Version November 2023

Schedule 2

Lessor data processing agreement

Standard Contractual Clauses

For the purposes of Article 28(3) of Regulation 2016/679 (the GDPR)

between

[NAME]
CVR [CVR-NO]
[POSTCODE AND CITY]
[COUNTRY]

hereafter the "data controller" or the "Customer"

and

Lessor A/S
CVR 24240010
Engholm Parkvej 8
3450 Allerød
Denmark

hereafter the "data processor" or "Lessor"

each a 'party'; together 'the parties'

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to meet the requirements of the GDPR and to ensure the protection of the rights of the data subject.

1. Table of Contents

2. Preamble

1. These Contractual Clauses (the Clauses) set out the rights and obligations of the data controller and the data processor, when processing personal data on behalf of the data controller.

2. The Clauses have been designed to ensure the parties' compliance with Article 28(3) of Regulation 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).

3. In the context of the provision of the System, the data processor will process personal data on behalf of the data controller in accordance with the Clauses.

4. The Clauses shall take priority over any similar provisions contained in other agreements between the parties.

5. Four appendices are attached to the Clauses and form an integral part of the Clauses.

6. Appendix A contains details about the processing of personal data, including the purpose and nature of the processing, type of personal data, categories of data subject and duration of the processing.

7. Appendix B contains the data controller's conditions for the data processor's use of sub-processors and a list of sub-processors authorised by the data controller.

8. Appendix C contains the data controller's instructions with regards to the processing of personal data, the minimum security measures to be implemented by the data processor and how audits of the data processor and any sub-processors are to be performed.

9. Appendix D contains provisions for other activities which are not covered by the Clauses.

10. The Clauses along with appendices shall be retained in writing, including electronically, by both parties.

11. The Clauses shall not exempt the data processor from obligations to which the data processor is subject pursuant to the General Data Protection Regulation (the GDPR) or other legislation.

3. The rights and obligations of the data controller

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

2. The data controller has the right and obligation to make decisions about the purposes and means of the processing of personal data.

3. The data controller shall be responsible, among other, for ensuring that the processing of personal data, which the data processor is instructed to perform, has a legal basis.

[1] References to "Member States" made throughout the Clauses shall be understood as references to "EEA Member States".

4. The data processor acts according to instructions

1. The data processor shall process personal data only on documented instructions from the data controller, unless required to do so by Union or Member State law to which the processor is subject. Such instructions shall be specified in appendices A and C. Subsequent instructions can also be given by the data controller throughout the duration of the processing of personal data, but such instructions shall always be documented and kept in writing, including electronically, in connection with the Clauses.

2. The data processor shall immediately inform the data controller if instructions given by the data controller, in the opinion of the data processor, contravene the GDPR or the applicable EU or Member State data protection provisions.

5. Confidentiality

1. The data processor shall only grant access to the personal data being processed on behalf of the data controller to persons under the data processor's authority who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and only on a need to know basis. The list of persons to whom access has been granted shall be kept under periodic review. On the basis of this review, such access to personal data can be withdrawn, if access is no longer necessary, and personal data shall consequently not be accessible anymore to those persons.

2. The data processor shall at the request of the data controller demonstrate that the concerned persons under the data processor's authority are subject to the abovementioned confidentiality.

6. Security of processing

1. Article 32 GDPR stipulates 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, the data controller and data processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

   The data controller shall evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. Depending on their relevance, the measures may include the following:

   a. Pseudonymisation and encryption of personal data;

   b. the ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services;

   c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

   d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. According to Article 32 GDPR, the data processor shall also – independently from the data controller – evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. To this effect, the data controller shall provide the data processor with all information necessary to identify and evaluate such risks.

3. Furthermore, the data processor shall assist the data controller in ensuring compliance with the data controller's obligations pursuant to Articles 32 GDPR, by *inter alia* providing the data controller with information concerning the technical and organisational measures already implemented by the data processor pursuant to Article 32 GDPR along with all other information necessary for the data controller to comply with the data controller's obligation under Article 32 GDPR.

   If subsequently – in the assessment of the data controller – mitigation of the identified risks require further measures to be implemented by the data processor, than those already implemented by the data processor pursuant to Article 32 GDPR, the data controller shall specify these additional measures to be implemented in Appendix C.

7. Use of sub-processors

1. The data processor shall meet the requirements specified in Article 28(2) and (4) GDPR in order to engage another processor (a sub-processor).

2. The data processor shall therefore not engage another processor (sub-processor) for the fulfilment of the Clauses without the prior general written authorisation of the data controller.

3. The data processor has the data controller's general authorisation for the engagement of sub-processors. The data processor shall inform in writing the data controller of any intended changes concerning the addition or replacement of sub-processors at least **2 months** in advance, thereby giving the data controller the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s). Longer time periods of prior notice for specific sub-processing services can be provided in Appendix B. The list of sub-processors already authorised by the data controller can be found in Appendix B.

4. Where the data processor engages a sub-processor for carrying out specific processing activities on behalf of the data controller, the same data protection obligations as set out in the Clauses shall be imposed on that sub-processor by way of a contract or other legal act under EU or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the Clauses and the GDPR.

   The data processor shall therefore be responsible for requiring that the sub-processor at least complies with the obligations to which the data processor is subject pursuant to the Clauses and the GDPR.

5. A copy of such a sub-processor agreement and subsequent amendments shall – at the data controller's request – be submitted to the data controller, thereby giving the data controller the opportunity to ensure that the same data protection obligations as set out in the Clauses are imposed on the sub-processor. Clauses on business related issues that do not affect the legal data protection content of the sub-processor agreement, shall not require submission to the data controller.

6. The data processor shall agree a third-party beneficiary clause with the sub-processor where – in the event of bankruptcy of the data processor – the data controller shall be a third-party beneficiary to the sub-processor

agreement and shall have the right to enforce the agreement against the sub-processor engaged by the data processor, e.g. enabling the data controller to instruct the sub-processor to delete or return the personal data.

7. If the sub-processor does not fulfil his data protection obligations, the data processor shall remain fully liable to the data controller as regards the fulfilment of the obligations of the sub-processor. This does not affect the rights of the data subjects under the GDPR – in particular those foreseen in Articles 79 and 82 GDPR – against the data controller and the data processor, including the sub-processor.

8. Transfer of data to third countries or international organisations

1. Any transfer of personal data to third countries or international organisations by the data processor shall only occur on the basis of documented instructions from the data controller and shall always take place in compliance with Chapter V GDPR.

2. In case transfers to third countries or international organisations, which the data processor has not been instructed to perform by the data controller, is required under EU or Member State law to which the data processor is subject, the data processor shall inform the data controller of that legal requirement prior to processing unless that law prohibits such information on important grounds of public interest.

3. Without documented instructions from the data controller, the data processor therefore cannot within the framework of the Clauses:

    a. transfer personal data to a data controller or a data processor in a third country or in an international organization

    b. transfer the processing of personal data to a sub-processor in a third country

    c. have the personal data processed in by the data processor in a third country

4. The data controller's instructions regarding the transfer of personal data to a third country including, if applicable, the transfer tool under Chapter V GDPR on which they are based, shall be set out in Appendix C.6.

5. The Clauses shall not be confused with standard data protection clauses within the meaning of Article 46(2)(c) and (d) GDPR, and the Clauses cannot be relied upon by the parties as a transfer tool under Chapter V GDPR.

9. Assistance to the data controller

1. Taking into account the nature of the processing, the data processor shall assist the data controller by appropriate technical and organisational measures, insofar as this is possible, in the fulfilment of the data controller's obligations to respond to requests for exercising the data subject's rights laid down in Chapter III GDPR.

    This entails that the data processor shall, insofar as this is possible, assist the data controller in the data controller's compliance with:

    a. the right to be informed when collecting personal data from the data subject
    b. the right to be informed when personal data have not been obtained from the data subject
    c. the right of access by the data subject

d. the right to rectification
e. the right to erasure ('the right to be forgotten')
f. the right to restriction of processing
g. notification obligation regarding rectification or erasure of personal data or restriction of processing
h. the right to data portability
i. the right to object
j. the right not to be subject to a decision based solely on automated processing, including profiling

2. In addition to the data processor's obligation to assist the data controller pursuant to Clause 6.3., the data processor shall furthermore, taking into account the nature of the processing and the information available to the data processor, assist the data controller in ensuring compliance with:

   a. The data controller's obligation to without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority, the **Danish Data Protection Agency**, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons;

   b. the data controller's obligation to without undue delay communicate the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons;

   c. the data controller's obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a data protection impact assessment);

   d. the data controller's obligation to consult the competent supervisory authority, the **Danish Data Protection Agency**, prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the data controller to mitigate the risk.

3. The parties shall define in Appendix C the appropriate technical and organisational measures by which the data processor is required to assist the data controller as well as the scope and the extent of the assistance required. This applies to the obligations foreseen in Clause 9.1. and 9.2.

10. Notification of personal data breach

1. In case of any personal data breach, the data processor shall, without undue delay after having become aware of it, notify the data controller of the personal data breach.

2. The data processor's notification to the data controller shall, if possible, take place within **48 hours** after the data processor has become aware of the personal data breach to enable the data controller to comply with the data controller's obligation to notify the personal data breach to the competent supervisory authority, cf. Article 33 GDPR.

3. In accordance with Clause 9(2)(a), the data processor shall assist the data controller in notifying the personal data breach to the competent supervisory authority, meaning that the data processor is required to assist in obtaining the information listed below which, pursuant to Article 33(3)GDPR, shall be stated in the data controller's notification to the competent supervisory authority:

a. The nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

b. the likely consequences of the personal data breach;

c. the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. The parties shall define in Appendix C all the elements to be provided by the data processor when assisting the data controller in the notification of a personal data breach to the competent supervisory authority.

11. Erasure and return of data

1. On termination of the provision of personal data processing services, the data processor shall be under obligation to delete all personal data processed on behalf of the data controller and certify to the data controller that it has done so unless Union or Member State law requires storage of the personal data.

12. Audit and inspection

1. The data processor shall make available to the data controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 and the Clauses and allow for and contribute to audits, including inspections, conducted by the data controller or another auditor mandated by the data controller.

2. Procedures applicable to the data controller's audits, including inspections, of the data processor and sub-processors are specified in appendices C.7. and C.8.

3. The data processor shall be required to provide the supervisory authorities, which pursuant to applicable legislation have access to the data controller's and data processor's facilities, or representatives acting on behalf of such supervisory authorities, with access to the data processor's physical facilities on presentation of appropriate identification.

13. The parties' agreement on other terms

1. The parties may agree other clauses concerning the provision of the personal data processing service specifying e.g. liability, as long as they do not contradict directly or indirectly the Clauses or prejudice the fundamental rights or freedoms of the data subject and the protection afforded by the GDPR.

14. Commencement and termination

1. The Clauses shall become effective on the date of both parties' signature.

2. Both parties shall be entitled to require the Clauses renegotiated if changes to the law or inexpediency of the Clauses should give rise to such renegotiation.

3. The Clauses shall apply for the duration of the provision of personal data processing services. For the duration of the provision of personal data processing services, the Clauses cannot be terminated unless other Clauses governing the provision of personal data processing services have been agreed between the parties.

4. If the provision of personal data processing services is terminated, and the personal data is deleted or returned to the data controller pursuant to Clause 11.1. and Appendix C.4., the Clauses may be terminated by written notice by either party.

5. Signature

On behalf of the data controller

Name	[NAME]
Position	[POSITION]
Date	[DATE]
Signature	[SIGNATURE]

On behalf of the data processor

Name	[NAME]
Position	[POSITION]
Date	[DATE]
Signature	[SIGNATURE]

15. Data controller and data processor contact points

1. The parties may contact each other using the following contacts/contact points:

2. The parties shall be under obligation continuously to inform each other of changes to contacts/contact points.

On behalf of the data controller

Name	[NAME]
Position	[POSITION]
Telephone	[TELEPHONE]
E-mail	[E-MAIL]

On behalf of the data processor

Name	[NAME]
Position	[POSITION]
Telephone	[TELEPHONE]
E-mail	[E-MAIL]

Appendix A - Information about the processing

A.1. The purpose of the data processor's processing of personal data on behalf of the data controller is:

The purpose of having the data processor carrying out the data processing is to let the data controller use the System and its features and to provide support and consultancy services in connection with the implementation and day-to-day operations etc. of the System.

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.

A.2. The data processor's processing of personal data on behalf of the data controller shall mainly pertain to (the nature of the processing):

Storage of and access to personal data.

A.3. The processing includes the following types of personal data about data subjects:

System(s)	Types of personal data
LessorRefusion	CPR number, name, address, employment, absence entries, leave entries, pay data, login details (encrypted and birthdates of newborn children)
Lessor Payroll, Lessor Time & Attendance and Lessor Human Resources for Microsoft Dynamics	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.
Lessor4	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.
Lessor4 Tid	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.
LessorLøn	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.

LessorPM	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.
	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.
LessorPortalen	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.
LessorSP Tid	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.
LessorWorkforce	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.

A.4. Processing includes the following categories of data subject:

System(s)	**Categories of data subjects**
LessorRefusion	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).
Lessor Payroll, Lessor Time & Attendance and Lessor Human Resources for Microsoft Dynamics	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).
Lessor4	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).
Lessor4 Tid	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).

LessorLøn	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).
LessorPM	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.
LessorPortalen	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).
LessorSP Tid	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).
LessorWorkforce	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).

A.5. The data processor's processing of personal data on behalf of the data controller may be performed when the Clauses commence.

Processing has the following duration:

The processing takes place until the Agreement is terminated.

Irrespective of the formal term of the Clauses, the Clauses will remain in effect for as long as Lessor is processing personal data as a data processor on behalf of the Customer.

Appendix B - Authorised sub-processors

B.1. Approved sub-processors

On commencement of the Clauses, the data controller authorises the engagement of the following sub-processors:

NAME	CVR	ADDRESS	DESCRIPTION OF PROCESSING
Post Danmark A/S	26663903	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	31375428	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	37048658	Lyngbyvej 102 2100 København Ø, Denmark	If the Customer uses an Emply solution, Lessor collaborates with Emply International ApS.
InterLogic Danmark ApS	38179365	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 Denmark A/S	33636431	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 back-up data.
Trifork Security A/S	26762642	Alfred Nobels Vej 25 9220 Aalborg Øst, Denmark	Lessor uses Trifork Security in relation to the delivery of Managed Security Services which ensures and controls traffic on Lessors servers.

The data controller shall on the commencement of the Clauses authorise the use of the abovementioned sub-processors for the processing described for that party. The data processor shall not be entitled – without the data controller's explicit written authorisation – to engage a sub-processor for a 'different' processing than the one which has been agreed upon or have another sub-processor perform the described processing.

B.2. Prior notice for the authorisation of sub-processors

The data processor must notify the data controller in writing with regard to potential planned changes concerning changes or replacements of sub-processors giving at least 2 months notice.

Appendix C - Instruction pertaining to the use of personal data
C.1. The subject of/instruction for the processing

The data processor's processing of personal data on behalf of the data controller shall be carried out by the data processor performin g the following:

System(s)	Description of the processing
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.
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).
Lessor4	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.
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.
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.
LessorPM	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.
LessorPortalen	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.
LessorSP 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.
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, ab-

	sence 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.

Disclosure of personal 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.

C.2. Security of processing

The level of security shall take into account:

The processing encompasses storage of and access to personal data (including confidential personal data) and in some cases sensitive personal data. The processing takes place as part of the data controllers use of the System and the data controller has the possibility to control what personal data that is entered into the relevant System.

The data processor is entitled to and obliged to make decisions about which technical and organizational security measures that must be implemented in order to establish the necessary (and agreed) security level.

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.

The data processor must – in all circumstances and as a minimum - take the technical and organisational measures which is agreed to with the data controller:

For SaaS solutions hosted by Lessor the following security measures apply with regard 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; • 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. As a default setting, a user has 3 login attempts before the user is rejected (this can be changed by the Customer). 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 (TLS 1.2 as a minimum). A HTTPS connection is used with regard to data transfers. The Customer's User ID (user name) and password are encrypted using an algorithm.
Back-up an accessability	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. Lessor has applied multifactor authentication on the different Lessor solutions. 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.
For on-premise solutions the following security measures apply with regard to Lessor's processing of personal data as a data 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. Lessor has applied multifactor authentication on the different Lessor solutions. 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.

C.3. Assistance to the data controller

The data processor shall insofar as this is possible – within the scope and the extent of the assistance specified below – assist the data controller in accordance with Clause 9.1. and 9.2. by implementing the following technical and organisational measures:

- Personal data, that are entered into the System in which the data controller has access to, can at all times be accessed and controlled by the data controller itself or by contacting the data processor which will assist the data controller in obtaining the necessary access to the personal data.
- The data processor has arranged itself organisationally in such a way that relevant contact persons at the data processor can report or escalate questions regarding e.g. assistance to relevant members of the data processor's management and/or the data processors technical and legal personnel.

C.4. Storage period/erasure procedures

The personal data is stored in accordance with the deletion rules that the data controller itself, or by the assistance of the data processor, has established in the relevant System, after which the personal data is deleted at the data processor.

Upon termination of the provision of personal data processing services, the data processor shall either delete or return the personal data in accordance with Clause 11.1., unless the data controller – after the signature of this agreement – has modified the data controller's original choice. Such modification shall be documented and kept in writing, including electronically, in connection with the Clauses.

C.5. Processing location

Processing of the personal data under the Clauses cannot be performed at other locations than the following without the data controller's prior written authorisation:

- Engholm Parkvej 8, 3450 Allerød, Denmark
- Industriparken 35, 2750 Ballerup, Denmark

The locations of the relevant sub-processors engaged by the data processor can be found in Appendix B.1.

C.6. Instruction on the transfer of personal data to third countries

The data processor does not transfer personal data to third countries unless such transfer is specifically agreed to with the data controller. If the data controller and the data processor agree that transfer of personal data to third countries will take place, the parties shall jointly ensure that an appropriate legal basis is in place before such a transfer is initiated.

If the data controller does not in the Clauses or subsequently provide documented instructions pertaining to the transfer of personal data to a third country, the data processor shall not be entitled within the framework of the Clauses to perform such transfer.

C.7. Procedures for the data controller's audits, including inspections, of the processing of personal data being performed by the data processor

The data processor shall each year, at its own expense, obtain an audit report from an independent third party regarding the data processors compliance with the requirements concerning security measures established in the Clauses, and that the audit report is uploaded to the data processors website, http://www.lessor.dk/.

The data processor may, by notifying the data controller in writing, change the website where the audit report is uploaded.

The parties have agreed to that the following audit report always can be used in connection with the Clauses:

- ISAE 3402
- ISAE 3000

Furthermore, the Customer is entitled to appoint an independent expert, at its own expense, who must be given access to such parts of the data processor's physical facilities where the processing of personal data takes place and to receive the information necessary to carry out the investigation into whether the data processor has implemented the appropriate technical and organisational security measures.

The Customer's independent expert will not have access to information about the data processor's general cost structure or to information concerning the data processor's other customers. At the data processor's request, the expert must sign a usual non-disclosure agreement and must, in any circumstance, treat any information obtained or received from the data processor confidentially and may 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.

C.8. Procedures for audits, including inspections, of the processing of personal data being performed by sub-processors

The data processor establishes appropriate procedures regarding audits of the sub-processors based upon the specific risks posed by processing of personal data performed by the individual sub-processor cf. the risk-based approach mentioned in Appendix C.2, as well as the Danish Data Protection Agency's guidelines regarding audit of processors.

Appendix D - The parties' terms of agreement on other subjects

1. **Definitions:** The Clauses constitute an appendix to the agreement which is entered into by the Customer and Lessor regarding the purchase of the System (the Agreement). Defined words and phrases in the Clauses have the same meaning as those in the Agreement unless explicitly stated in the Clauses.

2. **Precedence**: In case of discrepancy between the Clauses and the provisions in other written or oral agreements agreed to by the parties, the Clauses shall have precedence, unless otherwise explicitly agreed to by the parties.

3. **Remuneration:** The data controller shall remunerate the data processor separately for handling specific inquiries and tasks with regard to the Clause 6 (security of processing), 9 (assistance to the data controller), 12 (Audit and inspection) as well as Appendix C.7 and C.8 to the extent that it does not explicitly state that the tasks are delivered at the data processor's own expense. The remuneration is calculated based upon the time and material used by the data processor according to Lessor's hourly rates applicable from time to time.

4. **Third-party Beneficiary**: The data processor shall as far as possible comply with the requirement in the Clause 7.6. However, the data controller is aware of and accepts that it is not possible in all cases for the data processor to include the data controller as a third-party beneficiary in its agreements with every engaged sub-processor, and that parties agree that in such a case where this is not possible, it shall not constitute a breach of the data processors obligations under the Clauses.

5. **Sub-processors:** After Lessor has notified the Customer regarding planned changes in terms of adding or replacing sub-processors (as described in Clause 7.6), if the Customer wishes to object to such a change it must be done within 2 weeks after receiving the notification from Lessor. The Customer may object without giving a specific reason. If the Customer objects, Lessor is entitled to terminate all agreements with the Customer where Lessor processes personal data on behalf of the Customer by giving 2 months' notice.