Data Processor Agreement

Standard contract conditions in reference to Article 28(3) in regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation) in preparation for the Data Processor's processing of personal data.

Between **the Data Controller:**

Name of organisation:

Address:

Postal code and city:

Country:

VAT number:

File number:

And **the Data Processor:**

MedCom

Forskerparken 10

5230 Odense M

Denmark

CVR number: 26919991

File number:

Each a "party" and together "the parties" have agreed on the following standard Contractual Clauses (Data Processor Agreement) in order to meet the requirements of the GDPR and to ensure privacy and the protection of peoples' fundamental rights and constitutional rights.

Indhold

1 Preamble

1. These Contractual Clauses (the Clauses) set out the Data Processer's rights and obligations, when processing personal data on behalf of the Data Controller.

2. The Clauses concerns the Data Controller's and the Data Processor's obligation to comply with Article 28(3) of Regulation 2016/679 of the European Union 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 and repealing Directive 95/46/EC (General Data Protection Regulation) as well as the Danish Act on supplementary provisions to the Regulation (the Data Protection Act).

3. Regarding the delivering of:

Connection to The Danish Health Data Network (SDN) cf. the SDN Connection Agreement.

4. The Data Processor shall process personal data in accordance with the rules and regulations for the processing of personal data in agreement to these Clauses.

5. The Clauses take precedence regarding pre-existing equivalent Clauses between the Parties.

6. There are four appendices associated to these Clauses and the appendices account for an incorporated part of the Clauses.

7. Appendix A contains further information on the processing of personal data, including the objective and character of the processing, type of personal data, category of the registered, and duration of the processing.

8. Appendix B contains the Data Controller's conditions for the Data Processor's use of Sub-Processors and a list of Sub-Processors, which the Data Controller have approved.

9. Appendix C contains the Data Controller's instructions for the Data Processor's processing of personal data, a description of the security measures, which the Data Processer must fulfil as a minimum, how the Data Processor assists the Data Controller, including how to supervise the Data Processer and potential Sub-Processors.

10. Appendix D contains other activities, which are not included by the Clauses as well as agreed additions or deviations from the Clauses.

11. Both parties shall keep the Data Processor Agreement with the accompanying Appendices in writing, including as an electronic version.

12. These Clauses shall not exempt the Data Processor from the obligations to which the Data Processor is subject pursuant to the General Data Protection Regulation (GDPR) or any other law.

2 Rights and obligations of the Data Controller

1. The Data Controller is responsible for ensuring that the processing of personal data takes place in accordance with GDPR (see Article 24 of the Regulation), the applicable EU or Member State data protection provisions and the Clauses.

2. The Data Controller has the right and obligation to make decisions about the purpose(s) and by which means personal data may be processed.

3. The Data Controller is responsible, among other things, for ensuring that there is a legal basis for the processing of personal data that the Data Processor is instructed to perform.

3 The Data Processer acts according to instructions

1. The Data Processor may only process personal data based on documented instructions from the Data Controller, unless required by the Union or Member State law to which the Data Processor is subject. This instruction shall be specified in Appendix A and C. Subsequent instructions may also be given by the Data Controller during the processing of personal data, but the instruction must always be documented and stored in writing, including electronically, together with the Data Processor Agreement.

2. The Data Processor shall immediately inform the Data Controller if an instruction, in the Data Processor's opinion, violates the General Data Protection Regulation or the applicable EU or Member State data protection provisions.

3. The parties should anticipate and consider any consequences that may arise from a possible illegal instruction given by the Data Controller. If relevant, the parties shall regulate this issue according to Appendix D.

4 Confidentiality

1. The Data Processor may only grant access to personal data processed on behalf of the Data Controller to persons who are subject to the Data Processor's authority, who have committed themselves to confidentiality, or who are subject to an appropriate statutory duty of confidentiality, and only to the extent necessary. The list of persons who have been granted access must be regularly reviewed. Based on this review, access to personal data may be closed if access is no longer necessary, and the personal data shall no longer be available to these persons.

2. Upon request from the Data Controller, the Data Processor must be able to demonstrate that the persons subject to the Data Processor's authority are subject to the above-mentioned duty of confidentiality.

5 Security of processing

1. Article 32 of the General Data Protection Regulation stipulates that considering the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, appropriate technical and organisational measures must be implemented to ensure a level of security appropriate to the risks.
   The Data Controller shall evaluate the risks for natural persons' rights and freedoms and implement measures to address the identified risks. Depending on relevance, this may include the following measures:

    a. Pseudonymisation and encryption of personal data.
    b. Ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.
    c. Ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.
    d. Process for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. In addition, pursuant to Article 32 of the Regulation, the Data Processor must - independently of the Data Controller - assess the risks to the rights of natural persons posed by the processing and implement measures to mitigate those risks. To carry out this assessment, the Data Controller must provide the necessary information to the Data Processor to enable them to identify and evaluate such risks.

3. Furthermore, the Data Processor shall assist the Data Controller in fulfilling the Data Controller's obligations under Article 32 of the GDPR by providing the necessary information to the Data Controller regarding the technical and organisational security measures that the Processor has already implemented pursuant to Article 32 of the GDPR, as well as any other information necessary for the Data Controller to fulfill its obligations under Article 32 of the GDPR. If addressing the identified risks - as determined by the Data Controller - requires the implementation of

additional measures beyond the measures already implemented by the Processor, the Data Controller must specify the additional measures to be implemented in Appendix C.

6 The use of Sub-Processors

1. The Data Processor must fulfill the conditions specified in Article 28, paragraphs 2 and 4, of the General Data Protection Regulation in order to use another Data Processor (a Sub-Processor). Therefore, the Data Processor may not use a Sub-Processor to fulfil these Clauses without prior **specific** or **general written approval** from the Data Controller. The list of Sub-Processors that the Data Controller has already approved is listed in Appendix B.
2. The Data Processor must inform the Data Controller of any planned changes regarding additional or replacement of Sub-Processors. Changes must be reported to the Data Controller with appropriate notice.

PRECEDING SPECIFIC APPROVAL	N/A	N/A
PRECEDING GENERAL APPROVAL	YES	At least 3 months notice

3. When the Data Processor uses a Sub-Processor regarding specific processing activities on behalf of the Data Controller, the Data Processor must, through a contract or other legal document in accordance with EU or Member State law, impose on the Sub-Processor, the same data protection obligations as set out in the Clauses, in particular providing the necessary guarantees that the Sub-Processor will implement the technical and organisational measures in such a way that the processing meets the requirements of the Clauses and the General Data Protection Regulation. Therefore, the Data Processor is responsible for requiring that the Sub-Processor, at a minimum, complies with the Data Processor's obligations under the Clauses and the General Data Protection Regulation.

4. Sub-Processor agreement(s) and any subsequent amendments shall be provided, upon the Data Controller's request, to the Data Controller in a copy, allowing the data controller to ensure that equivalent data protection obligations, as set out in these Clauses, have been imposed on the Sub-

Processor. The Clauses concerning commercial terms that do not affect the data protection content of the Sub-Processor agreement shall not be provided to the Data Controller.

5. The Data Processor shall include the Data Controller as a third-party beneficiary in its agreement with the Sub-Processor in the event of the Data Processor's bankruptcy, enabling the Data Controller to enforce the Data Processor's rights against Sub-Processors, for example, by instructing the Sub-Processor to delete or return personal data.

6. If the Sub-Processor fails to fulfil its data protection obligations, the Data Processor remains fully liable to the Data Controller for the fulfilment of the Sub-Processor's obligations. This does not affect the rights of data subjects under the General Data Protection Regulation, in particular under Articles 79 and 82, towards the Data Controller and the Data Processor, including the Sub-Processor.

7 Transfer of data to third countries or international organisations

1. Any transfer of personal data to third countries or international organisations may only be conducted by the Data Processor based on documented instructions from the Data Controller and must always be in accordance with Chapter V of the General Data Protection Regulation.

2. If transfer of personal data to third countries or international organisations, which the Data Processor has not been instructed to conduct by the Data Controller, is required under EU or Member State law to which the Data Processor is subject, the Data Processor shall inform the Data Controller of this legal requirement prior to processing, unless that law prohibits such notification in the interest of important societal interests.

3. Without documented instruction from the Data Controller, the Data Processor cannot, within the framework of these Clauses:
    a. Transfer personal data to a Data Controller or Data Processor in a third country or an international organisation.
    b. Entrust the processing of personal data to a Sub-Processor in a third country.
    c. Process the personal data in a third country.

4. The Data Controller's instructions regarding the transfer of personal data to a third country, including the possible transfer basis in Chapter V of the General Data Protection Regulation, on which the transfer is based, shall be specified in Appendix C.6.

5. These Clauses should not be confused with standard contractual clauses referred to in Article 46(2)(c) and (d) of the General Data Protection Regulation, and this Clauses cannot serve as a basis for the transfer of personal data as referred to in Chapter V of the General Data Protection Regulation.

8 Assistance to the Data Controller

1. The Data Processor shall, considering the nature of the processing, assist the Data Controller, as far as possible, by appropriate technical and organisational measures in fulfilling the Data Controller's obligation to respond to requests for the execution of the data subjects' rights as laid down in Chapter III of the General Data Protection Regulation.
   This means that the Data Processor shall, as far as possible, assist the Data Controller in ensuring compliance with:

   a. the obligation to provide information when collecting personal data from the data subject
   b. the obligation to provide information if personal data is not collected from the data subject
   c. the data subject's right of access
   d. the right to rectification
   e. the right to erasure ("right to be forgotten")
   f. the right to restriction of processing
   g. the obligation to notify in connection with rectification or erasure of personal data or restriction of processing
   h. the right to data portability
   i. the right to object
   j. the right not to be subject to a decision based solely on automated processing, including profiling

2. The Data Processor assists the Data Controller in ensuring compliance with the Data Controller's obligations under Articles 32-36 of the General Data Protection Regulation, considering the nature of the processing and the information available to the Data Processor, pursuant to Article 28(3)(f). This means that, considering the nature of the processing, the Data Processor shall assist the Data Controller in ensuring compliance with:

    a. the obligation to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks presented by the processing;
    b. the obligation to notify personal data breaches to the supervisory authority (The Danish Data Protection Agency) without undue delay and, where feasible, not later than 72 hours after the Data Controller becomes aware of the breach, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons;
    c. the obligation to communicate to the data subjects the personal data breach, without undue delay, when the breach is likely to result in a high risk to the rights and freedoms of natural persons;
    d. the obligation to carry out a data protection impact assessment if a type of data processing is likely to result in a high risk to the rights and freedoms of natural persons;
    e. the obligation to consult the supervisory authority (The Danish Data Protection Agency) prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the Data Controller to mitigate the risk.

3. Any regulation/agreement between the Parties regarding compensation or similar in connection with the Data Processor's assistance to the Data Controller will appear in the Parties' Main Agreement or in Appendix D to this agreement.

9 Notification of Personal Data Breach

1. The Data Processor shall promptly notify the Data Controller upon becoming aware of a personal data breach.
2. The Data Processor's notification to the Data Controller shall be made without undue delay after becoming aware of the breach, allowing the Data Controller to comply with its obligation to notify

the competent supervisory authority of the breach of personal data security, pursuant to Article 33 of the General Data Protection Regulation. The deadline for notifying the Data Controller is specified in Appendix C.

3. In accordance with Clause 9.2, the Data Processor shall assist the Data Controller in reporting the breach to the competent supervisory authority. This means that the Data Processor shall assist in providing the following information, which, according to Article 33(3) of the General Data Protection Regulation, shall be included in the Data Controller's notification of the breach to the competent supervisory authority:
    a. the nature of the personal data breach, including, where possible, the categories and approximate number of data subjects concerned and approximate number of personal data records concerned;
    b. the likely consequences of the personal data breach;
    c. the measures taken or proposed to be taken by the Data Controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. The parties shall specify in Appendix C the information that the Data Processor shall provide in connection with its assistance to the Data Controller in its obligation to notify breaches of personal data security to the competent supervisory authority.

10 Deletion and Return of Personal Data

1. Upon termination of the services related to the processing of personal data, the Data Processor is obliged to either delete all personal data that has been processed on behalf of the Data Controller or return all personal data and delete existing copies. If no data storage is done by the Data Processor, this is not relevant.

Delete all personal data.

2. Any rules in EU or Member State law that prescribe the storing of personal data after termination of the services related to the processing of personal data shall be specified in Appendix D. The Data Processor undertakes to process the personal data solely for the purpose(s), within the period and under the conditions prescribed by such rules.

11 Inspection and Audit

1. The Data Processor shall provide all information necessary to demonstrate compliance with Article 28 of the General Data Protection Regulation and these Clauses to the Data Controller, and shall allow and contribute to audits, including inspections, carried out by the Data Controller or another auditor mandated by the Data Controller.

2. The procedures for the Data Controller's audits, including inspections, with the Data Processor and Sub-Processors are further specified in Appendix C.7.

3. The Data Processor is obliged to grant supervisory authorities, which under applicable law have access to the Data Controller's or the Data Processor 's facilities, or representatives acting on behalf of the supervisory authority, access to the Data Processor physical facilities upon proper identification.

12 The Parties Agreement on Other Conditions

1. The parties may agree on other clauses to the service related to the processing of personal data, such as liability, if these other clauses do not directly or indirectly conflict with these Clauses or undermine the fundamental rights and freedoms of the data subjects under the General Data Protection Regulation.

13 Commencement and Termination

1. The Clauses becomes effective on the date of signature by both parties.

2. Both parties may request that the Clauses be renegotiated if changes in the law or if significant shortcomings in the Clauses give cause for it. The procedure for renegotiation is described in Appendix D, including any agreements regarding the time period between renegotiations.

3. The Clauses shall apply for the duration of the provision of personal data processing services. During this period, the Data Processor Agreement cannot be terminated unless other Clauses governing the Data Processor Agreement of the service related to the processing of personal data are agreed upon between the parties.

4. If the delivery of the services regarding the processing of personal data ceases, and the personal data has been deleted or returned to the Data Controller in accordance with Clause 10.1 and Appendix C.4, the Clauses may be terminated with written notice by both parties.

14 Data Controller and Data Processor contacts/contact points regarding the Data Processing Agreement

1. The Parties must contact each other via the information listed below.

2. The Parties are obligated to continuously inform each other about changes regarding the contact information.

The Data Controller:		The Data Processor:	MedCom
Name:		Name:	Peder Illum
Position:		Position:	Head of Security
Telephone number:		Telephone number:	(+45) 29263654
E-mail:		E-mail:	pi@medcom.dk
Department:		Department:	System Management
Possible functional mailbox:		Possible functional mailbox:	sdn@medcom.dk

15 Signature

On behalf of the Data Controller:		On behalf of the Data Processor:	
Name:		Name:	Lars Hulbæk
Position:		Position:	CEO
Date:		Date:	
Signature:		Signature:	

Appendix A: Information on processing

NOTE: IN CASE OF MULTIPLE PROCESSING ACTIVITIES, THESE DETAILS MUST BE PROVIDED FOR EACH INDIVIDUAL PROCESSING ACTIVITY.

A1. The purpose of the Data Processor's processing of personal data on behalf of the Data Controller is:

The processing consists of transporting personal data between and on behalf of both public and private parties in the Danish healthcare sector.

The transportation occurs in the Danish Health Data Network (SDN), a closed, encrypted, and virtual network that includes network infrastructure and several supporting systems.

Instructions for transporting personal data in SDN are governed by agreements in the supporting system, the SDN's Agreement System, in which the Data Controllers themselves manage and administer services, clients, users, and transport agreements.

The Data Processor is the contract holder and joint public system manager of SDN.

A2. The Data Processor's processing of personal data on behalf of the Data Controller pertains to (the nature of the processing):

The Data Processor hosts, operates, maintains, monitors, and supports SDN through Sub-processors.

The Data Processor transports personal data based on the instructions of the Data Controller. Configuration of the transport of personal data in SDN is done automatically in accordance with the segmentation resulting from agreements made in the Agreement System.

The Data Processor processes personal data of users in the Agreement System to enable user registration and access to the Agreement System, where the Data Controllers themselves manage and administer the creation, deletion, maintenance, and documentation of services, clients, and agreements for access to exposed services in SDN.

The Data Processor processes personal data of users in the Agreement System to support security logging.
The Data Processor processes personal data of users in the Agreement System to send service notifications about the operation and maintenance of SDN.

The Data Processor receives alerts about anomalies in the monitoring of SDN. The Data Processor performs deletion in collaboration with Sub-processors when a connection to SDN is terminated. The Data Processor assists Sub-processors in resolving support inquiries related to SDN. As a joint public system manager, the Data Processor manages suppliers in connection with the delivery of SDN to the Data Controller.

A3. The processing includes the following types of personal data about the registered data subjects:

In SDN, non-sensitive, confidential and sensitive personal data, including health information, are processed. In the Agreement System, non-sensitive personal data such as name, organisational affiliation, mobile phone number, work email, and logging of actions in the Agreement System are processed.

A4. The processing includes the following categories of the registered data subjects:

In SDN, the following categories of data subjects are processed: Patients, citizens, and healthcare personnel. In the Agreement System, the following categories of data subjects are processed: Users in the Agreement System, i.e., technical and administrative personnel of the Data Controller.

A5. The processing of personal data by the Data Processor on behalf of the Data Controller may commence upon the entry into force of this agreement. The duration of the processing follows:

The duration of the processing shall be in accordance with the concluded Connection Agreement for SDN.

Appendix B: The Sub-Processors

Upon the entry into force on commencement of the Clauses, the Data Controller has approved the use of the below-mentioned Sub-Data Processors for the described processing activity. The Data Processor may not, without the written approval of the Data Controller, use a Sub-Processor for a different processing activity than the one described and agreed upon, or use a different Sub-Processor for this processing activity.

One appendix is completed per Sub-Processor. If there are more than one Sub-Processor, use the template for Appendix B, which is included with the Data Processor Agreement template.

Company name	Nuuday – TDC Erhverv
CVR number (or other equivalent company registration number)	40075291
Company address	Teglholmsgade 1, 2450 København SV, Denmark
Other addresses where personal data is processed (if relevant)	The exact addresses are confidential for security reasons but can be provided upon request. MedCom can be contacted for further information at sdn@medcom.dk
Contact information of the Sub-Processor	dpo@nuuday.dk
Does the Data Processor have an agreement with the Sub-Processor that meets the requirements of the Clauses?	Yes
The processing(s) the Sub-Processor is a part of	The Data Processor's task is to host, operate, maintain, monitor, manage, and support the SDN.

Categories of personal information which the Sub-Processor process	Same as described in A3.
Location of the data processing	Data is processed on dedicated servers located within the EU/EEA. The exact addresses are confidential for security reasons but can be provided upon request. MedCom can be contacted for further information at sdn@medcom.dk.
Transferring of personal data to third country (if relevant)	
Does the Sub-Processor process personal data in a third country?	SDN can establish connections with foreign parties, including in unsecure third countries. Foreign parties must first be approved by MedCom's steering group before establishing a connection. The transfer of personal data to a foreign party requires an agreement/instruction from the Data Controller. It is the responsibility of the Data Controller to ensure that there is a legal basis for the transfer of personal data to unsecure third countries.
If yes, state all the third countries	N/A
If yes, please indicate the legal basis for the transfer (e.g., EU standard contractual clauses or Binding Corporate Rules)	N/A

If yes, please specify any additional organisational or technical security measures (including encryption and storage of encryption keys)	N/A

The Data Processor will provide agreements with Sub-processor(s) and any additional relevant documentation, such as documentation of pre-audit in accordance with Article 28(1), upon request from the Data Controller.

Appendix C Instructions on processing of personal data

If it is agreed between the parties that one or more of the listed security requirements should not be complied with or should be complied with in a different manner than described in the Data Processor's instructions, this will be inserted in appendix D of this agreement.

C.1 The subject of/instruction for the processing

The Data Processor's processing of personal data on behalf of the Data Controller is done by the Data Processor performing the following:

Identify the data processing activities performed by the Data Processor and describe them as specifically as possible:

Data processing	**Preformed by**	**Description of the data processing**
Data collection		
Registration		
Organisation/systematisation		
Storage	X	Hosting, operation, maintenance, and backup.
Modifications	X	Adjustment or modification of personal information in the Agreement System at the request of the Data Controller.
Recovery		
Search		
Use	X	The non-sensitive personal information in the Agreement System is used for support and sending service messages about the operation of SDN.
Disclosure through transmission	X	Hosting, operation, maintenance
Provision or any other form of hand-over		
Combining or matching		

Limitations		
Deletion or termination	X	When the Connection Agreement for SDN expires, the personal data in the Agreement System will be deleted.
Supplier management	X	As joint public-sector systems manager, the Data Processor manages the supplier in connection with the delivery of SDN to the Data Controller.
Support	X	The general personal information in the Agreement System is used for support.

C.2 Security of processing

C.2.1 Determination of level of security

C.2.1.1 The security level must reflect the category and quantity of personal data involved in the processing:

The security level must reflect that sensitive and confidential personal data is processed in SDN.

C.2.1.2 The Data Processor must have appropriate technical measures to limit the risk of any unauthorised access. The Data Processor must evaluate and improve the effectiveness of such measures when necessary.

C.2.1.3 The Data Processor must support the Data Controller in documenting the identified risks and how the risk has been reduced to an acceptable level and implementing the measures necessary to address identified risks.

This may include, among other things, the following measures, depending on what is relevant:

i. Pseudonymization and encryption of personal data.
ii. Ability to ensure ongoing confidentiality, integrity, availability, and resilience of processing systems and services.
iii. Ability to timely restore availability and access to personal data in the event of a physical or technical incident.
iv. A procedure for regularly testing, assessing, and evaluating the effectiveness of the technical and organisational measures to ensure processing security.

C.2.1.4 The processing of data covered by the Clauses shall be carried out in accordance with this instruction.

C.2.1.5 This instruction reflects what is applicable at the time of the signing of the Clauses. If there are changes in the conditions, including those filled out by the Data Processor, the Data Controller must be informed.

C.2.1.6 This instruction is a description of the technical and organisational security measures that the Data Processor is responsible for implementing, complying with, and ensuring compliance with by the Data Processor and its Sub-Processors. Any agreements between the Data Controller and the Data Processor regarding deviation or partial deviation from one or more of the requirements below are documented in Appendix D.

C.2.1.7 If more extensive technical and organisational security measures are necessary to ensure compliance with Chapter 5 of the Clauses, such measures must always be taken. Additional security measures are specified in Appendix D.

C.2.1.8 The Data Processor implements the following technical and organisational security measures to ensure a level of security that is appropriate to the agreed-upon processing and, thus, complies with Article 32 of the General Data Protection Regulation. The measures are determined based on considerations of:

i. What is technically feasible
ii. Implementation costs
iii. The nature, scope, context, and purpose of the processing
iv. The consequences for the data subjects' rights in case of a security breach
v. The risks associated with the processing, as outlined in section C.2.1.3

C.2.2 Pseudonymization and encryption

C.2.2.1 External communication connections may only be established if the connection is encrypted, for example, to a website, front-end, or login portal. This also applies to connections to sub-contractors, such as site-to-site connections or IP filtering.

For confidential and sensitive personal data, strong encryption is expected. HTTPS and the latest version of TLS are required. Compliance with this requirement should be described, for example, in section C.2.2.4 below.

C.2.2.2 Emails containing confidential and sensitive personal information must also be protected by encryption.

C.2.2.4 If there are requirements from the Data Controller for encryption of data at rest, this should be described in Appendix D.

Encryption of transport in SDN is done with at least TLS 1.3.

Encryption of the connection to the Agreement System is done with at least TLS 1.3. The Agreement System is only accessible via SDN.

C.2.3 Training and instructions

C.2.3.1 All employees of the Data Processor must receive sufficient training and instructions to ensure that personal data is processed in accordance with relevant legislation as well as the policies and procedures of the Data Processor and the Data Controller.

C.2.4 Authentication and access control, incl. monitoring of rejected access attempts

C.2.4.1 Access to personal data should be managed and controlled.

C.2.4.2 Only persons employed for the specific purposes for which personal data is processed may be authorised. Individual users must not be authorised for purposes they do not require.

C.2.4.3 Access to systems and personal data processed in accordance with the Data Processing Agreement is limited by defining user roles, where possible, and assigning privileged access rights, as well as performing user certification.

The Data Processor must take measures to ensure that only authorised users can access personal data that they are authorised to access.

C.2.4.4 There must be an overview/documentation of each employee's rights to the individual systems and personal data processed under the Clauses.

C.2.4.5 Strong passwords and authentication must be used when accessing systems or personal data processed under the Clauses. Multifactor authentication is required when accessing from the open internet, or equivalent security measures must be taken.

C.2.4.6 The Data Processor must have formal procedures for handling password resets and other situations where normal logical access control is suspended.

C.2.4.7 There must be ongoing monitoring to ensure that users are assigned the access and authorisations that they should have. This monitoring may involve the systems creating a statistic for each user's use of the system, to determine if issued access and authorisations are still being used. The frequency of monitoring must be determined based on risk assessment and described in point C.2.4.13.

C.2.4.8 The data processor must promptly withdraw authorisations and access for users who, after an individual assessment, should no longer have them.

C.2.4.9 All rejected access attempts must be registered when handling confidential and/or sensitive personal data. The Data Processor must continuously follow up on rejected access attempts.

C.2.4.10 If a risk assessment deems it necessary, requirements for blocking login attempts from the same workstation or with the same user identification after a certain number of attempts can be determined - depending on the security level and other security measures. Any requirements for blocking should be described in section C.2.4.13.

C.2.4.11 When access is restored, documentation/a description of the reasons for the restoration must be available, and if access attempts have been blocked, notification to the Data Controller should be sent.

C.2.4.12 Authorised persons must be able to present a photo ID during on-site data processing at the Data Controller's premises.

C.2.4.13 The Data Processor's description of its compliance with the requirements in section C2.4, if relevant to the processing of personal data in accordance with the Data Processing Agreement:

The Data Controller is responsible for authorisation, creation, allocation of rights and access control for its own employees to the Agreement System. The Agreement System provides information for the Data Controller to monitor rights and usage of the Agreement System. The Data Processor and Sub-Processor are each responsible for authorisation, creation, allocation of rights and access control for their own employees to the SDN and the Agreement System. The authorised users of the Sub-Processor are reviewed in joint operational meetings. The Data Processor and Sub-Processor attest their employees' access every six months. Monitoring and control are carried out on rejected access attempts. Access is blocked after 5 failed login attempts. Access is granted through multi-factor authentication.

C.2.5 Restoration of availability in case of physical or technical incidents (backup and management of operational disruptions)

C.2.5.1 The same guidelines apply for backup as for all other processing of personal data under the Clauses.

C.2.5.1 The Data Processor must ensure that systems and personal data processed under the Clauses are regularly backed up.

C.2.5.3 Backup should be stored separately from the server in a non-adjoining room to ensure that it is not lost. Backup must be protected, and the storage of backup must always be done securely to avoid loss.

C.2.5.4 The Data Processor must regularly verify that the backup is readable. This should be done from a contingency perspective, for example, in the case of significant changes to a system's technical setup.

C.2.5.5 The Data Processor must have documented IT contingency procedures that ensure the restoration of services within a reasonable time in the event of a disruption.

C.2.5.6 The Data Processor must regularly test and evaluate the effectiveness of the technical and organisational measures to ensure processing security by conducting IT contingency exercises. The Data Controller may request documentation of this.

C.2.5.7 The Data Processor's description of its compliance with the requirements in section C2.5, if relevant to the processing of personal data in accordance with the Data Processing Agreement:

Personal data transported through SDN is not stored. However, backups of the Agreement System are taken and stored at a different geographic location. The exact address is confidential for security reasons, but it can be provided upon request to sdn@medcom.dk.

C.2.6 Updates and chances

C.2.6.1 The Data Processor must have formal procedures to ensure that updates to operating systems, databases, applications, and other software are assessed and implemented within a reasonable time frame.

C.2.6.2 The Data Processor must have formal procedures for managing changes to ensure that any changes are duly authorised, tested, and approved before implementation. The procedure must be supported by effective functional separation or management oversight to ensure that no individual can implement a change alone.

C.2.7 Physical security

C.2.7.1 The Data Processor shall make sure that IT equipment used for processing data is physically secure according to current legal requirement.

C.2.7.2 The Data Processor must have appropriate technical measures to limit the risk of any unauthorized access. The data processor must also evaluate and improve the effectiveness of such measures where necessary.

C.2.7.3 Mobile storage devices containing personal data must be labelled and stored with sufficient strong encryption under supervision or locked away when not in use.

C.2.7.4 Mobile storage devices containing personal data may only be provided to authorized persons for auditing or operational and technical tasks.

C.2.7.5 A record must be kept of which mobile storage devices are used with the data processing.

C.2.7.6 Written instructions for the use and storage of mobile storage devices must be prepared.

C.2.7.7 In connection with repair and service of data equipment containing personal data, as well as the sale and disposal of used data media, necessary measures must be taken to ensure that the personal data is not accidentally or deliberately destroyed, lost, or deteriorated, or that the personal data becomes known to unauthorized parties, is misused, or otherwise processed in violation of current law. This must be done according to best practice.

C.2.7.8 When disposing of equipment and storage media containing personal data, the storage media must be destroyed or demagnetized to ensure effective deletion of the personal data. Documentation that the disposal has been carried out in accordance with the above must be kept for the duration of the data processing and presented when requested by the Data Controller.

C.2.8 Use of home/ad hoc workstations

C.2.8.1 If the Data Processor is not allowed to use ad hoc workstations in connection with the data processing, this should be agreed between the parties and specified in Appendix D.

C.2.8.2 When using home/ad hoc workstations, multi-factor authentication or an equivalent security level must be used, and consideration must be given to time-out settings.

C.2.8.3 The Data Processor and its authorized employees may perform data processing from mobile workstations, including accessing the Data Controller's personal data over the internet, provided that the data processing is carried out from workstations subject to the Data Processor's own security rules. Furthermore, data processing must be carried out in accordance with the Clauses and this instruction.

C.2.8.4 The home/ad hoc workstations must be secured with technical controls that ensure the processing of personal data is in accordance with applicable laws and the instructions of the Data Controller and Data Processor.

C.2.8.5 Access to personal data processed at home workstations must be restricted to prevent unauthorized access. Employees must be instructed on how to prevent unauthorized access.

C.2.8.6 The data processor's description of its compliance with section C2.8, if relevant to the processing of personal data covered by the Clauses:

Remote access to SDN is done via a VPN access encrypted with a minimum of AES256-bit encryption and multifactor authentication.

Inactive user sessions in the Agreement System are closed after 15 minutes.

C.2.9 Logging

C.2.9.1 As a general rule, machine registration (logging) must be carried out when processing personal data. Requirements for logging and the content of the log are determined based on the risk assessment and any legal requirements, and the scope of the agreed logging is described in C.2.9.3.

C.2.9.2 The log must be stored for the period agreed between the Data Controller and the Data Processor, considering any legal requirements. The agreement on the storage period and disclosure of log information to the Data Controller is described in section C2.9.3.

C.2.9.3 The Data Processor's description of their compliance with section C2.9, if relevant to the processing of personal data covered by the Data Processing Agreement:

User actions in the Agreement System are documented in an event log, which is deleted after 2 years. The log is accessible to the Data Controller for follow-up on their own authorized employees' actions in accordance with their own policies.

The Data Processor has established logging on all active network equipment in the SDN through Sub-Processors. The logging includes a log of the use of privileged accounts on active network equipment, including name, start and end time, and the purpose of using the privileged account.

The Sub-Processor monitors and responds to unauthorized requests in the log, as well as monitors the log to identify any misuse of the SDN.

The Sub-Processor stores the transaction log on the Sub-Processor's access to the SDN for 2 years.

Operational logs without personal data are stored for 5 years for use in follow-up/investigation of any illegal or criminal activities.

All logs are protected against unauthorized access, manipulation, and technical errors.

C.2.10 Supervision

C.2.10.1 The Data Processor shall conduct and document oversight of the Data Processor's organisation's compliance with legal requirements, policies, procedures, and this Data Processing Agreement with attachments.

C.2.11 Notification

C.2.11.1 In case of a breach of personal data security, the Data Controller must be notified in writing without unnecessary delay at the address below, so that the Data Controller can report the breach to the Danish Data Protection Agency and, if necessary, notify the data subjects. The notification must be sent to:

Email address and, if applicable, phone number for contact at the Data Controller: Security contact person from the SDNv4 Connection Agreement. *Notification of the Data Controller must be provided within [specify time period*]: The Data Processor shall notify the Data Controller without undue delay after becoming aware of a personal data breach. The Data Processor's notification to the Data Controller shall be made without undue delay and in any event within 24 hours after becoming aware of the breach, so that the Data Controller can fulfil its obligation to notify the competent supervisory authority of the personal data breach in accordance with Article 33 of the GDPR.

C.3 Assistance to the Data Controller

To the extent possible, the Data Processor shall assist the Data Controller in accordance with the Clauses of Clauses 8.1 and 8.2 of the Data Processing Agreement by implementing the following technical and organisational measures:

The Data Processor maintains appropriate policies and procedures within its internal organisation that support the Data Processor's ability to comply with its obligations as a Data Processor, including the ability to assist the Data Controller in a manner that supports the Data Controller's compliance with the deadlines imposed by applicable data protection legislation.

C.4 Storage and deletion routine

The personal data transported in SDN is not stored. The Data Controller creates and deletes personal data in the Agreement System themselves. Personal data is stored for as long as necessary to fulfil the purpose of the data processing.

When the connection to SDN is terminated, the Data Processor deletes the personal data of the Data Controller in the Agreement System. The personal data will still appear in the log of events, which is deleted after 2 years. The log of events from the underlying network infrastructure in SDN, which only contains personal data about the Data Processor's and any Sub-Processor's employees, must be kept for 2 years for use in follow-up/investigation of any illegal or criminal activities.

In case of termination of the service related to the processing of personal data, the Data Processor shall either delete or return the personal data in accordance with Clause 10.1, unless the Data Controller - after the signing the Clauses - has changed the Data Controller's original choice. Such changes shall be documented and kept in writing, including electronically, in connection with the Clauses.

C.5 Processing location

C.5.1 Processing of personal data covered by the Clauses may not take place at locations other than those listed herein, and, if the Sub-Processors are used, at the locations specified in Appendix B without the prior written approval of the Data Controller.

Company	**Role (Data Processor/Sub-Processor)**	**Address**	**Type of data processing performed by the company**
Nuuday – TDC Erhverv	Sub-Processor	Teglholmsgade 1 2450 København SV, Denmark	Hosting, operation, maintenance, backup, monitoring, support

C.6 Instructions or approval of personal data transfer to third countries

C.6.1 Approval of transfer and any specific instruction regarding transfer of personal data to third countries or international organisations shall be included in Appendix D.

C.6.2 If the Data Controller has not provided an instruction or approval regarding the transfer of personal data to a third country in Appendix D or in a subsequent written communication, the Data Processor may not make such a transfer within the framework of the Clauses.

Specify transfer basis according to Chapter 5 of the General Data Protection Regulation in the table below:

	Mark with x
Transfers based on a decision of sufficiency security	
EU-standard contract	
Binding company rules (Article 47)	
Transfer or disclosure without basis in EU law (Article 48)	
Special circumstances (Article 49) Indicate which:	

C.7 Data Controller's supervision of the processing carried out by Data Processor and Sub-Processors

C.7.1 The Data Controller's supervision of the Data Processor is determined based on a risk assessment. When assessing the type of supervision, consideration must be given to the extent and sensitivity of the personal data, any legal requirements, and the criticality of the data processing for the organisation's task performance.

C.7.2 As a starting point, the supervision is conducted annually, and the time is indicated below.

C.7.3 The type of supervision, including any type of audit report, is agreed upon by the parties and indicated below.

C.7.4 Based on the results of the supervision, the Data Processor must take any necessary additional measures to comply with the requirements of the Data Processing Agreement.

C.7.5 The Data Processor is obligated to supervise any Sub-Processors. The type of supervision for the Sub-Processor must be approved by the Data Controller. Upon request by the Data Controller, documentation of the supervision must be provided to the Data Controller.

C.7.6 The Data Controller may decide that in addition, the Data Controller or a representative should have access to carry out inspections, including physical inspections, of the premises where the Data Processor or any Sub-Processors carry out the processing of personal data.

The Data Processor will annually and at its own initiative and expense prepare an ISAE3000 Declaration from an independent auditor to document compliance with the Data Protection Act and GDPR. The declaration also documents compliance with selected relevant security requirements for SDN and the Agreement System. The declaration is tailored to the specific relationship between the Data Processor and the Data Controller. The declaration is submitted to the Data Controller.

It is the Data Controller's responsibility to assess whether the declaration is sufficient to meet the Data Controller's supervision needs.

The Data Processor will annually and at its own initiative obtain and process declarations from Sub-Processors.

The Data Controller must bear the costs of any additional audits, including the participation of Sub-Processors, except if an audit is prompted by a breach of personal data security, remarks in audit declarations, or other objectively identifiable circumstances.

Appendix D The parties' regulation of other subjects

D1 Governance

The requirements for SDN are determined by MedCom's steering group, and the Data Controller cannot independently impose requirements on SDN. If the Data Controller requires specific measures to be implemented in SDN without corresponding requirements having been adopted by MedCom's steering group, such measures must be implemented solely at the Data Controller's expense.

To the extent that multiple Data Controllers require the same measures, the respective Data Controllers may share the costs of the measures.

Security policies and other relevant information regarding SDN can be requested from MedCom at any time.

D2 Employee security clearance

The Data Controller may require security clearances for employees of the Data Processor or its Sub-Processors. The Data Processor or its Sub-Processors must make themselves available for this in case of su a requirement.

Any associated costs will be at the expense of the Data Controller.

D3 Responsibility to notify the other Party

The Data Processor must:

a) Inform the Data Controller promptly about any surveillance activities and measures taken against the Data Processor concerning information processed on behalf of the Data Controller, in accordance with applicable law, unless such law prohibits the Data Processor from informing the Data Controller.
b) Inform the Data Controller if a data subject brings legal action against the Data Processor, in accordance with Article 79 of the GDPR.

The Data Controller must:

a) Inform the Data Processor promptly if the Data Controller becomes aware of a personal data breach that the Data Processor may have a role in.
b) Inform the Data Processor if a data subject brings legal action against the Data Processor, in accordance with Article 79 of the GDPR.

D4 Choice of law and jurisdiction

Any dispute or claim arising out of these Clauses shall be resolved in accordance with the Clauses on choice of law and jurisdiction in the Connection Agreement for SDN.

D5 Liability for damages

The terms of the Connection Agreement on limitation of liability and indemnification shall apply to the Clauses and nothing in the Clauses shall be construed as an extension of the liability and indemnification obligations in the Connection Agreement for SDN. The Data Processor's liability under Article 82 of the GDPR in relation to any recourse claims by the Data Controller is correspondingly limited in accordance with the Connection Agreement's regulation on indemnification and limitation of liability.

D6 Terms from the Connection Agreement for SDN after its termination

If the Connection Agreement for SDN expires before the Clauses, the following regulatory terms from the Connection Agreement shall continue to apply to the Clauses for as long as the Clauses remains in effect:

- Liability for damages and limitation thereof
- Supervision/control and compliance
- Economic regulation, including pricing
- Roles and responsibilities in relation to third parties
- Confidentiality
- Choice of law and jurisdiction
- Termination and expiry

D7 Particularly regarding backup

After deletion has occurred in the Agreement System in accordance with the Contract and section 10 of the Clauses, deletion in backup will occur at the expiration of the specified retention period for the relevan backup. This will be specified in the operations manual.

D8 Secure configurations and protection against malware

The Data Processor ensures, through Sub-Processors, maintenance of software/firmware and configuratio - as well as, to the extent relevant, maintenance of anti-malware and antivirus.

D9 Network security

IDS/IPS functionality is used in SDN, and vulnerability scans are conducted monthly.

D10 Surveillance

The Data Processor monitors the SDN through the Sub-Processor so that the Sub-Processor can react to interruptions and prevent interruptions based on exceeding threshold values.

D11 Changes

Renegotiation of the terms of the Clauses will take place in the governance agreed for SDN.