Data Processing Instructions

Re 1. Responsibility of the Data Processor

1.1 Data Processing covered by the Data Processing Agreement shall be carried out in accordance with the present Instructions.

Re 3. Technical and organisational security measures

3.1 The Data Processor shall at least take the below technical and organisational security measures in connection with the processing of personal data covered by the Data Processing Agreement.

3.1.1 If more extensive technical and organisational security measures are required to ensure compliance with clause 3 of the Data Processing Agreement, such measures shall be taken at all times.

3.2 Security risks

3.2.1 The Data Processor shall take the necessary steps to identify, assess and limit any reasonably foreseeable internal and external risks regarding the accessibility, confidentiality and/or integrity of all personal data covered by the Data Processing Agreement.

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

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

The above obligation implies that the Data Processor shall carry out a risk assessment and thereafter take measures to meet the identified risks. This may, depending on what is relevant, include the following measures:

a. Pseudo-anonymization and encryption of personal data

b. The ability to ensure continuous confidentiality, integrity, availability and soundness of processing systems and services.
c. The ability to restore availability of and access to personal data in due time in the event of a physical or technical event
d. A procedure for regular testing, assessment and evaluation of the effectiveness of the technical and organisational measures to ensure processing security

3.2.4 The Data Processor must have formal procedures for the handling of security incidents.

3.3 Authorisation and access control

3.3.1 Authorisations shall state the extent to which the user is entitled to enquire, enter or erase personal data.

3.3.2 Only authorised persons shall have access to personal data processed in accordance with the Data Processing Agreement.

3.3.3 The Data Processor shall be able to document which employees are authorised to access personal data processed in accordance with the Data Processing Agreement.

3.3.4 Authorised persons must be able to present photo ID in connection with on-site data processing on the premises of the Data Controller.

3.3.5 Only individuals involved in the purposes for which the personal data is processed shall be authorised. The individual users shall not be authorised for tasks for which they have no use.

3.3.6 Furthermore, individuals for whom access to personal data is required for the purpose of performing audit or operational and system-technical tasks can be authorised.

3.3.7 The authorised user shall be provided with personal user identification and a personal password which must be used whenever access is granted to the data processing. Passwords shall be changed every six months. Passwords shall be sufficiently long and complex. As a general rule, two-factor authentication shall be used for access to systems with sensitive personal data via the Internet or other insecure networks. The authentication method may for example be Nem-id, SMS token, Rfid, or similar methods.

3.3.8 The Data Processor shall take measures to ensure that only authorised users can get access to the personal data for which the individual in question is authorised.

3.3.9 The Data Processor shall enforce reasonable restrictions against physical access. Areas in which personal data is processed in accordance with the Main Agreement must be separated effectively from areas to which there is general access.

3.3.10 The Data Processor shall have established formal procedures for the handling of resetting of passwords and other situations in which the normal logical access control is inoperative.

3.3.11 On an ongoing basis and at least once every six months, controls shall be carried out to ensure that the users have been provided with the necessary access and authorisations. Such checks may for example involve creating statistics in the systems regarding the individual user’s use of the system in order to establish whether access and authorisations issued are still used.

3.3.12 The Data Processor shall without undue delay revoke authorisations and access for users who, according to a specific assessment, no longer need such authorisation and access.

3.4 Training and instruction

3.4.1 The Data Processor shall ensure that its employees receive adequate training and instructions in order to ensure that personal data is processed in accordance with relevant legislation and the policies and procedures of the Data Processor and the Data Controller.

3.5 Control of denied access and log-in attempts

3.5.1 All denied access attempts shall be recorded. If during a fixed period of time a maximum of three consecutive denied attempts have been registered with the same user identification, additional attempts by such user identification shall be blocked. Access shall not be given until the reason for the denied access attempts has been clarified.

3.5.2 Machine registration (logging) shall be carried out when processing identifiable information. The log shall as a minimum include information about time, user, type of use, and statement of the individual to which the information used related, or the search criterion used. The log shall be maintained for six months, after which it shall be erased unless a longer period is fixed in accordance with the purpose of the log with a view to using it as a tool in an investigation.

3.6 Input data material

3.6.1 Input data material shall only be used by individuals involved in the entry process. Input data material must be stored so that unauthorised people will not be able to familiarise themselves with the personal data included therein.

3.6.2 When it is no longer necessary to maintain the input data material, the Data Processor must erase or destroy it. The procedure shall be in accordance with best practice.

3.6.3 The stipulation regarding erasure or destruction of the material shall not apply if the material is covered by maintenance/discarding stipulations in accordance with other legislation, or if recorded material is processed in accordance with the general archive stipulations about maintenance, including the handing over of archives to the Danish State Archives.

3.7 Output data material

3.7.1 Output data material is covered by the same instructions as input data material with the following supplement:

3.7.2 Output data shall only be used by persons who are involved in the purposes for which the personal data is processed and in connection with auditing, technical maintenance, operation monitoring, and troubleshooting, etc.

3.8 Mobile storage media

3.8.1 Mobile storage media with personal data must be marked and stored with sufficiently strong encryption and under supervision or locked up when not in use.

3.8.2 Mobile storage media with personal data must only be handed over to authorised people with a view to performing audit or operational and system-technical tasks.

3.8.3 A list must be maintained of the mobile storage media used in connection with the data processing.

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

3.8.5 In connection with repair and service of data equipment containing personal data and sale and discarding of used data media, the necessary measures must be taken to ensure that personal data is not accidentally or deliberately destroyed, lost or deteriorated, or that the personal data is not disclosed to irrelevant parties, abused or otherwise processed contrary to current legislation. This shall be carried out in accordance with best practice.

3.9 Backup copies

3.9.1 Backup copies are covered by the same guidelines as any other processing of personal data in accordance with the present Agreement.

3.9.2 The Data Processor shall ensure that backup copies of systems and personal data are made regularly.

3.9.3 Backup copies must be stored separately from the server in a non-adjacent room to ensure that they are not lost, for example because of fire or flooding. Backup copies must at all times be stored safely to avoid loss thereof.

3.9.4 The Data Processor must check regularly that backup copies are legible. This must be done among other things with a view to emergency situations, for example in connection with major changes to the technical setup of a system.

3.10 Updates and changes

3.10.1 The Data Processor must have established formal procedures to ensure that updates of operating systems, databases, applications and other types of software are assessed and implemented within a reasonable period.

3.10.2 The Data Processor must have established formal procedures for the handling of changes with a view to ensuring that any change is appropriately authorised, tested and approved prior to implementation. The procedure must be supported by effective separation of duties or management follow-up to ensure that no individual is able to implement a change on his/her own.

3.11 Interruption of operations

3.11.1 The Data Processor must have documented emergency procedures to ensure re-establishment of services within a reasonable period in the event of interruption of operations.

3.12 Disposal of equipment

3.12.1 The Data Processor must have established formal processes in accordance with best practice and the demands made by the Data Controller in order to ensure effective erasure of personal data prior to the disposal of electronic equipment.

3.12.2 When equipment is disposed of, the Data Processor must document the procedure and be able to present such documentation when requested to do so.

3.13 Monitoring

3.13.1 The Data Processor must carry out and document monitoring of compliance by the Data Processor’s organisation with legislative requirements, policies, procedures and the present Data Processing Agreement with appendices.

Re 6. Ad hoc workplaces

6.1 The Data Processor must not carry out data processing from ad hoc workplaces (distance workplaces or home workplaces), unless clause 14 of the Data Processing Agreement includes a description of such workplaces.

6.1.1 The Data Controller must approve the use of ad hoc workplaces.

6.1.2 External communication connections must observe IT security text ST1 issued by the Danish Data Protection Agency.

6.1.3 Two-factor authentication must be used. The method of authentication may for example be Nem-id, SMS-token, Rfid or similar methods.

6.1.4 External IT communication may only be established if, after approval and in accordance with detailed agreement, measures are taken to ensure that unauthorised parties cannot get access to personal data through such connections.

6.1.5 The Data Processor must observe the guidelines issued by the Data Controller for the use of ad hoc workplaces.

Re 8. Notification and assistance

In case of breach of the personal data security, the Data Controller shall be notified without undue delay and in writing to enable the Data Controller to report the violation to the Danish Data Protection Agency and if necessary notify the Data Subjects. Notification shall be directed at:

[the Region’s contact’s information]