



Region Syddanmark

Department xxx
Contact: xxx xxx
xxx.xxx@rsyd.dk

Month xx 20XX
Page 1/13

File no.: **xx/xxx**

System-/project responsible person |
Tel. +45 XXXX XXXX |
e-mail@e-mail.dk |

DATA PROCESSOR AGREEMENT

Regarding **Project name/title/system/description**

The present data processing agreement (hereinafter referred to as the "Data Processing Agreement") relates to the obligations of the Data Processor in regards to observing REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) and Act on additional stipulations for Regulation on the protection of natural persons in connection with the processing of personal data and free movement of such data (the Data Protection Act).

The Data Processing Agreement has been entered into

Region Syddanmark
Damhaven 12
7100 Vejle
CVR no.: 29190909
(hereinafter referred to as the "*Data Controller*")

and

Name of the firm

Address

Possible branch

Contact

CVR no.

(hereinafter referred to as the "*Data Processor*")

and forms part of **agreement of xx. Xxxxxx 201x on... (hereinafter referred to as the "Main Agreement")**

The data covered by the Data Processor Agreement shall be processed (and subsequently among other things stored) at the following **address(es)**

1. Responsibilities of the Data Processor

- 1.1. The Data Processor shall only act on instructions from the Data Controller and only to the extent which is necessary to enable the Data Processor to fulfil its obligations in accordance with the Main Agreement and the Data Processor Agreement.

The Data Processor Agreement shall thus form part of the instructions of the Data Controller to the Data Processor. The Data Processor shall not process data covered by the present Data Processor Agreement for his own purposes.

- 1.2. The Data Processor Agreement shall not release the Data Processor from obligations imposed directly on the Data Processor in accordance with the Regulation on the Protection of Data or any other legislation.
- 1.3. If the Data Processor is subject to the legislation in a third country, the Data Processor shall immediately inform the Data Controller in writing if the legislation in question prevents the Data Processor from observing the Data Processing Agreement and the related instructions.

- 1.4. If a Data Processor is subject to national legislation permitting processing of personal data contrary to the Data Processing Agreement and the related instructions, the Data Controller shall be informed accordingly before processing is initiated, unless the legislation in question prohibits such notification for reasons of compelling public interest.

2. Task of the Data Processor

- 2.1. **The purpose of and background for the data procession shall be...**

- 2.2. **The task of the Data Processor shall be to...**

(for example to host/support/operate the system, etc. – clear description of the data processing carried out by the Data Processor, including how data is exchanged between the Data Controller and the Data Processor...)

- 2.3. **The data processing will include the following categories of data subjects...**

- 2.4. **The data processing will include the following categories of data**

3. Technical and organisational security measures

- 3.1. The Data Processor shall implement the necessary technical and organisational security measures to ensure that information is not accidentally or illegally destroyed, lost or deteriorated, and to ensure that it is not disclosed to irrelevant persons, abused or otherwise processed contrary to the legislation on personal data.

Minimum requirements regarding the necessary technical and organisational security measures appear from Appendix 1.

- 3.2. Furthermore, the Data Processor undertakes to process the personal data in accordance with the information security policy covering the Data Controller, cf. Appendix 2.

- 3.3. The principles and recommendations set out in ISO 27001 with subsequent amendments shall be used as an informative framework for observing the requirements of the present Data Processor Agreement.

4. A. The Data Processor's use of Sub-Processors

- 4.1. The Data Processor must not engage a Sub-Processor in the processing of personal data covered by the present Data Processor Agreement, unless otherwise stated in Appendix 3 to the Data Processor Agreement.
- 4.2. If a Sub-Processor is engaged, the Data Processor shall hand over the Data Processor Agreement entered into by the Data Processor and the Sub-Processor at the request of the Data Controller. The Data Processor must be able to document that the Sub-Processor has been instructed, cf. Appendix 1 to the Data Processor Agreement.
- 4.3. In the agreement with the Sub-Processors, the Data Processor shall ensure that as a minimum the Sub-Processor is able to meet the data protection obligations undertaken by the Data Processor under the present Data Processor Agreement regarding the processing of personal data carried out by the Sub-Processor, just as the Sub-Processor must have the same level of security as the Data Processor.
- 4.4. The Data Processor shall be responsible for the contractual and legal nature of the Sub-Processor's processing of personal data, including conclusion of a data processing agreement with at least the same obligations as those applying to the Data Processor in accordance with the data protection rules and the present Data Processor Agreement with its Appendices. The fact that the Data Processor enters into an agreement with a Sub-Processor shall not release the Data Processor from the obligation to observe the present Data Processor Agreement.
- 4.5. Upon expiry of an agreement with a Sub-Processor regarding the processing of personal data covered by the present Data Processor Agreement, the Data Processor shall inform the Data Controller accordingly. In this connection, the Data Processor shall ensure that the Sub-Processor will erase data appropriately in accordance with clause 10.
- 4.6. Furthermore, the Data Processor shall not be entitled to transfer or to allow the transfer of personal data to countries outside the EU and the EEA, un-

less the Sub-Processors in question appear from Appendix 3 to the Data Processor Agreement.

- 4.7. If the Data Controller has given the Data Processor an explicit permission to transfer personal data to a Sub-Processor in countries outside the EU and the EEA, the Data Processor shall be obliged to ensure that data is not transferred until there is a legal basis for the transfer of personal data to the countries in question. If an engaged Sub-Processor is located in countries outside the EU and the EEA, this must appear from Appendix 3 to the Data Processor Agreement.
- 4.8. In his agreement with the Sub-Processor, the Data Processor shall enter the Data Controller as the beneficiary third party in the event of the liquidation of the Data Processor, so that the Data Controller may enter into the rights of the Data Processor and claim such rights towards the Sub-Processor, for example so that the Data Controller may order the Sub-Processor to erase or return data.

4. B. Change of Sub-Processor during the term of the agreement

- 4.9. The Data Processor may appoint a new Sub-Processor if the new Sub-processor (1) observes current legislation on data protection and (2) is bound by a data processing agreement, or an EU model contract or a similar agreement, and (3) has a security level corresponding at least to that of the current Sub-Processor.
- 4.10. The Data Processor shall notify the Data Controller if a new Sub-Processor is appointed. Such notice must be given three months prior to the engagement of the new Sub-Processor. The notice must be forwarded to **(XX possibly mail box)**.
- 4.11. If the Data Controller is of the opinion that a Sub-Processor appointed by the Data Processor does not meet one or more of the above mentioned requirements under clauses (1), (2), and (3), it will be considered a material breach. Reference is made to clause 13 on breach.
- 4.12. The Data Controller shall at any time be entitled to receive a copy from the Data Processor of the Data Processor's agreement (flow down-agreements) with the Sub-Processor(s) mentioned in appendix 3.

5. Transfer of data to third countries or international organisations

- 5.1. The Data Processor shall only be entitled to process personal data in accordance with documented instructions from the Data Controller, including regarding the transfer (handing over, disclosure and internal use) of personal data to third countries or international organisations, unless it is required in accordance with EU legislation or the national legislation of the member states to which the Data Processor is subject; in such cases, the Data Processor shall inform the Data Controller of the statutory requirement prior to processing, unless the legislation in question prohibits such notification for reasons of compelling public interest, cf. article 28 (3) letter a.
- 5.2. Without instruction or approval from the Data Controller, the Data Processor shall therefore – within the framework of the Data Processor Agreement – among other things not be entitled to:
- a. Disclose personal data to a data controller in a third country or in an international organisation,
 - b. Leave the processing of personal data to a Sub-Processor in a third country,
 - c. Have the personal data processed in another branch of the Data Processor situated in a third country
- 5.3. The Data Controller's possible instructions or approval of the transfer of personal data to a third country will appear from Appendix 3 to the present Agreement.

6. Ad hoc workplaces

- 6.1. If the Data Processor carries out data processing from ad hoc workplaces, the Data Processor shall ensure that they comply with the security requirements in the present Data Processor Agreement with appendices, and the IT security texts issued by the Danish Data Protection Agency.
- 6.2. If ad hoc workplaces are used, this must be stated in clause 15.
- 6.3. The Data Processor must among other things observe and document the following:

- Description of encrypted connection used between the ad hoc workplace and the network of the Data Processor/Data Controller.
- Use of two-factor authentication.
- The Data Processor's internal instructions to own employees regarding ad hoc workplaces.

7. Supervisory authorities, audits and audit report

- 7.1. At the request of the Data Controller, the Data Processor shall provide the Data Controller with necessary information to enable the Data Controller to supervise the obligations in accordance with the present Agreement, including whether the above technical and organisational security measures, etc., have been taken. Furthermore, the Data Processor must be able to document that identified vulnerabilities are met on the basis of a risk-based assessment.
- 7.2. If the Data Controller and/or the relevant public authorities, in particular the Data Protection Agency, wants/want to carry out a physical inspection (audit) of the measures taken by the Data Processor in accordance with the Data Processor Agreement, the Data Processor undertakes – with a reasonable notice – to make time and resources available for this purpose. Similarly, the Data Processor undertakes to ensure that such audits can also be carried out by the Data Processor at his Sub-Processors.
- 7.3. As a supplement or alternative to the above audits, an agreement may be made to the effect that the Data Processor and any Sub-Processors shall at their own expense ensure that an independent expert will annually prepare an audit report on the basis of an acknowledged standard for the Data Processor's compliance with the requirements regarding security measures determined in the Data Processor Agreement. The report shall be prepared considering the task solved by the Data Processor for the Data Controller. An agreement in this respect must appear from clause 15, unless otherwise provided in the Main Agreement.

8. Information and assistance

- 8.1. The Data Processor undertakes to inform the Data Controller without undue delay and in writing of deviations from the requirements in the Data Processor Agreement, for example:

- any deviation from instructions given
- any deviation from the agreement regarding availability
- planned releases, upgrades, tests, etc.
- any suspicion of breach of confidentiality, abuse, loss and deterioration of data, etc.

8.2. Furthermore, the Data Processor undertakes to inform the Data Controller without undue delay and in writing of breach of personal data security, for example:

- any determination of abuse, loss and deterioration of data, etc.
- any accidental or unauthorised disclosure of or access to personal data processed in accordance with the present Data Processor Agreement.

Information about breach of personal data security shall include the following information:

- The nature of the breach of data security and, if possible, the people involved, the number of people affected, and the number of registrations of personal data affected.
- Description of the probable consequences of the breach.
- Description of the measures taken or suggested by the Data Processor in order to handle the data breach, and what can be done to limit the damage it may possibly cause.

8.3. Without undue delay, the Data Processor shall assist the Data Controller with the handling of any communication from a data subject regarding request for exercising the rights of the data subject, cf. chapter III of the General Data Protection Regulation, including for example access by the data subject, rectification, blocking, erasure ('the right to be forgotten') if the relevant personal data is processed by the Data Processor.

8.4. The Data Processor shall assist the Data Controller in observing any obligations of the Data Controller in accordance with current legislation, and

when assistance is required to enable the Data Controller to observe such obligations, including the obligation to carry out a data protection impact assessment if a type of processing is likely to involve a high risk for the rights and freedoms of natural persons.

9. Effective date and term of the Agreement

- 9.1. The Data Processor Agreement shall become effective when signed by all parties.
- 9.2. The Data Processor Agreement shall apply for the duration of the processing and shall remain effective until the end of the processing and erasure of the personal data with the Data Processor and any Sub-Processors.

10. Handling of data after expiry of the Agreement

- 10.1. The Data Processor and any Sub-Processors undertake to return and/or erase personal data when the data processing in accordance with the Main Agreement ends. The Data Controller shall inform the Data Processor of the time when the data processing is to end. The Data Processor shall then be obliged to return and/or erase the personal data and to erase existing copies at the date and time stated, unless the personal data is to be stored in accordance with EU legislation or national law.
- 10.2. The Data Processor shall be responsible for erasing the data so recovery thereof will not be possible. The Data Processor shall be responsible for ensuring that the data is also erased from backup systems and from the systems of possible Sub-Processors.
- 10.3. When the personal data has been erased, the Data Processor must forward a written statement to the effect that data has been erased as agreed upon.
- 10.4. If the Data Processor or any Sub-Processors in connection with liquidation, etc., stops processing personal data for the Data Controller, all personal data must immediately be returned to the Data Controller in a way which makes it possible for the Data Controller to use it in the future. The Data Processor, its estate in liquidation, etc., shall then effectively erase the personal data from its own systems in accordance with the above.

11. Personal data covered by the present Agreement is confidential

- 11.1. The Data Processor shall ensure, and at the request of the Data Controller demonstrate, that the employees, Sub-Processors, cooperating partners, external consultants, temporary workers, etc., who are authorised to process the personal data covered by the Agreement have undertaken confidentiality or are subject to statutory secrecy.
- 11.2. The Data Processor shall inform employees, Sub- Processors, cooperating partners, external consultants, temporary workers, etc., of the duty to secrecy.
- 11.3. The Data Processor shall ensure that the access to personal data covered by the present Data Processor Agreement is limited to the employees for whom it is necessary to process personal data in order to observe the obligations of the Data Processor towards the Data Controller. The access to information must therefore immediately be stopped if authorisation is revoked or expires.
- 11.4. The obligations of the Data Processor to secrecy and confidentiality shall apply also after termination of the Main Agreement.

12. Assignment

- 12.1. The Data Processor shall not be entitled to assign his rights and obligations in accordance with the present Data Processor Agreement without the prior consent of the Data Controller.

13. Breach

- 13.1. The stipulations in the present section shall take precedence of the Main Agreement in so far as the processing of personal data is concerned.
- 13.2. If the Data Processor is in breach of the Data Processor Agreement, the Data Controller shall be entitled to the usual remedies for breach with the additions and clarifications which appear from the stipulations in the present section.
- 13.3. In the case of material breach of the Data Processor Agreement, the Data Controller shall be entitled to cancel the Main Agreement, and therefore also the Data Processor Agreement. As a starting point, it is considered material breach if the Data Processor does not observe the obligations in

the Data Processor Agreement, the legislation in force at any time regarding data protection, and the requirements in the documents which are appendices to the Data Processor Agreement.

- 13.4. Cancellation of the Main Agreement and the Data Processor Agreement by the Data Controller shall not mean that the Data Controller waives his right to claim compensation if the relevant conditions have been met, cf. sub-clause 13.7.
- 13.5. If the Data Controller chooses not to cancel the Main Agreement and the Data Processor Agreement in one or more cases, even if the Data Controller is entitled to do so, this shall not mean that the Data Controller loses the right to cancel the Main Agreement and the Data Processor Agreement in other cases.
- 13.6. In connection with cancellation of the Main Agreement and the Data Processor Agreement, the Data Processor shall provide data processing in accordance with the Main Agreement and the present Data Processor Agreement until data processing has been arranged with another data processor. Furthermore, the Data Processor shall provide relevant termination assistance to the Data Controller, including in relation to any Sub-Processors to whom the Data Processor may have left part of the data processing.
- 13.7. The Data Processor shall be liable to pay compensation in accordance with the general rules of Danish law in the event of breach of the Data Processor Agreement. If the Data Controller is held liable by a third party to pay compensation for the Data Processor's and/or any Sub-Processors' failure to observe the Data Processor Agreement, including the appendices of the Data Processor Agreement, and/or violation of current legislation regarding data protection, the Data Processor shall indemnify the Data Controller for all costs, fees, amounts of compensation, expenses or losses paid or incurred by the Data Controller as a consequence thereof.
- 13.8. The Data Controller shall be entitled to demand that the Data Processor shall assist in the defence of the interests of the Data Controller during potential legal or arbitration proceedings, regardless of the Data Processor's objections, if any, in relation to the claimed breach, if the assistance of the Data Processor is of material importance to the safeguarding of the Data Controller's interests.

14. Governing law and venue

- 14.1. The stipulations in the present section shall not apply if governing law and venue have been regulated separately in the Main Agreement.
- 14.2. The present Data Processor Agreement, including any question of the validity of the Data Processor Agreement, shall be governed by Danish law.
- 14.3. *Negotiation*
If a dispute occurs between the Parties in connection with the Data Processor Agreement, the Parties shall with a positive, cooperative and responsible attitude start negotiations with a view to solving the dispute.

Either:

- 14.4. *Arbitration*
If agreement cannot be reached by negotiation or otherwise, the dispute shall be solved by arbitration.

The dispute shall be solved before the Danish Institute of Arbitration in accordance with the rules adopted by the institute and in force at the initiation of the arbitration case.

Or:

- 14.5. *Hearing before a court*
If agreement cannot be reached by negotiation or otherwise, the dispute shall be solved before the Data Controller's Danish home court.

15. Changes to clause 1-14

- 15.1. If it is absolutely necessary to change the clauses 1-14, such changes shall be described here.

16. Appendices

Appendix 1: Data Processor Instructions

Appendix 2: The Data Controller's Information Security Policy

Appendix 3: The Data Processor's Sub-Processors

Any other appendices

Signatures



On behalf of the Data Controller:

Name:

Position:

Address

Date:

Signature:

The Data Controller's project responsible person/the system owner's contact:

Name:

Position:

Address:

Date:

Signature:

On behalf of the Data Processor:

Name:

Position:

Address:

Date:

Signature: