Version January 2023

SCHEDULE – DATA PROCESSING AGREEMENT

The following Data Processing Agreement (the "Data Processing Agreement") is applicable between Lessor and the Customer:

DEFINITIONS

Agreement	the agreement concluded between Lessor and the Customer, including Schedules and appendices.
Appendix	an appendix to the Data Processing Agreement.
Customer	The customer which has entered into an agreement with Lessor regarding use of Lessor's system(s).
Data Processing Agreement	this data processing agreement, including Appendices.
General Data Protection Regulation	Regulation (EU) 2016/679 of 27 April 2016.
Lessor	Lessor A/S, CVR-nr. 24240010, Engholm Parkvej 8, 3450 Allerød, Danmark.
Party	Lessor or the Customer.
Parties	Lessor and the Customer.
Personal Data	any information relating to an identified or identifiable natural person; see article 4(1) of the General Data Protection Regulation.
Schedule	a schedule to the Agreement.
System	the sub-system(s) covered by the Agreement.

1 SCOPE OF THE DATA PROCESSING AGREEMENT

1.1 Lessor is processor for the Customer as Lessor performs the processing activities specified in Appendix 1 on behalf of the Customer.

1.2 The Personal Data processed by Lessor, the purposes of the processing, the categories of Personal Data and the categories of data subjects are stated in Appendix 1.

1.3 The Data Processing Agreement only governs the processing of Personal Data performed by Lessor as processor on behalf of the Customer.

2 PROCESSING OF PERSONAL DATA

2.1 Lessor can only process Personal Data on documented instructions from the Customer, including with regard to transfers of Personal Data to a third country or an international organisation, unless required to do so by EU or Member State law to which Lessor is subject. In such a case, Lessor informs the Customer of that legal requirement before processing, unless the relevant law prohibits such information on important grounds of public interest.

2.2 Instructions: Lessor has been instructed to only process the Personal Data for the purpose of performing the processing activities specified in Appendix 1.

2.3 Lessor will immediately inform the Customer if, in Lessor's opinion, an instruction is infringing the General Data Protection Regulation or data protection provisions of other EU law or Member State law.

2.4 The Customer guarantees to Lessor that the Customer has the required right to process Personal Data subject to the Data Processing Agreement and to permit Lessor to process such Personal Data on its behalf, including without limitation by obtaining the relevant consents.

3 REQUIREMENTS FOR LESSOR

3.1 Lessor must process Personal Data in accordance with current Danish data protection legislation, including the General Data Protection Regulation.

3.2 Lessor must ensure that persons authorised to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory duty of confidentiality.

3.3 Lessor must take all measures required under article 32 of the General Data Protection Regulation, including implementing the appropriate technical and organisational security measures to ensure that the processed Personal Data

(i) are not accidentally or unlawfully destroyed, lost or changed;

(ii) are not disclosed or made available without authorisation; and

(iii) are not otherwise processed contrary to legislation, including the General Data Protection Regulation.

3.4 The appropriate technical and organisational security measures must be determined taking into account

(i) the state of the art;

(ii) costs of implementation; and

(iii) the nature, scope, context and purposes of the relevant processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

3.5 In connection with the above, Lessor must at least take the technical and organisational measures specified in Appendix 2 to the Data Processing Agreement.

3.6 At the Customer's request, Lessor must make available to the Customer all pieces of information necessary to demonstrate compliance with the obligations laid down in the Data Processing Agreement and allow for and contribute to audits under the Data Processing Agreement, including inspections conducted by the Customer or another auditor mandated by the Customer.

3.7 Each year, Lessor must, at its own expense, obtain a declaration by an independent expert on Lessor's compliance with the obligations laid down in the Data Processing Agreement in respect of the security measures. The declaration will be uploaded to Lessor's website www.lessor.dk annually. Lessor may change the website to which the declaration will be uploaded by giving written notice to the Customer.

3.8 In addition, the Customer is entitled to appoint an independent expert at the Customer's own expense who must be given access to such parts of Lessor's physical facilities where the processing of Personal Data takes place and to receive the information necessary to carry out the investigation into whether Lessor has implemented the appropriate technical and organisational security measures. The Customer's independent expert will not have access to information about Lessor's general cost structure or to information concerning Lessor's other customers. At Lessor's request, the expert must sign a usual non-disclosure agreement and, in any circumstance, treat any information obtained or received from Lessor confidentially and must only share such information with the Customer. The Customer must not disclose such information or use such information for other purposes than to determine whether Lessor has taken the appropriate technical and organisational security measures.

3.9 Lessor must give written notice to the Customer without undue delay after becoming aware of

(i) any public authority request for disclosure of Personal Data subject to the Data Processing Agreement unless notification of the Customer is prohibited under EU law or state law to which Lessor is subject;

(ii) any suspicion or identification of (a) a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed by Lessor under the Data Processing Agreement or (b) any other non-compliance with Lessor's obligations under clause 3.3; or

(iii) any request for access to the Personal Data received directly from the data subject or from a third party.

3.10 Taking into account the nature of the processing, Lessor must assist the Customer by appropriate technical and organisational measures, insofar as this is possible, with the fulfilment of the Customer's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the General Data Protection Regulation, including, e.g., requests for access, rectification, blocking or erasure.

3.11 Lessor must assist the Customer in ensuring compliance with the Customer's obligations under articles 32-36 of the General Data Protection Regulation taking into account the nature of processing and the information available to Lessor, and such other obligations imposed on the Customer by EU law or the legislation in a Member State in which Lessor's assistance is required, but only to the extent that Lessor's assistance is necessary for the Customer to comply with its obligations. This includes, *inter alia*, providing the Customer with any necessary information about an incident covered by clause 3.9(ii) and any information necessary to carry out a data protection impact assessment under articles 35-36 of the General Data Protection Regulation on request, to the extent that Lessor has access to such information.

3.12 In Appendix 1, Lessor has stated the physical location of servers, service centres, etc., involved in the data processing. Lessor undertakes to give prior written notice to the Customer of any change to such physical location. This will not require a formal amendment to Appendix 1; prior written notice will suffice.

3.13 The Customer will pay Lessor separately and based on hours spent and material used to process requests and tasks under clauses 3.6, 3.8, 3.9 (i) and (iii), 3.10, 3.11 and 5.4 of the Data Processing Agreement. Such payment will be determined according to Lessor's price list applicable from time to time and available on www.lessor.dk or on another website designated by Lessor.

4 SUB-PROCESSORS

4.1 The Customer gives Lessor a prior, general, written approval for the use of sub-processors. At the date of the Data Processing Agreement, Lessor is using the sub-processors listed in Appendix 3. Lessor must give written notice to the Customer of any planned changes in terms of adding or replacing sub-processors no later than 2 months before the change takes effect. The Customer will then be entitled to object to the change without specifying any reason within 2 weeks from the date of the notice of the change by refusing to use the new sub-processor. In that case, Lessor will be entitled to terminate all agreements with the Customer under which Lessor is processing Personal Data on behalf of the Customer, by giving 2 months' notice.

4.2 Before using a sub-processor, Lessor must conclude a written agreement with the sub-processor imposing at least the same obligations as those undertaken by Lessor under the Data Processing Agreement, including the obligation to implement appropriate technical and organisational measures for ensuring that the processing meets the requirements of the General Data Protection Regulation.

4.3 The Customer is entitled to receive a copy of such parts of Lessor's agreement with a sub-processor that concern mandatory data protection obligations under clause 4.2.

4.4 Where a sub-processor fails to fulfil its data protection obligations, Lessor will remain fully liable to the Customer for the performance of that sub-processor's obligations.

5 TERM AND TERMINATION OF THE DATA PROCESSING AGREEMENT

5.1 The Data Processing Agreement takes effect at the same time as the Agreement to which the Data Processing Agreement is a Schedule and will remain in effect until the termination of the Agreement.

5.2 Either Party may terminate the Data Processing Agreement on the same terms and conditions as those applicable to the Agreement to which the Data Processing Agreement is a Schedule.

5.3 Irrespective of the formal term of the Data Processing Agreement, the Data Processing Agreement will remain in effect for as long as Lessor is processing Personal Data as a processor on behalf of the Customer for which the Customer is the controller.

5.4 At the choice of the Customer, Lessor must delete or return all the Personal Data to the Customer after the termination of the Agreement and delete existing copies unless EU or Member State law requires storage of the Personal Data.

6 NOTICES

6.1 If a Party is required under the Data Processing Agreement to give written notice to the other Party, such obligations may be fulfilled by sending an email to the email address most recently stated by such other Party.

7 PREVAILING DOCUMENT

7.1 In case of a discrepancy between the provisions of the Data Processing Agreement and the provisions of other written or oral agreements between the Parties, the provisions of the Data Processing Agreement will prevail unless otherwise expressly agreed between the Parties.

APPENDIX 1

This Appendix contains, *inter alia*, the Customer's instructions in respect of Lessor's data processing on behalf of the Customer and is an integral part of the Data Processing Agreement. The instructions depend on which software is covered by the Customer's agreement with Lessor and to which the Customer has, therefore, been granted licences as further described under each sub-system below.

If, as part of the Agreement, Lessor is hosting the System, the Customer's instruction as set out below also includes that the Personal Data are processed for such hosting purposes. If data are not hosted by Lessor, Lessor will only have access to and process data following special agreements in that respect with the Customer; this will typically be the case in connection with remote support and/or consultancy work, but it may also be in the course of operation of a VPN tunnel or other matters subject to agreement.

Processing of Personal Data and instructions for LessorRefusion:

Purpose and nature of data processing in LessorRefusion

The purpose of having Lessor carry out the data processing is to let the Customer use LessorRefusion and its features and to provide support and consultancy services for such use. LessorRefusion is the Customer's tool to report and claim payment of reimbursement based on employees' absence due to sickness and maternity/paternity leave. The Customer may also see expected reimbursements and received reimbursements and the status of reimbursement claims.

The Customer may synchronise employees' absence from Lessor-Portal, Lessor-SP Tid or enter the first day of absence directly into LessorRefusion.

Categories of data subjects whose data are processed

(a) The persons whose data the Customer enters into LessorRefusion to the extent that Lessor is given access to such data in connection with specific tasks performed by Lessor for the Customer (including employees and/or former employees at the Customer and/or at other entities for whom the Customer has the right to use the System)

Categories of Personal Data processed

Re (a) CPR number, name, address, employment, absence entries, leave entries, pay data, login details (encrypted and birthdates of newborn children)

Processing of Personal Data and instructions for Lessor Payroll, Lessor Time & Attendance and Lessor Human Resources for Microsoft Dynamics

Purpose and nature of data processing in Lessor Payroll, Lessor Time & Attendance and Lessor Human Resources for Microsoft Dynamics

The purpose of having Lessor carry out the data processing is to provide support and/or consultancy services to the Customer in connection with the Customer's use of Lessor's Microsoft Dynamics software. Lessor may need access to and extracts from the Customer's environment and thereby Personal Data contained therein to be able to perform such tasks. The Personal Data are processed for the purpose of providing support and/or consultancy services requested by the Customer. It should be noted that the software is not hosted by Lessor, but by the Customer or a third party. The process relating to such assistance may begin with the Customer's request for assistance to the partner with whom the Customer has concluded the agreement, such partner then involves Lessor in the relevant assistance, whereby Lessor receives the relevant Personal Data from the partner instead of the Customer. Data may be synchronised with Lessor-Portal or other external systems supporting Lessor Integration Framework (LIF).

Categories of data subjects whose data are processed

(a) The persons whose data the Customer enters into the products developed by Lessor for Microsoft Dynamics to the extent that Lessor is given access to such data in connection with specific tasks performed by Lessor for the Customer (including employees and/or former employees at the Customer and/or at other entities for whom the Customer has the right to use the System).

Categories of Personal Data processed

Re (a) The data about individuals entered into the systems by the Customer, e.g. but not necessarily limited to: CPR number, name, address, age, gender, job title, civil status, telephone numbers, email address, employment, absence entries, leave entries, pay data, pension data, tax card details, family members, memberships, competences, industrial injuries, education and courses, citizenship, personal documents, login details (encrypted) and all data reported to the System by the Customer.

Processing of Personal Data and instructions for Lessor-4

Purpose and nature of data processing in Lessor-4

The purpose of having Lessor carry out the data processing is to let the Customer use Lessor-4 and its features and to provide support and consultancy services for such use. Lessor-4 is used for paying out pay and pension. It is possible to make entries such as transport, variable components of pay, absence and employee data. It is also possible to feed in data from external systems. Data may be synchronised with Lessor-Portal, Lessor's time systems or HR systems or other external systems supporting Lessor Integration Framework (LIF). Payslips may be sent to e-Boks, if elected. Payments may be transferred via Nets or a bank, at the Customer's option.

Categories of data subjects whose data are processed in Lessor-4

(a) The persons whose data the Customer enters into Lessor-4 to the extent that Lessor is given access to such data in connection with specific tasks performed by Lessor for the Customer (including employees and/or former employees at the Customer and/or at other entities for whom the Customer has the right to use the System).

Categories of Personal Data processed in Lessor-4

Re (a) CPR number, name, address, age, gender, job title, civil status, telephone numbers, email address, employment, absence entries, leave entries, pay data, pension data, tax card details, family members, memberships, competences, industrial injuries, education and courses, citizenship, personal documents, login details (encrypted) and all data reported to the System by the Customer.

Processing of Personal Data and instructions for Lessor4 Tid

Purpose and nature of data processing in Lessor4 Tid

The purpose of having Lessor carry out the data processing is to let the Customer use Lessor4 Tid and its features and to provide support and consultancy services for such use. Lessor4 Tid is an online time recording solution used by employees, managers and administrative functions for staff scheduling and recording variable components of pay, absence and time recording. Users may use the System via a Windows client, a web browser, an app or an industrial terminal. The employees can see and, if relevant, update their own master data. Data may be exchanged with Lessor's other payroll, staff scheduling and HR systems, and there is a possibility of integration with third-party systems via XML or file exchange. The managers may approve or reject data entries and changes before exchanging variable components of pay.

Categories of data subjects whose data are processed in Lessor4 Tid

(a) The persons whose data the Customer enters into Lessor4 Tid to the extent that Lessor is given access to such data in connection with specific tasks performed by Lessor for the Customer (including employees and/or former employees at the Customer and/or at other entities for whom the Customer has the right to use the System)

Categories of Personal Data processed in Lessor4 Tid

Re (a) CPR number, name, address, gender, telephone numbers, email address, employment, job title, contact details, relatives, absence entries, balances, staff schedules, coming/going entries, competences, sickness absence interview details, personal documents, login details (encrypted) and all data reported to the System by the Customer.

Processing of Personal Data and instructions for LessorLøn

Purpose and nature of data processing in LessorLøn

The purpose of having Lessor carry out the data processing is to let the Customer use LessorLøn and its features and to provide support and consultancy services for such use. LessorLøn is used for paying out pay and pension, budgeting, and supporting the HR functions of the business. It is possible to make entries such as transport, variable components of pay, absence and HR data. It is also possible to feed in data from external systems. Data may be synchronised with Lessor-Portal, Lessor's time systems or HR systems or other external systems supporting Lessor Integration Framework (LIF). LessorLøn has an integration with the Danish Tax and Customs Administration (SKAT) and the Danish Civil Registration System to and from which data may be sent. Payslips will be sent to e-Boks, if elected. Payments may be transferred via Nets.

Categories of data subjects whose data are processed in LessorLøn

(a) The persons whose data the Customer enters into LessorLøn to the extent that Lessor is given access to such data in connection with specific tasks performed by Lessor for the Customer (including employees and/or former employees at the Customer and/or at other entities for whom the Customer has the right to use the System)

Categories of Personal Data processed in LessorLøn

Re (a) CPR number, name, address, age, gender, job title, civil status, telephone numbers, email address, employment, absence entries, leave entries, pay data, pension data, tax card details, family members, memberships, competences, industrial injuries, education and courses, citizenship, personal documents, login details (encrypted) and all data reported to the System by the Customer.

Processing of Personal Data and instructions for Lessor-PM

Purpose and nature of data processing in Lessor-PM

The purpose of having Lessor carry out the data processing is to let the Customer use Lessor-PM and its features and to provide support and consultancy services for such use. Lessor-PM is used for paying out pay and supporting the HR functions of the business. It is possible to make entries such as transport, variable components of pay, absence and HR data. It is also possible to feed in data from external systems. Data may be synchronised with Lessor-Portal, time systems and HR systems or other external systems supporting Lessor Integration Framework (LIF). Lessor-PM has the possibility of integration with the Danish Tax Agency to and from which data may be sent. Payslips may be sent to e-Boks, if elected. The Customer may transfer payments to Nets or a bank.

Categories of data subjects whose data are processed in Lessor-PM

(a) The persons whose data the Customer enters into Lessor-PM to the extent that Lessor is given access to such data in connection with specific tasks performed by Lessor for the Customer (including employees and/or former employees at the Customer and/or at other entities for whom the Customer has the right to use the System)

(b) Applicants for the Customer's job vacancies

Categories of Personal Data processed in Lessor-PM

Re (a) CPR number, name, address, age, gender, job title, civil status, telephone numbers, email address, employment, absence entries, pay data, pension data, tax card details, family members, memberships, competences, industrial injuries, education and courses, citizenship, personal documents, login details (encrypted) and all data reported to the System by the Customer.

Re (b) CPR number, name, address, age, gender, job title, civil status, telephone numbers, email address, CV, applications and all data reported to the System by the Customer.

Processing of Personal Data and instructions for Lessor-Portal

Purpose and nature of data processing in Lessor-Portal

The purpose of having Lessor carry out the data processing is to let the Customer use Lessor-Portal and its features and to provide support and consultancy services for such use. Lessor-Portal is used as an employee self-service and management portal for entries such as transport, variable components of pay, absence, coming/going data and travel costs. The employees can also see and, if relevant, update their own master data. Data may be synchronised with Lessor's payroll systems, time systems or HR systems. The managers may approve or reject data entries and changes before synchronising data.

Categories of data subjects whose data are processed in Lessor-Portal

(a) The persons whose data the Customer enters into Lessor-Portal to the extent that Lessor is given access to such data in connection with specific tasks performed by Lessor for the Customer (including employees and/or former employees at the Customer and/or at other entities for whom the Customer has the right to use the System)

Categories of Personal Data processed in Lessor-Portal

Re (a) Employment, CPR number, name, job title, contact details, payslips, absence data, transport data, coming/going data, travel data, competences, education, relatives, personal documents, login details (encrypted) and all data reported to the System by the Customer.

Re (b) Employment, CPR number, name, job title, contact details, payslips, absence data, transport data, coming/going data, travel data, competences, education, relatives, personal documents, login details (encrypted) and all data reported to the System by the Customer.

Processing of Personal Data and instructions for Lessor-SP Tid

Purpose and nature of data processing in Lessor-SP Tid

The purpose of having Lessor carry out the data processing is to let the Customer use Lessor-SP Tid and its features and to provide support and consultancy services for such use. Lessor-SP Tid is an online time recording solution used by employees, managers and administrative functions for staff scheduling and recording variable components of pay, absence and time recording. Users may use the System via a Windows client, a web browser, an app or an industrial terminal. The employees can see and, if relevant, update their own master data. Data may be exchanged with Lessor's other payroll, staff scheduling and HR systems, and there is a possibility of integration with third-party systems via XML or file exchange. The managers may approve or reject data entries and changes before exchanging variable components of pay. Data may be synchronised with Lessor-Portal.

Categories of data subjects whose data are processed in Lessor-SP Tid

(a) The persons whose data the Customer enters into Lessor-SP Tid to the extent that Lessor is given access to such data in connection with specific tasks performed by Lessor for the Customer (including employees and/or former employees at the Customer and/or at other entities for whom the Customer has the right to use the System)

Categories of Personal Data processed in Lessor-SP Tid

Re (a)

CPR number, name, address, gender, telephone numbers, email address, employment, job title, contact details, relatives, absence entries, balances, staff schedules, coming/going entries, competences, sickness absence interview details, personal documents, login details (encrypted) and all data reported to the System by the Customer.

Processing of Personal Data and instructions for LessorWorkforce

Purpose and nature of data processing in LessorWorkforce

The purpose of having Lessor carry out the data processing is to let the Customer use LessorWorkforce and its features and to provide support and consultancy services for such use. LessorWorkforce is an online staff scheduling solution used by employees, managers and administrative functions for staff scheduling and recording variable components of pay, absence and time recording. Users may use the System via a web browser or an app. The employees can see and, if relevant, update their own master data. Data may be exchanged with Lessor's other payroll, time and HR systems, and there is a possibility of integration with third-party systems via a web service. The managers may approve or reject data entries and changes before exchanging variable components of pay.

Categories of data subjects whose data are processed in LessorWorkforce

(a) The persons whose data the Customer enters into LessorWorkforce to the extent that Lessor is given access to such data in connection with specific tasks performed by Lessor for the Customer (including employees and/or former employees at the Customer and/or at other entities for whom the Customer has the right to use the System)

Categories of Personal Data processed in LessorWorkforce

Re (a)

Employment, CPR number, name, job title, contact details, absence data, staff schedules, coming/going data, competences, personal documents and all data reported to the System by the Customer.

Processing locations

Engholm Parkvej 8, 3450 Allerød, Denmark
Industriparken 35, 2750 Ballerup, Denmark
Holmbladsgade 142, 2300 København S, Denmark

Please also refer to the list of existing sub-processors below.

Disclosure of data

Depending on the system used by the Customer, and if Lessor is hosting the system used by the Customer, Lessor may disclose Personal Data on behalf of the Customer in the course of Lessor's provision of services to the Customer, including, e.g., to the Danish Tax Agency, pension companies, Nets, Statistics Denmark, KOMBIT, etc.

Version January 2023

APPENDIX 2

Introduction

Lessor is using a risk-based approach to IT security and to the protection of the Personal Data that we process about our Customers and our Customers' employees. Lessor has taken the required technical and organisational security measures to mitigate the risks relating to the processing of Personal Data in Lessor's systems in respect of which Lessor is acting as processor for the Customer. Lessor will always at least take the technical and organisational measures below, but may, at any time, upgrade the level of security and the measures related thereto if the risk scenario changes.

Since Lessor's solutions are provided as SaaS solutions hosted by Lessor and/or on-premise solutions hosted by the Customer, the description below of Lessor's security measures is divided into those two types of solutions.

Re (a) The following security measures apply to SaaS solutions hosted by Lessor in relation to processing of Personal Data:

Physical security at Lessor's premises and data centres

Lessor has established access security allowing only authorised persons to gain access to premises and data centres where Personal Data are stored and processed. External consultants and other visitors will only have access to data centres if they are accompanied by an authorised employee.

Lessor's facilities and data centres are under video surveillance.

Alarm systems have been installed at Lessor's premises and data centres which can be accessed only with a key or access card and code.

The data centres are equipped with a cooling system, redundant power supply, fire protection, fibre network and a monitoring system.

Logging

All network traffic and server logs are monitored and logged.

The following is logged in systems, databases and networks:

- all access attempts;
- all searches; and
- activities performed by systems administrators and others having special rights;
- security incidents, including (i) deactivation of logging; (ii) change of system rights; and (iii) failed login attempts.

Lessor does not operate with shared login which means that it is always possible to identify the employee performing an activity.

The relevant log files are stored and protected against manipulation and technical errors. The log files are checked on a regular basis to ensure normal operations and to examine accidental events or incidents.

Antivirus and firewalls

Any external access to systems and databases used to process Personal Data goes through a secure firewall with a restrictive protocol.

A port and IP address filter has been set up to ensure restricted access to ports and specific IP addresses.

To prevent hostile attacks, antivirus software and Intrusion Prevention System (IPS) have been installed on all systems and databases used to process Personal Data. The antivirus software used is updated regularly.

XSS and SQL injection protection has been implemented in all services.

Only authorised persons can access Lessor's internal network.

Encryption

An algorithm-based encryption is used for transmission of Personal Data via the Internet and/or email.

The Customer's User ID (user name) and password are encrypted using an algorithm.

Back-up and accessibility

The technical measures and Lessor's systems are tested regularly using vulnerability scans and penetration tests.

All changes of systems, databases and networks follow Change Management procedures laid down to ensure that they are maintained with relevant updates and patches, including security patches.

System monitoring is performed on all systems used in the processing of Personal Data.

The data environment is monitored for vulnerabilities and any identified problems are cured.

Backups are made to ensure that all systems and data, including Personal Data, may be restored if they are lost or changed.

Authorisation, access restrictions and security

Only employees having a work-related need will have access to Personal Data. All assessments of an employee's work-related need are made based on a need-to-have approach to ensure respect for the principle of data minimisation. The employee's access is re-assessed regularly.

Employees are trained in awareness on a regular basis in relation to IT security and security of processing of Personal Data. All employees are informed of the written information security policy approved by the management.

All new employees are screened. On employment, the employees sign a non-disclosure agreement. Further, new employees are introduced to the information security policy and to the procedures for processing of the Personal Data within the employee's responsibilities.

Procedures have been laid down to ensure that user rights granted to employees are taken away from them when they leave the company.

Lessor has implemented a password policy that helps ensure (i) that employees' passwords do not fall into the hands of unauthorised persons; (ii) that only sufficiently complex passwords are approved; and (iii) that passwords are changed on a regular basis.

Protection has been set up for portable devices. Employees' laptops are protected, *inter alia*, by encryption and passwords at hard drive level. A VPN connection and a two-factor authentication are used for remote access.

External persons moving about at Lessor's locations and data centres where there may be access to Personal Data are informed of Lessor's security rules and must sign a non-disclosure agreement.

Control

Lessor carries out internal audits and controls of the laid down technical and organisational security measures based on the controls set out in the recognised ISO 27002 standard. The ISO 27002 standard is used to ensure control of the implementation of the Information Security Management System ("ISMS") used by Lessor for risk management in determining the necessary safety measures.

Moreover, an independent auditor will prepare an annual ISAE 3402 audit opinion. The ISAE 3402 audit opinion focuses on whether Lessor has set up and maintains an adequate level of IT security.

Re (b) The following security measures apply to on-premise solutions in relation to Lessor's processing of Personal Data as a processor:

Security measures relating to specific remote support

Initially, Lessor will take the necessary measures to ensure that the request is made by the relevant Customer. All requests are registered in Lessor's processing system.

Most requests may be dealt with in a support call between the Customer and the support consultant. If a support consultant needs to access the Customer's system and the Customer's platform allows for direct access, the support consultant may use remote access to service the Customer's systems. Remote access requires specific approval by the Customer as the Customer has to approve that the support consultant takes control of the Customer's screen, keyboard and mouse. During remote access, the Customer can see all actions taken by the support consultant on the Customer's screen. Encrypted communication is used during remote access.

To enable Lessor to troubleshoot Lessor's test environment, the Customer may transmit extracts of data sets from the System or send screenshots from the System to Lessor. Lessor recommends only to transmit data sets and screenshots to Lessor in encrypted files through encrypted connections as the data sets may contain confidential Personal Data for which the Danish Data Protection Agency has laid down requirements for encryption. Lessor will make a file sharing tool available for encrypted transmission of data.

Authorisation and access restrictions

Only support consultants having a work-related need will have access to Personal Data in connection with support issues. All assessments of a support consultant's work-related need are made based on a need-to-have approach to ensure respect for the principle of data minimisation.

Support consultants are trained in awareness on a regular basis in relation to IT security and security of processing of Personal Data. All support consultants are informed of the information security policy approved by the management.

All new support consultants are screened. On employment, the support consultants sign a non-disclosure agreement. Further, new support consultants are introduced to the information security policy and to the procedures for processing of the Personal Data within the support consultant's responsibilities.

Procedures have been laid down to ensure that user rights granted to support consultants are taken away from them when they leave the company.

Lessor has implemented a password policy that helps ensure (i) that employees' passwords do not fall into the hands of unauthorised persons; (ii) that only sufficiently complex passwords are approved; and (iii) that passwords are changed on a regular basis.

Protection has been set up for portable devices. Support consultants' laptops are protected, *inter alia*, by encryption and passwords at hard drive level. A VPN connection and a two-factor authentication are used for remote access.

External persons moving about at Lessor's locations and data centres where there may be access to Personal Data are informed of Lessor's security rules and must sign a non-disclosure agreement. In addition, Lessor operates with a clean-desk policy.

Physical security

Lessor has established physical access security allowing only authorised persons to gain access to Lessor's premises and data centres where Personal Data are stored and processed. External consultants and other visitors will only have access to data centres if they are accompanied by an authorised employee.

Lessor's facilities are under video surveillance.

Alarm systems have been installed at Lessor's premises which can be accessed only with a key or access card and code.

Antivirus and firewalls

Any external access to systems used to process Personal Data goes through a secure firewall with a restrictive protocol.

A port and IP address filter has been set up to ensure restricted access to ports and specific IP addresses.

To prevent hostile attacks, antivirus software and Intrusion Prevention System (IPS) have been installed on all systems used to process Personal Data. The antivirus software used is updated regularly.

XSS and SQL injection protection has been implemented in all services.

Only authorised persons can access Lessor's internal network.

APPENDIX 3 – list of existing sub-processors

Sub-processor	**Location(s)**	**Processing**
Post Danmark A/S	Hedegaardvej 88 2300 København S, Denmark	If the Customer's solution is hosted by Lessor, Lessor is collaborating with Post Danmark A/S who, if so agreed with the Customer, makes it possible to distribute payslips via e-Boks.
Compaya A/S	Palægade 4, 2. tv 1261 København K, Denmark	If the System is used to send text messages to the Customer's employees, Lessor is collaborating with Compaya A/S who is responsible for sending text messages.
Emply International ApS	Lyngbyvej 102 2100 København Ø, Denmark	If the Customer uses an Emply solution, Lessor collaborates with Emply International ApS.
InterLogic Danmark ApS	Ellestien 7 8250 Egå, Denmark Dok 1 80-958 Gdańsk, Poland	If Lessor makes use of its external consultant for the purpose of managing/solving certain support tickets, and such support tickets contain Personal Data.
NetNordic Danmark A/S	Lyskær 1 DK2730 Herlev, Denmark Råsundavägen 4, 5TR, 16967 Solna, Sweden	If the Customer's solution is hosted by Lessor, Lessor is collaborating with NetNordic Denmark A/S who is hosting backup data.