decision by the European Commission on an adequate level of protection in the applicable third country.

When transferring data to countries outside the EU/EEA, the establishment must ensure that it has sufficient expertise (for example, legal expertise) at its disposal in order to carry out the assessments and follow up the Data Processing Agreement in accordance with relevant requirements.

See the Norwegian Data Protection Authority's website for updated and supplementary information regarding transfers to other countries.

2.10.1 Specifics regarding the use of cloud services

A cloud service is a term that encompasses everything from data processing and data storage to software on servers located in remote server parks, which normally use the Internet as a carrier of the data traffic.

Cloud services are characterized by being designed for dynamic scaling in the event of a change in capacity requirements, and by it being the general rule that one pays for actual use. For example, providers offer server capacity in the cloud on an hourly basis.

If personal health data are to be processed using a cloud service, there are some specific requirements that should be set for the provider. This particularly applies to the requirements in clauses 8.1 and 8.2 of the Data Processing Agreement and the controller must consider whether these requirements need to be further specified in Appendix 2 – Detailed requirements concerning information security.

See the Code of Conduct's guide to the use of cloud services for the processing of personal health data for topics of assessment that the controller should consider including in a Data Processing Agreement that relates to the provision of cloud services. The assessments must be carried out before the service commences.

Points that are of particular relevance will be:

- The principles for access control
- How the return of data/ application shall take place at the conclusion of the agreement.
- How the controller can obtain access in the technical solution.
- How the rights of patients to access the personal data, make corrections and deletions are safeguarded, as well as access to logs.
- Requirements that the provider carries out risk assessments and that these are revised in the event of changes, and that the controller has the right to view or access the assessments.

See also the Norwegian National Security Authority's "Expert security recommendations when outsourcing services".

2.10.2 Assessments when transferring to third countries

In July 2020, the Court of Justice of the European Union declared that the European Commission's Privacy Shield Decision was invalid as grounds for transferring personal data.[2] The consequence of this was that establishments cannot use Privacy Shield as grounds for transfer when the processing of personal data takes place in the USA. The assessments that must now be carried out when transferring personal data to the USA must also be carried out for all third countries.

If an establishment wishes to transfer personal data to a third country, the establishment must consider the other grounds for transfer that can be used.

For more information regarding the grounds for transfer when transferring to countries outside the EU/EEA and the assessments that the establishment needs to carry out, see the Norwegian Data Protection Authority's website.

2.11 Obligations of secrecy

The Data Processing Agreement stipulates that the confidentiality provisions in the Public Administration Act shall apply correspondingly to the parties and any subcontractors. Furthermore, any party that processes personal health data in a personal health data filing

[2] Case C-311/18 (Schrems II)

system for therapeutic purposes pursuant to the Patient Records Act and/or in a personal health data filing system pursuant to the Personal Health Data Filing System Act, has an obligation of secrecy pursuant to Section 21 et seq of the Health Personnel Act. Other parties that are granted access to or knowledge of personal health data from a personal health data filing system for therapeutic purposes or personal health data filing system have the same obligation of secrecy.

The parties shall take the necessary precautions to prevent unauthorised parties from gaining access to or knowledge of confidential material or information.

The obligation of secrecy shall also apply after the conclusion of the assignment. Employees or others who resign from their position with one of the parties or their subcontractors shall be required to maintain secrecy regarding the matters referred to above, including following their resignation.

2.12 Audits

This clause establishes the controller's right to access and control the processor's processing of data. This reflects that the processor only processes the data on behalf of the controller, and that it is incumbent on the controller to ensure that the data protection regulations are being complied with.

The clause pertaining to audits in the standard agreement has been taken from the corresponding provision in the Norwegian Digitalisation Agency's Data Processing Agreement. Appendix C to the Norwegian Digitalisation Agency's Data Processing Agreement lists several alternatives to specific routines for conducting audits that can be linked to the agreement. These alternatives can also be used in this standard agreement. If such auditing routines are agreed to, these must be included in Appendix 3 – Administrative Provisions. The guide to Appendix 3 provides examples that may be used.

2.13 Duration and termination

The agreement is valid for the duration of the processor assignment. Once the assignment has concluded, the processor shall no longer have access to the data that was processed on behalf of the controller. The clause provides instructions on how the data are to be returned/erased after the assignment has concluded.

2.14 Amendments to the agreement

Amendments to legal framework conditions may entail a need to change/adapt the agreement. The parties shall cooperate in connection with such necessary amendments.

There will also be a need to amend the agreement if changes are made to the processor assignment while the assignment is ongoing, for example, the assignment is expanded to include a new purpose or processing activities.

Such changes must be entered together in a change catalogue in Appendix 6. The processor is responsible for keeping this updated.

The other appendices must also be updated as required.

2.15 Governing Law, disputes and venue

This will be regulated in the Service/assignment agreement.

3 Remarks to the appendices

The appendices to the Data Processing Agreement must specifically describe what actions the processor will in fact perform.

- **Appendix 1** must always be filled in, and must be completed as much as possible before the agreement is presented to the processor. This includes:
    - The purpose of the processing.
    - The type of processing the processor will carry out on behalf of the controller.
    - The type of personal data that will be processed.
    - The categories of data subjects for whom data will be processed.
- **Appendix 2** must be filled in, unless this has already been satisfactorily described in the Service/assignment agreement. This applies to:
    - The technical and organisational measures the processor has to initiate to ensure information security.
- **Appendix 3** must always be filled in with contact details and any other relevant administrative information, for example, audit routines.

- **Appendix 4** must be filled in if the processor uses subcontractors when carrying out the processing activities.
- **Appendix 5** must be used if the parties have agreed to make amendments to the general text of the agreement when the agreement is entered into.
- **Appendix 6** must not be filled in when the agreement is entered into, but shall be used if changes are made to the assignment/processing or the agreement in general after the agreement has been entered into.

Note that the examples provided in the tables below are not intended to be indicative, limited or exhaustive. The list is only intended to provide examples of processing/processing activities, types of data, categories of persons and security requirements that are often included or typically set in a processor assignment. A specific assessment must be carried out in each instance to ensure that the tables are completed in accordance with the applicable assignment.

Most of the information required for appendices 1 and 2 will often be found in the record of processing activities linked to each processing purpose.[3] If the establishment (controller) has not maintained a record of the processing activities carried out by the processor, the record may, to a large extent, be completed with the data that needs to be inserted in Appendix 1 and Appendix 2, and possibly also Appendix 4.

The tables shall be kept up-to-date to ensure that they reflect the factual circumstances of the data processing assignment at all times. This entails that the appendices to the agreement must be updated if, for example, the controller wishes to have multiple categories of personal data processed or requires the processor to perform other types of services.

3.1 Appendix 1 – Purpose of the processing, data and processing activities

The following must be further specified in this appendix:

- the purpose and duration of the processing activity/activities - point A)
- the processing activities that are included - point B)
- the types of data that are included - point C)
- the categories of persons who are registered – point D)

If the processor assignment involves processing data in multiple services/for multiple purposes, it is recommended that these are described separately so that the agreement is

[3] Pursuant to Article 30 of the General Data Protection Regulation, the controller has an obligation to maintain a record of all processing activities carried out in the establishment. For each processing activity, the record must also include the purposes of the processing, the categories of data subjects and categories of personal data, recipients of personal data, any transfers to third countries, envisaged time limits for erasure, and a general description of security measures as referred to in Article 32 of the General Data Protection Regulation.

easier to read. This will enable each processing activity to be linked to specific and explicitly stated purposes.

If, for example, the assignment applies to two services: "*Processing Service XX"* and "*Transfer Service YY*", the structure of Appendix 1 could be as follows:

1. Processing service XX
   1A – Purpose and duration of the processing
   1B - Processing of personal health data
   1C – Types of Data
   1D – Categories of data subjects
2. Transfer service YY
   2A - The purpose and duration of the processing
   2B - Processing of personal health data
   2C – Types of data
   2D – Categories of data subjects

A. Purpose and duration of the processing[4]

Purpose

Before the processing of personal health data can commence, there must be one or more clearly defined purposes for the processing. This is one of the fundamental data protection principles in the General Data Protection Regulation.

A purpose is a clear and established description of what the personal data will be used for. The defined purpose determines what the data can be used for, and the establishment cannot subsequently use the data for other purposes. An example of the purpose in the health and care services sector could be health personnel’s duty relating to documentation.

It is not sufficiently clear to state that the purpose is, for example, *"administration of employee data".* It must be specified as to what the data will be used for, for example, "*registration of working hours and processing of applications for absence*".

Duration

The duration of the processing must be specified as accurately as possible. If, for example, the processing relates to a time-limited project, the start and completion date of the project can be specified. In other instances, it will not be possible to state the duration of the processing as accurately, and this will have to be linked to other assessments of when the purpose of the processing has been achieved.

Examples:

[4] For more guidance regarding the establishment of purpose, see the Norwegian Data Protection Authority's website.

Name of service	Purpose of the processing	Duration of the processing
Cloud storage service	*Storage of database/registry*	*Until the purpose has been achieved*
Helseinformasjon.no	*Collect, store and forward data to enable the user (researcher) to search for personal health data for secondary use.*	*Essentially for as long as the user profile exists. Further details will be provided in subsequent instructions.*
Overview of applications	*The purpose of the Overview of Applications is to have a visual presentation and a continuous overview of all applications that have been received by the application reception centre.*	*From the start of the application reception centre on date XX until and including date XX.*
Application and case processing service	*Provide guidance to applicants regarding the application process, data sources and analysis services.* *Assist the Controller in processing applications for access to personal health data, including ensuring equal treatment and fulfilment of the Controller's duty to investigate and provide information.* *Assist the Controller in ensuring that applications for access to personal health data are adequately disclosed.* *Coordinate the application process between different registries and other public stakeholders.* *Facilitate the applicant's access to the proceedings.* *Communication with the applicant during the entire process.* *Facilitate archiving.*	*Starts upon initial contact with the user/applicant.* *Stored for as long as this is relevant for processing the application or fulfilling other purposes of the processing.* *Archiving takes place in accordance with applicable regulations.*

B. Processing of personal health data

The general type of processing of personal health data must be specified under “Processing”. All processing should be described in more detail, including associated processing activities. Examples of processing are provided in the table below. Other types of processing are inserted as required.

The processing must be described in more detail under "Processing activities". There should be a brief description of how the processing is specifically carried out. For example: If “collection” is a form of processing that is carried out, a description must be provided of how such collection takes place, including which technical solution is used and from whom the data are collected. This data can, for example, be collected by the data subject entering the data in a portal, or by the data being collected automatically from a database.

In the table below, the service "Application and case processing service" (see table above) is used as a general example where relevant. The purpose of the general example is to demonstrate the appropriate level of detail for the various activities.

Examples:

Processing	**Processing activities**
Collection	*The data are collected by the data subject entering data in an application portal.*
Registration	
Organisation	
Structuring	*The application service structures the application information in order for it to be legible and accessible to the controller.*
Storage	*The processor stores the application information until the purpose is achieved. The controller provides instructions regarding when the data shall no longer be stored.*
Adaptation or alteration	
Retrieval	
Collation	
Erasure or destruction	*The Processor shall erase the application information when the Controller gives instructions to this effect/The Processor shall erase the application information on date XX, in accordance with instructions from the Controller.* *The Processor shall ensure that erasure takes place if the data subject withdraws his/her consent to the processing of personal data or requests erasure.*
Disclosure	*The Processor shall disclose data to the data subject if the data subject requests access to his/her own personal data. The data shall be made available to the data subject in an easily accessible format.*

C. Types of data

Type of personal data refers to the specific data that will be processed.

Examples:

Personal data	Special categories of personal data: health data
Name	*Medicine use*
Telephone number	*Diagnostic data*
National Identity Number	*Data from personal health data filing systems*
Place of residence	*Identifying audio or video recordings*
Customer number	*Written communication between the health service and patient*
Log information	
Work experience	

D. Categories of data subjects

Here a description must be provided of who the processing of personal health data pertains to. If data are processed about particularly vulnerable or exposed groups, this should be stated separately.

Examples:

Categories of data subjects
Patients
Children
Parents
Applicants for ...
Users of ...
Health personnel
Staff at ...
Employees at ...
Suppliers to ...

3.2 Appendix 2 – Detailed requirements concerning information security

In this appendix, the information security requirements that apply to the processor assignment must be described in more detail. To begin with, the controller should describe the requirements that are set for the processor. A more detailed description should then be provided of how the processor will fulfil the obligations in clause 8.2 of the agreement “The Processor’s obligations”.

A number of examples of requirements are listed in the table below. Not all requirements will be applicable for all agreements, and are intended to serve as examples of requirements and how precisely the requirements should be specified. For example, the requirements may obligate the processor to comply with certain standards, or impose a specific method of encryption.

In some instances, information security requirements will be specified in the Service/assignment agreement. If the controller considers these requirements to be sufficient for the specific processor assignment, it will not be necessary to describe the requirements once more in this appendix. Reference should then be made to where information security is regulated in the Service/assignment agreement.

Note that the Data Processing Agreement with appendices takes precedence over the Service/assignment agreement in the event of a conflict. This means that if a matter is regulated differently in the Data Processing Agreement and in the Service/assignment agreement, it is the content of the Data Processing Agreement that is used as a basis. For example, if different storage periods for personal data are defined in the two agreements, the storage period specified in the Data Processing Agreement will apply.

Examples:

No.	Topic	Requirement
	Code of conduct for information security and data protection in the healthcare and care services sector	*The Processor shall fulfil all relevant requirements in the Code of conduct for information security (see fact sheet 10, and the requirements that are stipulated for the Processor).*
	ISMS/Management System	*The Processor shall have an information security management system which ensures that the Processor implements and follows up information security at the establishment in a systematic and documented manner in accordance with relevant requirements and within an acceptable level of risk. The management system must be based on recognised standards.*
	Security audits[5]	*The Processor shall conduct regular internal audits of information security. The documentation shall be available to the Controller.* *The Controller has the right to carry out security audits at the Processor, including by using third parties. Notice of audits must be provided at least 14 days in advance.* *The right to audit includes testing of technical, organisational and physical security measures.*

[5] See also the remarks to section 2.12

	Protection of data	*The Processor shall have mechanisms in place for data during transport, processing and storage to safeguard integrity and confidentiality.*
	Remote access	*The requirements in the Code of Conduct's guide to remote access must be followed.*
	Access control	*In principle, the Processor shall not have access to the content of the Controller's data, unless this is necessary to comply with obligations the Processor may have pursuant to this agreement. In such instances, only personnel at the Processor who have an official need shall have access. Access must be logged and the grounds for access cited.* *For users with privileged access, irrespective of whether this provides direct access to the Controller’s data, each user shall be personal, strictly limited and controlled, and have the associated, necessary security measures.*
	Authentication	*In connection with access to data for professional purposes, personal user names with a password shall be used. The Processor shall have an established password policy.* *The Controller may use instructions that set specific requirements for authentication, for example, that strong authentication must be used.*
	Measures to combat cyberattacks	*The Processor shall implement measures to combat cyberattacks, for example, denial-of-service attacks and malicious code.*
	Logging and traceability	*The Processor shall implement logging that shows access to the Controller's data and the operations that the Processor has performed on the data.* The logs must be protected against unauthorised access, alteration and deletion. *The storage period shall be determined based on the purpose of the logging and clarified with the Controller.*
	Redundancy and scaling	*The Processor shall have an infrastructure that ensures capacity and uptime in line with the agreed service level through measures such as redundancy and scaling.*
	Test data	*The Controller's data must not be used for testing purposes without a prior written agreement with the Controller. Any anonymisation must take place at the instructions of the Controller. In instances in which the Controller's data are used for testing in accordance with an agreement, this data shall be protected in the same manner as production data.* *When production data are used for testing purposes, these must be deleted after the test has been performed.*
	Erasure and return	*The Processor shall have routines and technical solutions which ensure that all of the Controller's data are erased or returned at*

		the instruction of the Controller, or upon termination of the Data Processing Agreement. This also includes data stored on backup media and logs.
	Storage period	*The storage of data shall be determined by the Controller based on the purpose of the processing. When the purpose of the processing has been achieved, the data shall be erased in accordance with the clause pertaining to erasure and return in this appendix.*
	Back-up and restore	*The Processor shall have adequate back-up and restore routines that are regularly tested.*
	Encryption upon storage	*Data shall be encrypted upon storage if the Controller sets requirements for this.*
	Encryption in communication	*Data must always be encrypted in communication in accordance with Norwegian National Security Authority (NSM) specifications.*
	Access control	*The Processor must have adequate physical security at the location(s) where the Controller's data are accessible.*
	Security architecture	*The Processor must separate data belonging to different customers. The Processor's own data must be separated from the customers' data. The Processor shall have routines which ensure that the Controller's data are not transferred to other establishments without this being agreed to in writing with the Controller.*
	Authorisation log	*The Processor shall have an updated authorisation log at all times for personnel who are authorised to access the Controller's information and services.*

3.3 Appendix 3 – Administrative provisions

In this appendix, each of the parties shall specify their contact persons.

Each party should specify the name and contact details of a primary contact for the Data Processing Agreement.

If appropriate, multiple contact persons who are responsible for various matters may be specified - for example, who should receive notices of non-conformities and who should be informed of any plans to use other subcontractors or replace subcontractors.

If other administrative matters are agreed to, for example, regular meetings, reporting, transmission formats, etc., such information must also be inserted in this appendix.

The same applies if more detailed auditing routines are agreed to, cf. clause 12 of the agreement. The alternatives below are examples that can be used in their present form, individually or collectively, depending on requirements. They can also be used as a starting point for specific adaptations.

Examples of auditing routines:

In order to verify compliance with applicable data protection rules and the Data Processing Agreement, the following auditing routines have been agreed (several possible choices):

Example 1

> *The Controller has the right to perform audits at the Processor's place of business to verify the Processor's compliance with its obligations under this Data Processing Agreement or applicable data protection rules.*
>
> *Such audits shall:*
>
> - *Be performed following reasonable advance notice and maximum once a year, unless security breaches at the Processor or other special circumstances provide grounds for more frequent audits.*
> - *Take place within normal working hours and not unnecessarily disturb the Processor's activities.*
> - *Be performed by employees of the Controller or by third parties approved by the Parties and subject to an obligation of secrecy.*
>
> *The Processor is obligated to make available the resources that may reasonably be required to perform the audit.*

Example 2

> *The Processor shall use an external auditor to certify that security measures have been established and are functioning as intended. This audit shall:*
>
> - *be performed once a year,*
> - *be performed in accordance with recognized certification standards, for example, ISAE 3402.*
> - *be performed by an independent third party with sufficient knowledge and experience.*
>
> *The reports shall be submitted to the Controller upon request.*
> *In addition, the Processor shall provide the information and assistance that may be necessary for the Controller to comply with its obligations pursuant to applicable data protection regulations.*

Example 3

> *For standardised third-party services provided by the Subcontractor, a third-party audit may be submitted, provided that the audit has been performed in accordance with generally recognised principles and by a certified public accountant.*

3.4 Appendix 4 – Subcontractors

It must be specified in the table as to what subcontractors the Processor uses on the date the agreement is entered into. If the Processor wishes to use multiple subcontractors or change a subcontractor, the Controller must be notified and given the opportunity to oppose the change. If the Controller accepts the change, either explicitly or by remaining passive, this appendix must be updated and sent to the Controller's contact person (who must be specified in Appendix 3 - Administrative Provisions).

The subcontractor's name, organisation number or other identifier and address must be specified in the table, as well as the service (overall description of the processing) the subcontractor performs on behalf of the Processor. The location at which the personal health data are processed must also be specified. This also includes locations that the subcontractor has access to or otherwise processes personal data from (remote access). It is particularly important to specify the place of processing, because it may concern the Controller's obligation to have valid grounds for transfer to countries outside the EU/EEA.

Further details regarding the requirements that apply for transfers to other countries is provided in section 2.10.

The tables are updated in the event of changes and sent to the Controller's contact person.

Examples:

Name	Organisation no.	Address	Service type (processing)	Place of processing
[Name]	*[Organisation no.]*	*[Address]*	*Data centre, hosting*	*Stockholm, Sweden*
[Name]	*[Organisation no.]*	*[Address]*	*IT support services*	*Oslo, Norway* *Chennai, India* *Kiev, Ukraine*
[Name]	*[Organisation no.]*	*[Address]*	*Back-up*	*Paris, France*

3.5 Appendix 5 - Amendments to the general text of the agreement upon entering into the agreement

The amendments to the text of the agreement or supplements thereto must be stated here, such that the general text of the agreement remains unchanged in the document. It must be clearly and unequivocally stated as to which provisions in the agreement have been amended and how the clause/paragraph/sentence will be worded following the amendment.

It is possible to make amendments to all clauses in the agreement, even where it is not clearly stated that amendments can be agreed. Amendments that are contrary to relevant legislation will not be valid. This is stipulated in clause 1 of the agreement.

Example of change table:

Clause in the agreement	Replaced with
Chapter x.x.x, paragraph y	*[Insert new wording/text]*

3.6 Appendix 6 – Amendments after the agreement has been entered into

This appendix must not be filled in when the agreement is entered into, however must be enclosed even if it is currently empty.

If the parties have reached an agreement on a change to the processing/assignment, the text of the agreement or other conditions, the change must be stated here. If the change applies to matters regulated in an appendix to the agreement, it may be appropriate to prepare an updated version of the appendix that includes the change.

Each change must be signed by an authorised representative of the parties.

The Processor is responsible for maintaining a continuous catalogue of the changes that make up Appendix 6. The Processor is also responsible for ensuring that the Controller is provided with an updated copy without undue delay.

Change table:

No.	Date	Change	Any appendices	Applies from

Direktoratet for e-helse