Sub-Data Processor Agreement

The Parties

Name of organisation:

Address:

Postal code and city:

CVR number:

(in the following referred to as **the Data Processor)**

and

MedCom

Forskerparken 10

DK-5230 Odense C

26 91 99 91

(in the following referred to as **the Sub-Data Processor**)

have concluded the following Sub-Data Processor agreement (in the following referred to as **the Sub-Data Processor Agreement**) regarding the Sub-Data Processor's processing of personal data on behalf of the Data Controller.

By this Sub-data processor agreement, the Data Processor secures that the Sub-data Processor is imposed the same data protection arrangements as the Data Processor is, concerning the Data Processor's instructions from the Data Controller about transmission of health data in the SDN.

1. Definitions

Data Controller	A natural or legal person, a public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the Data Controller or the specific criteria for its nomination may be provided for by Union or Member State law.
Data Processor	A natural or legal person, a public authority, agency or other body which processes personal data on behalf of the Data Controller.
Main Agreement	The agreement or contract concluded between the parties regarding the performance of the tasks to which the Sub-Data Processor Agreement relates.
Security Clearance	A status assigned to a person following an investigation conducted into that person so that he/she may be granted access to classified material or areas. In Denmark, investigations into persons and security clearances are performed by the Danish Security and Intelligence Service.
Third countries and international organisations	A third country is a country that is not a member of the EU or EEA (Iceland, Lichtenstein and Norway). An international organisation can be e.g. the International Red Cross, WHO, UN, OECD, etc. In order for the provisions of Chapter V of the Regulation to apply to international organisations, such international organisation must be located in a third country.
Sub-Data Processor	A Data Processor to whom the Data Processor has assigned all or part of the processing undertaken by Data Processor on behalf of the Data Controller.

2. General

2.1 This Sub-Data Processor Agreement concerns the Data Controller's and the Sub-Data Processor's obligation to comply with REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and repealing Directive 95/46/EC (General Data Protection Regulation) as well as the Danish act on supplementary provisions to the Regulation on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of Such Data (the Danish Data Protection Act).

2.2 The principles and recommendations of ISO27001, as amended, will in all relevant areas be applicable unless otherwise prescribed by this Sub-Data Processor Agreement.

2.3 The Sub-Data Processor shall process personal data in accordance with the rules and regulations for the processing of personal data in force from time to time.

2.4 If, in connection with the conclusion of this Sub-Data Processor Agreement, the Parties have agreed that the Sub-Data Processor is obligated to familiarise itself with and comply with the Data Controller's information security policy or other security guidelines, this must be stated in clause 17.2.

2.5 Both Parties shall keep a printed copy of the Sub-Data Processor Agreement including any appendices as well as a copy in electronic format.

3. Purpose

3.1 The Sub-Data Processor's task and the purpose of the processing are specified in clause 17.1.

3.2 The Sub-Data Processor must not process data covered by this Sub-Data Processor Agreement for its own purposes.

4. The Data Controller's rights and obligations

4.1 In respect of the surrounding world (including the data subject), the Data Controller is generally responsible for ensuring that personal data are processed within the scope of the General Data Protection Regulation and the Danish Data Protection Act.

4.2 Accordingly, the Data Controller has the right and obligation to make decisions on the purposes for which and the means by which processing can take place.

4.3 The Data Controller is, i.a., responsible for ensuring that a statutory basis exists for the processing which the Sub-Data Processor is instructed to carry out.

5. The Sub-Data Processor's general obligations

5.1 The Sub-Data Processor is the Sub-Data Processor of the personal data being processed by the Data Processor on behalf of the Data Controller in accordance with the Main Agreement and the Sub-Data Processor Agreement.

5.2 The Sub-Data Processor only acts according to documented instructions from the Data Controller as communicated by the Data Processor and only to the extent needed in order for the Sub-Data Processor to observe its obligations under the Main Agreement and Sub-Data Processor Agreement, see Appendix 1 Data Processor Instruction.

5.3 The Sub-Data Processor shall inform the Data Processor immediately if an instruction, in the opinion of the Sub-Data Processor, is in violation of the General Data Protection Regulation or data protection provisions of other Union or Member State law.

5.4 The Sub-Data Processor has the obligations as stipulated by legislation, see clause 2.1.

5.5 The Sub-Data Processor is obligated to provide accurate address specifications for where the Data Controller's personal data are stored, see clause 17.1. The Sub-Data Processor shall notify the Data Processor who notifies the Data Controller of any change.

5.6 This Sub-Data Processor Agreement does not release the Sub-Data Processor from obligations directly imposed on the Sub-Data Processor by the General Data Protection Regulation or other legislation.

6. Technical and organisational security measures

6.1 The Sub-Data Processor shall initiate all measures required under Article 32 of the General Data Protection Regulation, which stipulate, i.a., that taking into account 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.

6.2 The above obligation entails that the Sub-Data Processor shall make a risk assessment and then implement measures to address the identified risks. Depending on relevancy, 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

6.3 In connection with the above, the Sub-Data Processor shall – in all cases – as a minimum introduce the level of security and the measures as specified in Appendix 1 to this Agreement.

6.4 At least once a year, the Sub-Data Processor shall review its internal security regulations and guidelines for processing of personal data with a view to ensuring that the requisite security measures are continuously observed.

6.5 The Sub-Data Processor shall instruct any employees with access to or who otherwise process the Data Controller's personal data in the Sub-Data Processor's obligations, including any provisions on professional secrecy and confidentiality, see clause 11 and Appendix 1 Sub-Data Processor Instruction.

7. Use of ad hoc workstations

7.1 Use of ad hoc stations (remote or home workstations) must be approved by the Data Processor and the Data Controller.

7.2 If the Sub-Data Processor processes data from ad hoc workstations, the Sub-Data Processor shall ensure that such workstations comply with the security requirements specified in this Data Processor Agreement, including appendices and the Danish Data Protection Agency's related security information.

7.2.1 To the extent that data are processed from ad hoc workstations, the Sub-Data Processor shall describe the following in clause 17.2

- The type of encrypted connection used between the ad hoc workstation and the Sub-Data Processor's/Data Controller's network
- Use of 2-factor authentication
- The Sub-Data Processor's instruction to its own employees about the use of ad hoc workstations.

8. Notification obligation and assistance

8.1 The Sub-Data Processor shall notify the Data Processor who shall notify the Data Controller without undue delay of any deviations from the requirements of the Sub-Data Processor Agreement, e.g.:

- regarding any deviation from instructions given
- regarding any deviation from the agreed availability
- regarding planned releases, upgrades, tests, etc.
- regarding any suspected breach of confidentiality, misuse, loss and deterioration of data, etc.

8.2 Moreover, the Sub-Data Processor shall without undue delay and not later than 24 hours after having become aware of such breach notify the Data Processor who shall notify the Data Controller of any personal data breach, e.g.:

- in connection with any identified misuse, loss or deterioration of data, etc.
- in connection with accidental or unauthorised disclosure of or access to personal data processed under this Sub-Data Processor Agreement.

So that the Data Controller is able to observe the obligation to report the breach to the supervisory authority within 72 hours.

A report on personal data breach must contain the following information:

- the nature of the data breach and, if possible, who is covered, number of affected and number of affected personal data registrations
- description of probable consequences of the breach
- description of the measures the Sub-Data Processor has taken or suggested to be taken to manage the data breach and what can be done to contain any adverse effects it might have.

8.3 The Sub-Data Processor shall follow up the security incident and notify tue Data Processor who shall notify the Data Processor of the specific circumstances, including prepare a situation report and state what personal data have been compromised and what measures the Sub-Data Processor has initiated or intends to initiate.

8.4 The Sub-Data Processor and its Sub-Data Processors may not communicate about security breaches publicly or to third parties without prior written agreement with the Data Controller about the content of such communication, unless the Sub-Data Processor is legally obligated to provide such communication.

8.5 The Sub-Data Processor and any Sub-Data Processors shall without undue delay assist the Data Controller together with the Data Processor in managing any inquiries from a data subject, including requests for access, rectification, blocking or erasure if the relevant personal data are processed by the Sub-Data Processor. The Sub-Data Processor and any -

Sub-Data Processors shall also assist the Data Controller together with the Data Processor in observing other obligations that may rest on the Data Controller according to current law, where such assistance is implied, and where such assistance is necessary in order for the Data Controller to observe its obligations.

9. The Sub-Data Processor's use of Sub-Sub-Data Processors[1]

9.1 The Sub-Data Processor may not without the Data Processor's express written consent use other Sub-Data Processors than those specified in Appendix 2 to process personal data which the Data Controller has transmitted to the Data Processor in pursuance of the Sub-Data Processor Agreement and the Main Agreement. The Data Processor is entitled to stipulate terms for such consent.

9.2 The Sub-Data Processor shall conclude a written agreement with its Sub-Data Processor to ensure that the Sub-Data Processor as a minimum observes the obligations assumed by the Sub-Data Processor under this Sub-Data Processor Agreement as concerns the processing of personal data undertaken by the Sub-Data Processor. The Sub-Data Processor warrants the conformity and lawfulness of the Sub-Data Processor's processing of personal data. The circumstance that the Sub-Data Processor concludes an agreement with a Sub-Data Processor does not release the Sub-Data Processor of its duty to comply with this Data Processor Agreement.

9.3 The Data Processor may at any time demand documentation from the Sub-Data Processor regarding the existence and content of Sub-Data Processor agreements for the Sub-Data Processors used by the Sub-Data Processor in observing its obligations to the Data Controller and the Data Processor.

9.4 The Sub-Data Processor shall ensure and document that any Sub-Data Processors are familiar with and comply with the instructions of the Data Controller (Appendix 1).

9.5 All communication between the Data Controller and the Sub-Data Processor must generally take place via the Sub-Data Processor and the Data Processor.

9.6 The Sub-Data Processor shall notify the Data Processor on termination of an agreement with a Sub-Data Processor. In this connection, the Sub-Data Processor shall make sure that the Sub-Data Processor duly erases data as stipulated in clause 13.

Change of Sub-Data Processor during the agreement period

9.7 The Sub-Data Processor may appoint a new Sub-Data Processor, provided that the new Sub-Data Processor (1) observes current data protection legislation, (2) is bound by a Sub-Data Processor agreement and (3) has a security level that is at least the same as that of the current Sub-Data Processor.

[1] If a Sub-Data Processor is established in a third country, the provisions of clause 11 must also be observed.

9.8 The Sub-Data Processor shall notify the Data Processor if it appoints a new Sub-Data Processor. Such notification must be made not later than 3 months before the new Sub-Data Processor is used.

9.9 If the Data processor does not find that a Sub-Data Processor appointed by the Sub-Data Processor meets one or more of the above requirements (1), (2) and (3), such appointment will be considered as a material breach, in which case reference is made to clause 14 on breach. Before the Data Processor can claim a material breach, the Data Processor shall notify the Sub-Data Processor of the matter and allow the Sub-Data Processor a suitable period to remedy the breach.

10. Transmission of personal data to third countries or international organisations

10.1 The Sub-Data Processor may only process personal data subject to documented instruction from the Data Controller, including as concerns transmission (making available, disclosing and internal use) of personal data to third countries or international organisations, unless required by Union or Member State law with which the Sub-Data Processor shall comply; in this case the Sub-Data Processor shall inform the Data Processor of that legal requirement prior to processing, unless that law prohibits such information on important grounds of public interest, see point (a) of Art. 28(3) of the General Data Protection Regulation.

10.2 In the absence of the Data Controller's instruction or approval, the Sub-Data Processor may – within the scope of the Sub-Data Processor Agreement – therefore not:

a) transmit personal data to a Data Controller in a third country or in an international organisation,
b) entrust the processing of personal data to a Sub-Data Processor in a third country[2],
c) have the data processed in another of the Sub-Data Processor's departments located in a third country.

10.3 Any instruction or approval from the Data Controller that personal data may be transmitted to a third country will appear from clause 17.2 of this Agreement.

[2] See also clause 9

11. Professional secrecy and confidentiality

11.1 Personal data comprised by this agreement are confidential.

11.2 The Sub-Data Processor shall ensure that the persons authorised to process personal data on behalf of the Data Controller have undertaken to observe confidentiality or are subject to an appropriate statutory duty of professional secrecy.

11.3 The Sub-Data Processor and any of its Sub-Data Processors shall notify its/their own employees, partners, external consultants, temporary workers, etc. about the extent of the professional secrecy and of the consequences of breaching the professional secrecy.

11.4 Only persons at the Sub-Data Processor or its Sub-Data Processors who are duly authorised may access the personal data being processed, and the users may only be authorised to any uses they need in order to observe the Data Processor's obligations to the Data Controller.

11.5 The Sub-Data Processor and its employees are prohibited from obtaining information of any kind whatsoever that is immaterial to the performance of its or their tasks.

11.6 The Sub-Data Processor's obligations in respect of professional secrecy and confidentiality also apply after the termination of this Agreement.

12. Audit and audit declarations

12.1 At the Data Processor's request, the Sub-Data Processor shall provide the Data Controller with the information needed to check the compliance with the obligations under this Agreement and that appropriate technical and organisational security measures have been taken. Moreover, the Sub-Data Processor shall be able to document that identified vulnerabilities are addressed based on a risk-based assessment.

12.2 If the Data Controller, a representative of the Data Controller, its auditor (internal or external) or relevant public authority, primarily the Danish Data Protection Agency, wants to conduct a physical inspection (audit) of the measures established by the Sub-Data Processor under the Agreement, the Sub-Data Processor shall – subject to reasonable notice – provide the time and resources for such audit. The Sub-Data Processor shall also ensure that such audits can be conducted at any of its Sub-Data Processors.

12.3 As a supplement or alternative to the above audits, an agreement can be concluded to the effect that the Sub-Data Processor and any Sub-Data Processors, for their own account, arrange for an independent expert to prepare an annual audit declaration based on a recognised standard regarding the Sub-Data Processor's compliance with the requirements for security measures set out in the Sub-Data Processor Agreement. The declaration must

be formulated specifically for the task which the Sub-Data Processor solves for the Data Controller. Such agreement must be specified in clause 17.2.

13. Management of data after termination of the Agreement

13.1 The Sub-Data Processor and any of its Sub-Data Processors shall return and/or erase personal data once the processing carried out under the Main Agreement terminates, unless Union or Member State law prescribes that such personal data must be stored.

13.2 Prior to the termination of the Main Agreement, the Data Processor shall notify the Sub-Data Processor in writing of whether all personal data must be erased or be returned to the Data Controller. The deadline for such erasure or return must be agreed between the Parties.

13.3 The Sub-Data Processor shall ensure that erasure of data is done so that the data cannot be recreated. The Sub-Data Processor shall also ensure that the data are erased from backup and at any Sub-Data Processors.

13.4 If the data are returned to the Data Controller, the Sub-Data Processor shall erase any copies of the data.

13.5 Once the erasure is complete, the Sub-Data Processor shall forward a written declaration stating that the data have been erased as agreed.

13.6 If the Sub-Data Processor or its Sub-Sub-Data Processors in connection with bankruptcy or the like stop processing personal data for the Data Controller, all personal data must without undue delay be returned in a manner that allows the Data Controller to use them going forward. The Sub-Data Processor, its bankrupt estate or the like shall subsequently erase data from their own systems in accordance with clauses 13.1-13.5.

14. Breach

14.1 The provisions of this clause take precedence over the Main Agreement as concerns the processing of personal data. If this is not the case, this must be stated in clause 17.1.

14.2 If the Sub-Data Processor is in breach of the Sub-Data Processor Agreement, the Data Processor is entitled to rely on ordinary remedies with the additions and specifications described in the provisions of this clause.

14.3 In case of material breach of the Sub-Data Processor Agreement, the Data Processor is entitled to terminate the Main Agreement and thereby also the Sub-Data Processor

Agreement. Generally, breach is deemed to exist if the Sub-Data Processor fails to observe the obligations of the Sub-Data Processor Agreement, the legislation regarding data protection in force from time to time as well as the requirements provided in the documents that serve as appendices to the Sub-Data Processor Agreement.

14.4 Termination of the Main Agreement and Sub-Data Processor Agreement does not imply that the Data Processor waives its right to claim compensation if the conditions for compensation are observed, see clause 14.7.

14.5 If the Data Processor chooses not to terminate the Main Agreement and Sub-Data Processor Agreement in one or more cases, even though the Data Processor is entitled to do so, the Data Processor shall not lose its right to terminate the Main Agreement and Sub-Data Processor Agreement under other circumstances.

14.6 Where the Main Agreement and Sub-Data Processor Agreement are terminated, the Sub-Data Processor shall provide processing in accordance with the Main Agreement and this Sub-Data Processor Agreement until processing can be provided by another Sub-Data Processor. The Sub-Data Processor shall also provide relevant termination assistance to the Data Processor, including in relation to any Sub-Data Processors to whom the Sub-Data Processor have assigned part of the processing.

14.7 The Sub-Data Processor is liable in accordance with the general rules of Danish law in the event of breach of the Sub-Data Processor Agreement. If the Data Processor is held liable by the Data Controller or a third party for the Sub-Data Processor's and/or any Sub-Data Processor's failure to comply with the Sub-Data Processor Agreement, including the appendices of the Sub-Data Processor Agreement, and/or violation of current legislation regarding data protection, the Sub-Data Processor shall indemnify the Data Processor for any and all costs, fees, compensation, expenses or losses the Data Processor have had or assumed as a consequence thereof.

14.8 The Data Processor is entitled to demand that the Sub-Data Processor assists in defending the Data Controller or Data Processor's interests in any legal or arbitration proceedings, regardless of any objections the Sub-Data Processor may have to the claimed breach, if the Sub-Data Processor's assistance is important to safeguard the Data Controller or the Data Processor's interests.

15. Governing law and venue

15.1 Unless governing law and venue are directly stipulated by the Main Agreement, the following provisions will apply:

15.1.1 This Sub-Data Processor Agreement, including any matter relating to the validity of the Sub-Data Processor Agreement, is subject to Danish law.

15.1.2 In case of disagreement between the Parties related to the Sub-Data Processor Agreement, the Parties shall in a positive, cooperative and responsible manner seek to engage in negotiations to resolve the dispute.

15.1.3 If the Parties are unable to reach agreement by negotiation or otherwise, the dispute must be resolved by the Danish courts at the Data Controller's home court.

16. Commencement and duration

16.1 This Sub-Data Processor Agreement is concluded by the Parties' signature and is valid until the processing of personal data under the Main Agreement terminates and the Sub-Data Processor has erased the data, see clause 13.

16.2 The Data Processor and the Sub-Data Processor are jointly and severally liable for ensuring that the necessary updates are made to the Sub-Data Processor Agreement in case of legislative amendments, if the Data Controller becomes obligated to observe new security standards or if technical or organisational matters at the Data Controller, Data Processor and/or Sub-Data Processor change.

17. Specific matters related to the processing

(if the Sub-Data Processor's task in accordance with the Main Agreement concerns various types of processing, copies of the following tables will be provided in the left-hand side of the PDF window. These must be used for each processing covered by the Sub-Data Processor Agreement)

17.1 General matters

Name of data processing	The Danish Health Data Network (SDN)
ID in the Data Controller's list of data processing	
ID in the Data Processor's list	3
Main Agreement/contract (date of conclusion, journal ID)	Connection agreement for the SDN on:
Purpose of data processing	Support sharing via transmission of personal data between and for parties in the Danish health care sector.
General description of the processing	Agreement on sharing of personal data is managed and regulated by the connected parties in the SDN's agreement system as an instruction for the transmission.
Data subjects (categories of persons included in the data processing)	Patients, citizens, healthcare professionals and technical/administrative staff.

Categories of personal data	Personal data, including confidential and sensitive personal data in the form of healthcare data.
Any recipients of data	The parties defined in the agreement.
Time limits for erasure	Personal data being transmitted via the SDN network are not saved and there is no backup. Personal data in the user database of the agreement system are created and erased by the connected party. The agreement database of the agreement system contains documentation of which users from the connected party have entered into agreements. Such personal data are erased when the agreement is erased – on or before the termination of the party's connection to the SDN.
Any legislation/provision authorising the data processing	
The Data Processor's task	The Sub-Data Processor is tasked with establishing, operating, managing and monitoring the SDN and providing support as specified in the Main Agreement.
Data processing locations	Data are processed at the subcontractor TDC NetDesign and at the subcontractor Netic. For connections via SDN-MPLS, data are also processed in active network equipment located at the connected parties. For security reasons, the specific addresses are confidential, but can be provided on request.

17.2 Special matters regarding data processing (marked if it is not relevant)

Any other regulatory requirements governing the data processing (e.g. requirements that data must be stored in Denmark or any specific requirements for consent)	
Any other requirements imposed by the Data Controller on the Data Processor	Replacement of Sub-Data Processor in the SDN should be addressed regularly since the contract is subject to the public procurement procedure and is provided by MedCom on behalf of all SDN players. The Data Controllers are represented in the procurement process – both in the requirements specification and decision making through the user group and steering committee. MedCom is bound by the procurement procedure under procurement law and cannot give the Data Controller access to change its assessment of a new Sub-Data Processor after the contract has been awarded. Accordingly, clause 9.9 of the Data Processor Agreement has been derogated from in this Data Processor Agreement. Conditions in the SDN connection agreement (the Main Agreement), including provisions regarding breach, have been adopted by MedCom's steering committee, and a separate agreement has been concluded between MedCom and the the Data Controller within the framework of public-public partnership. Provisions on breach in this Sub-Data Processor Agreement will therefore not apply. Accordingly, clause 14 of the Sub-Data Processor Agreement has been derogated from. If the Data Controller or Data Processor requires that specific measures be implemented into the SDN and similar requirements have not been adopted by MedCom's steering committee, such measures should only be implemented at the Data Controller or Data Processor's expense. To the extent that several Data Controllers or Data Processors require the same measures, the Data Controllers or Data Processors in question may share the costs of the measures.

Agreement between the parties to fully or partially derogate from requirements in the Data Processor Agreement (Describe agreed derogations and any compensatory security measures)	The requirements for the SDN are laid down by MedCom's steering committee, and the Data Controller cannot make its own requirements for the SDN. If the Data Controller requires that specific measures be implemented into the SDN and similar requirements have not been adopted by MedCom's steering committee, such measures should only be implemented at the Data Controller's expense. To the extent that several Data Controllers require the same measures, the Data Controllers in question may share the costs of the measures. Security requirements at MedCom are based on ISO27001, but may be subject to specific deviations. MedCom's current security measures can be ordered from MedCom. All failed log-in attempts are recorded. Repeated log-in attempts are not blocked, since a blocking might affect legitimate logins from the same user location at the connected party. Repeated log-in attempts will instead trigger an alarm to determine the cause. Accordingly, the instruction in clause 5.1 of the Data Processor Agreement has been derogated from.

The Data Processor is obligated to comply with the Data Controller's information security policy and/or guidelines. (State relevant documents)	The requirements for the SDN are laid down by MedCom's steering committee, and the Data Controller cannot make its own requirements for the SDN. If the Data Controller requires that specific measures be implemented into the SDN and similar requirements have not been adopted by MedCom's steering committee, such measures should only be implemented at the Data Controller's expense. To the extent that several Data Controllers require the same measures, the Data Controllers in question may share the costs of the measures. Security policy etc. for the SDN can be obtained from MedCom at any time.

The Data Controller has instructed or approved transmission of personal data to a third country or international organisation (state also transmission basis subject to Chapter V of the General Data Protection Regulation)	The SDN provides connection of international parties to the SDN, including unsecure third countries. International parties must be approved before being connected to MedCom's steering committee. The transmission of personal data requires an agreement between the parties in the agreement system, i.e. the Data Controller through the Data Processor and the international party. The Data Controller shall ensure that a legal basis exists for transmitting personal data to unsecure third countries.
Special technical or organisational security measures that need to be established at the Data Processor (e.g. security clearance of employees)	The requirements for the SDN are laid down by MedCom's steering committee, and the Data Controller cannot make its own requirements for the SDN. If the Data Controller requires specific measures to be implemented into the SDN and similar requirements have not been adopted by MedCom's steering committee, such measures should only be implemented at the Data Controller's expense. To the extent that several Data Controllers require the same measures, the Data Controllers in question may share the costs of the measures. Security policy etc. for the SDN can be obtained from MedCom at any time.
Description of security measures when using ad hoc workstations as agreed with the Data Controller	The use of ad hoc workstations by the Sub-Data Processor TDC Netdesign and by the Sub-Sub-Data Processor Netic is, as a minimum, subject to the following requirements: Remote access to the SDN takes place via AES256-bit-encrypted VPN access with 2-factor authentication. Access to the agreement system takes place via a web interface with TLS 1.2 encryption and 2-factor authentication.
Description of security measures in connection with external links	SDN-MPLS is a fully meshed private / segmented network ensuring, via the same VRF, that the SDN-connected parties can communicate with each other if allowed by the ACLs in the decentralised active network equipment of the connected parties. The security of fixed links, other MPLS links and VPN links are handled by ACLs in the centralised network equipment in the SDN hub.

Elaborate description of measures to protect the transmission of personal data in open networks	Security requirements for VPN links are specified on MedCom's website.
Log storage period (if more than 6 months, see clause 5.2 of the Data Processor Instruction).	Traffic on the SDN is logged for aggregation of monitoring and traffic statistics across the connected parties. The log does not contain personal data but only data about the completed transmission – and is not erased. Event log in the agreement system documents user actions and is erased after 2 years. When a connected party is cancelled in the agreement system, the event log is cleared of personal data from the connected party.
Any agreement on the preparation of audit declaration, including specification of type	MedCom ensures that an annual independent ISAE 3000 IT audit is carried out of the SDN, including the VDX, for the purpose of being able to document compliance with the Danish Data Protection Act. The Data Controller or Data Processor shall pay the costs of further auditing, including the costs of participation by Sub-Data Processors and its Sub-Data Processors.

17.3 Contact details for notification of security incidents

Contact persons of the Data Controller in the event of common deviations from normal operation	
Function	Technical contact person in the SDN Connection Agreement
Name	*(specified in the connection agreement)*
E-mail	*(specified in the connection agreement)*
Telephone	*(specified in the connection agreement)*
Comments	
Contact persons of the Data Controller in the event of actual and suspected critical errors and vulnerabilities	
Function	Security officer and technical contact person in the SDN Connection Agreement
Name	*(specified in the connection agreement)*
E-mail	*(specified in the connection agreement)*
Telephone	*(specified in the connection agreement)*
Comments	
Contact persons of the Data Processor in the event of common deviations from normal operation	

Function	Security officer
Name	Peder Illum
E-mail	sdn@medcom.dk
Telephone	6543 2030
Comments	In practice, all inquiries must be addressed to the SPOC of the Sub-Data Processor. Contact details and information can be found on www.medcom.dk.
Contact persons of the Data Processor in the event of actual and suspected critical errors and vulnerabilities	
Function	Security officer
Name	Peder Illum
E-mail	sdn@medcom.dk
Telephone	6543 2030
Comments	In addition to MedCom, all inquiries must be addressed to the SPOC of the Sub-Data Processor. Contact details and information can be found on www.medcom.dk.

18. List of appendices

Appendix 1: Data Processor Instruction
Appendix 2: Sub-Data Processor

For the Data Processor

Date:

Name:

_____

For the Sub-Data Processor

Date:

Name:

_____

Appendix 1
Data Processor Instruction

1. Data Processor's responsibility

Data processing under the Data Processor Agreement must be in compliance with this Instruction.

2. General

2.1 The Data Processor shall as a minimum take the technical and organisational security measures described below in connection with the processing of the personal data under the Data Processor Agreement.

2.1.1 If more comprehensive technical and organisational security measures, described in clause 17.2, are necessary to ensure compliance with clause 6.1 of the Data Processor Agreement, such more comprehensive measures must always be taken.

2.2 The Data Processor shall appoint a fixed point of contact for the Data Controller to handle all matters in relation to the processing of personal data on behalf of the Data Controller, see clause 17.3.

2.3 The Supplier shall take the necessary steps to identify, assess and limit any reasonably foreseeable internal and external risk for the availability, confidentiality and/or integrity of all personal data covered by the Data Processor Agreement.

3. Authorisation and access control

3.1 Authorisations must specify the extent to which the user may request, enter or erase personal data.

3.2 The Data Processor shall ensure that an appropriate background check is performed of all staff who, in connection with their employment, will have access to personal data covered by the Data Processor Agreement, regardless of the format in which the personal data are available.

3.2.1 If the Data Controller requires the staff of the Data Processor who have

access to personal data to be security cleared, this must be specified in clause 17.2 of the Data Processor Agreement.

3.3 Only authorised persons at the Data Processor may have access to personal data processed in accordance with the Data Processor Agreement. Authorisation may only be given to persons engaged with the purposes for which the personal data are processed.

3.4 Moreover, authorisation may be given to persons at the Processor whose access to the personal data is necessary to perform audit, operation and technical system-related tasks.

3.5 The Data Processor shall be able to document what employees have authorisation to access personal data processed in accordance with the Data Processor Agreement.

3.6 Authorised persons at the Processor are provided with a personal user identification and a personal password which must be used every time they log onto the system. 2-factor authentication must be used in connection with access to systems with sensitive personal data via the Internet or other insecure network.

3.7 The Data Processor shall ensure that its employees receive proper training and instructions to ensure that personal data are processed in compliance with relevant legislation and the policies and procedures of the Data Processor and Data Controller in this respect.

3.8 Measures must be taken to ensure that only authorised users can access personal data and that users can only access the personal data and applications (processing) for which they are authorised.

3.9 The Data Processor shall have formal procedures in place for managing resetting of passwords and for other situations where the normal logical access control is suspended.

3.10 At least once every 6 months, a control must be made to ensure that users only have the access that they need. Such control might entail that statistics is generated in the systems of the use by the individual user of the system, so that it can be established whether authorisations have been issued that are not used and should therefore be revoked. When such statistical follow-up is used, a specific assessment will still be needed of whether the employee still has a work-related need for access.

3.11 The Data Processor shall without undue delay revoke authorisations (including access) for users who no longer need the authorisation for their work.

4. Physical security

4.1 The Data Processor shall ensure that IT equipment used in connection with the data processing is physically secured according to current statutory requirements.

4.2 The Data Processor shall have appropriate technical measures in place to minimise the risk of any authorised access. Moreover, the Data Processor shall, where necessary, evaluate and improve the efficiency of such measures.

4.3 In connection with the repair and service of equipment, the Data Processor shall ensure that the repair and service staff treat as confidential any personal data of which they become aware during their work.

4.4 When equipment and storage media containing personal data are disposed of, such storage media must be destroyed or demagnetised to ensure effective erasure of the personal data. Documentation proving that disposal has been carried out in accordance with the above must be produced at the request of the Data Controller.

5. Control of failed login attempts and logging

5.1 All failed login attempts must be registered. If, within a predetermined period, a maximum of 35 consecutive failed login attempts are registered from the same workstation or with the same user identification, further login attempts must be blocked. Access will not be opened until the reason for the failed login attempts has been explained.

5.2 Machine registration (logging) must be made in connection with all processing of personally identifiable information. The log must as a minimum include information about time, user, type of use and specification of the person which the used data concern, or the search criterion used. The log must be stored for 6 months, unless, according to the purpose of the log, a longer storage period is determined for the purpose of being able to use the log as an investigation tool.

5.2.1 If a longer storage period is agreed for the log, this must be specified in clause 17.2 of the Data Processor Agreement.

5.3 At the request of the Data Controller, the Data Processor shall make all necessary login information available to the Data Controller for the purpose of periodic audits or investigation of abuse or suspected abuse.

6. Management of input and output data material containing personal data

6.1 Input data material may only be used by persons engaged with entering data. Input data material must be stored in such a way that unauthorised persons cannot access and familiarise themselves with the personal data contained therein.

6.2 When it is no longer necessary to store the input data material, the Data Processor shall erase or destroy the input data material. The procedure for this must be based on best practice.

6.3 Clause 6.2 does not apply if the material is covered by preservation/disposal provisions under other legislation, of if recorded material is handled according to the general archive provisions on preservation, including delivery of records to the Danish National Archives.

6.4 Output data material is covered by the same instructions as input data material.

6.5 In addition to the provision of clause 6.4, output data material may only be used by persons engaged with the purposes for which the personal data are processed and in connection with audit, technical maintenance, operational monitoring and error correction etc.

7. Mobile storage units

7.1 Mobile storage media containing personal information must be labelled, encrypted and kept under supervision or locked up when they are not used.

7.2 Mobile storage media containing personal data may only be handed over to authorised persons carrying out audit, operation and technical system tasks.

7.3 A list must be kept of the mobile storage media which are used in connection with the data processing.

7.4 Written instructions must be prepared for the use and storage of removable mobile storage media.

7.5 In connection with the repair and service of data equipment containing personal data and in connection with sale and disposal of used data media, the necessary measures must be

taken to ensure that personal data are not accidentally or intentionally destroyed, lost or impaired and that the personal data is not disclosed to unauthorised persons, is abused or is otherwise processed contrary to current legislation. This must be based on best practice.

8. Back-up copies

8.1 The same guidelines apply to back-up copies as for all other processing of personal data under this Agreement.

8.2 The Data Processor shall ensure that regular back-up copies are taken of systems and personal data. The back-up copies must be stored separately from the servers in a non-adjacent room to ensure that they are not lost, e.g. as a result of fire or flooding. Back-up copies must always be stored safely so that they are not lost.

8.3 The Data Processor shall regularly check that back-up copies are readable. This must be done from a continuity point of view, e.g. in connection with major changes to the technical system setup.

9. Updates and changes

9.1 The Data Processor shall have formal procedures in place to ensure that updates to operating systems, databases, applications and other software are assessed and implemented within reasonable time.

9.1.1 For critical security updates, the Data Processor shall have procedures in place which ensure that such updates can be implemented within 48 hours.

9.2 The Data Processor shall have formal change management procedures in place with a view to ensuring that any change is duly authorised, tested and approved before implementation. The procedure must be supported by an efficient functional restriction or management follow-up to ensure that no individuals can implement a change alone.

10. External communication links

10.1 External communication links may only be established subject to permission from the Data Controller and if measures are taken to ensure that unauthorised persons cannot gain access to personal data via these links.

10.1.1 Measures must be taken to protect personal data transmitted in open networks. Any detailed descriptions of the measures must be provided in clause 17.2 of the Data Processor Agreement.

11. IT business continuity planning

11.1 The Data Processor shall have documented IT business continuity procedures in place that ensure restoration of services within reasonable time in the event of business interruption.

12. Notification of security incidents and assistance in the management

12.1 The Data Processor shall have a procedure in place for the management of and follow-up on security breaches in compliance with the requirements of ISO27001.

12.2 The Data Processor shall document the identified risks and how the risk has been reduced to an acceptable level.

12.3 A list of contact persons in connection with notification of security incidents must be provided in clause 17.3 of the Data Processor Agreement.