DATA PROCESSING AGREEMENT

Appendix to Agreement about Danløn

This data processing agreement is an appendix to the Agreement about Danløn entered into by the Parties (the "Agreement about Danløn"). This data processing agreement is an integral part of the Agreement about Danløn as set out in the provisions regarding processing of personal data in the Agreement about Danløn.

The following data processing agreement ("the Agreement") is hereby entered into by and between the entity called the Customer in the Agreement about Danløn (the "Customer") and Danske Lønsystemer A/S, CVR nr.: 15611472, Engholm Parkvej 8, 3450 Allerød, Denmark (the "Supplier"), together referred to as the "Parties" and separately as a "Party":

1 Scope of the Agreement

1.1 The Supplier is the Customer's data processor, as the Supplier carries out the data processing tasks described in Appendix 1 on behalf of the Customer.

1.2 The personal data processed by the Supplier, the purposes of the processing, the categories of personal data and the categories of data subjects are specified in Appendix 1.

1.3 The Agreement only governs the processing of personal data performed by the Supplier as a processor on behalf of the Customer.

1.4 "Personal data" is defined as any information relating to an identified or identifiable natural person, in accordance with article 4(1) of the Regulation (EU) 2016/679 of 27 April 2016 (the "General Data Protection Regulation").

2 Processing of Personal Data

2.1 The Supplier will only process personal data on documented instruction from the Customer, including with regard to transfers of Personal Data to a Third Country or an international organization, unless required to do so by Union or Member State law to which the Supplier is subject. In such a case, the Supplier shall inform the Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

2.2 Instruction: The Supplier is instructed only to process personal data with the purpose to carry out the data processing tasks specified in Appendix 1.

2.3 The Supplier shall immediately inform the Customer if, in the Supplier's opinion, an instruction infringes the General Data Protection Regulation or other Union or Member State data protection provisions.

2.4 The Customer warrants that the Customer has all necessary rights to process all personal data governed by the Agreement and to let the Supplier process such personal data on behalf of the Customer, including but not limited to having acquired relevant consents.

3 Requirements for the Supplier

3.1 The Supplier must process personal data in compliance with applicable Danish data protection regulation, including the General Personal Data Regulation.

3.2 The Supplier must ensure that the persons authorized to process personal data have committed themselves to confidentiality or are bound by an appropriate statutory professional secrecy obligation.

3.3 The Supplier must take all measures required pursuant to article 32 of the General Data Protection Regulation, including implementing appropriate technical and organizational security measures to protect the processed personal data against

(i) accidental or unlawful destruction, loss or alteration,
(ii) unauthorized disclosure or access, or
(iii) processing in breach of applicable legislation including the General Personal Data Regulation.

3.4 The Supplier must also comply with any legally binding standards on security measures, which bind the Supplier directly, including any standards on security measures in the country in which the Supplier is established or in the country in which the data processing takes place.

3.5 The appropriate technical and organizational security measures must be determined with consideration given to

(i) the current technical level,
(ii) the implementation costs,
(iii) the character, extent, context and purpose of the processing as well as

the risks of varying probability and seriousness posed to the rights and freedoms of natural persons.

3.6 The Supplier shall in ensuring the above-mentioned security measures as a minimum implement the level of security and the measures specified in Appendix 3 to the Agreement.

3.7 At the request of the Customer, the Supplier must make available to the Customer all information necessary to demonstrate compliance with the obligations laid down in the Agreement and allow for and contribute to audits in accordance with the Agreement, including inspections, conducted by the Customer or another auditor mandated by the Customer.

3.8 Each year, the Supplier must, at his own expense, obtain a declaration from an independent expert concerning the Supplier's fulfillment of the requirements for the security measures stated in the Agreement. The declaration must be uploaded to the Supplier's website www.danlon.dk once per year. The supplier can designate a new webpage for the uploading of the declaration. The Customer must be notified about such a change in writing.

3.9 Additionally, the Customer is entitled to appoint an independent expert at the Customer's own expense who is entitled to have access to the parts of the physical facilities of the Supplier where personal data is processed and to receive necessary information to investigate whether the Supplier has implemented appropriate technical and organizational security measures. The independent expert appointed by the Customer cannot get access to information about the general cost structure of the Supplier or to information concerning other customers of the supplier. At the request of the Supplier, the expert must sign a non-disclosure agreement. Irrespective of whether a non-disclosure agreement has been signed or not, the expert must treat any information gathered or received from the Supplier confidentially and may under any circumstances only share such information with the Customer. The Customer may not disclose the information to any third party or use the information for any other purpose than to evaluate whether the Supplier has taken the necessary technical and organizational security measures.

3.10 The Supplier must, without undue delay after becoming aware of such circumstances, inform the Customer in writing about

(i) any request of an authority for disclosure of personal data covered by the Agreement unless the Supplier is prohibited to inform the Customer pursuant to EU law or the legislation of a state that applies to the Supplier,

(ii) any suspicion or observation of (a) security breaches leading to accidental or unlawful destruction, loss or alteration, unauthorized disclosure or access to personal data transmitted, preserved or in any other way processed by the Supplier under this Agreement, or (b) any other non-compliance with the obligations of the Supplier under clause 3.3 and 3.4, or

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

3.11 The Supplier must, taking into account the nature of the processing, assists the Customer by appropriate technical and organizational measures, for 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 and erasure.

3.12 The Supplier must assist the Customer in ensuring compliance with the Customer's obligations pursuant to articles 32 to 36 of the General Data protection Regulation, taking into account the nature of processing and the information available to the Supplier, as well as other obligations to which the Customer is subject, pursuant to Union or Member State law under which the assistance of the Supplier is required to the extent that the assistance of the Supplier is necessary for the Customer to comply with such obligations. This includes the provision of necessary information to the Customer of an incident covered by clause 3.10 (ii) as well as all necessary information for the use of an impact assessment under article 35-36 of the General Data Protection Regulation, to the extent the Supplier has access to such information.

3.13 The physical locations of servers, service centers etc. that are used for the processing of personal data are listed by the Supplier in Appendix 1. The Supplier is obligated to inform the Customer in writing before changing the physical location. This does not require a formal amendment of Appendix 1. A prior written notice by mail or email is sufficient.

3.14 The Customer pays the Supplier for the time and material spent on any services, which the Customer requests the Supplier to carry out under clauses 3.7, 3.9, 3.10

(i) and (iii), 3.11, 3.12, 6.4 and 6.5 of the Agreement. The cost of the services follows the prices listed on the Supplier's website at www.danlon.dk, or any website the Supplier designate in its place.

4 Sub-processors

4.1 The Customer gives to the Supplier a prior written consent to use sub-processors. At the time when the Agreement enters into force, the Supplier uses the sub-processors specified in Appendix 2. The Supplier must provide a written notice to the customer describing any planned changes concerning addition or replacement of sub-processors no later than two months before the change takes place. During the first 2 weeks following the Supplier's provision of notice regarding the planned change, the Customer may object to the change by rejecting the use of the new sub-processors, in which case the Supplier may terminate any agreements with the Customer under which the Supplier processes personal data on behalf of the Customer with 1 month's written notice.

4.2 Before using a sub-processor, the Supplier must enter into a written agreement with the sub-processor, in which at least equivalent obligations as assumed by the Supplier under the Agreement are imposed on the sub-processor, including the obligation to carry out appropriate technical and organizational measures to ensure that the processing satisfies the requirements of the General Data Protection Regulation.

4.3 The Customer is entitled to be provided with a copy of all parts of agreements between the Supplier and sub-processors regulating data protection obligations mandatory under clause 4.2.

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

5 Amendments and Transfers

5.1 The Agreement may be changed in accordance with the change procedures set out in the Agreement about Danløn.

5.2 The Supplier may transfer its rights and obligations under the Agreement without consent of the Customer, provided the entity to which the rights and obligations are transferred commits to process personal data in compliance with the Agreement.

6 Duration and Termination

6.1 The term of the Agreement will be the same as the term of the Agreement about Danløn. Upon termination of the Agreement about Danløn, the Agreement will terminate.

6.2 Either Party may terminate the Agreement on the same terms that apply to the Agreement about Danløn.

6.3 Regardless of the formal agreement period, the Agreement remains in force as long as the Supplier as a processor processes personal data on behalf of the Customer for which the Customer is the data controller.

6.4 In the event of termination and upon request of the Agreement, the Supplier must loyally help ensuring that the data processing is passed to another supplier or transferred back to the Customer.

6.5 The Supplier must, at the choice of the Customer, delete or return all the Personal Data to the Customer after termination of the Agreement, and delete existing copies unless Union or Member State law requires storage of the Personal Data.

7 Notifications

7.1 When a Party is required to provide written notice to the other Party under the Agreement, such obligation may be fulfilled, inter alia, by providing such notice via email to the other Party's most recently announced email address. The Supplier may also provide written notice to the Customer by posting messages directly in the system, to which the Customer has received a license of use under the Agreement about Danløn.

8 Precedence

8.1 In the event of a conflict between the provisions of the Agreement and the provisions of other written or oral agreements concluded between the parties, the provisions of the Agreement prevail.

APPENDIX 1

This appendix constitutes, inter alia, the Customer's instruction to the Supplier relating to the processing of data carried out by the Supplier on behalf of the Customer, and it is an integral part of the Agreement.

Instruction and description of the processing of personal data in Danløn

Purpose and nature of the data processing

The purpose of entrusting the data processing activities to the Supplier is to let the Customer use Danløn, which is an IT-system accessed by the Customer online, hosted and run by the Supplier. Danløn helps facilitating the Customer's payroll management, tax and pension matters relating to the Customer's employees, administration of holidays for the Customer's employees, payment of wages, and other payroll related administration. This also entail transfer of personal data to SKAT (Danish tax authorities), pension companies, Nets (digital payments system), Danmarks Statistik (Statistics Denmark) etc. on behalf of the Customer.

Categories of registered data subjects

I. The Customer's potential employees if the Customer enters details about such persons in Danløn.
II. The Customer's current employees if the Customer enters details about such persons in Danløn.
III. The Customer's former employees if the Customer enters details about such persons in Danløn.

Categories of personal data processed

For the above-mentioned categories of registered data subjects, the following personal data is processed: Name, address, CPR-number and date of employment. Furthermore, information regarding the data subjects' payroll details such as salary, taxes, pension, holidays, disbursements etc., including any personal data the Customers registers into Danløn regarding the data subjects, are processed. For optimal use of Danløn, email addresses, cell phone numbers and bank account details of the data subjects are also processed.
For the data subjects in category II the date of resignation is also processed.

Special categories of personal data processed

Depending on the recipient of holiday allowances, it is possible to determine the union membership of the data subject.

Data processing locations

Frederiksborgvej 171
3450 Allerød
Danmark

Gydevang 46
DK 3450 Allerød
Denmark

Skomagervej 10
DK 7100 Vejle
Denmark

Transmission of data

The Supplier may transfer personal data on behalf of the Customer as part of the services provided to the Customer by the Supplier, e.g. to SKAT (Danish tax authorities), pension companies, Nets (digital payments system), Danmarks Statistik (Statistics Denmark) etc.

APPENDIX 2 -specification of current sub-processors

All personal data is hosted by the Supplier's affiliated company Lessor A/S. Lessor A/S owns and maintains the data centers where the personal data is hosted.

Lessor A/S
Engholm Parkvej 8
3450 Allerød

The Supplier cooperates with Compaya A/S. The cooperation makes it possible for the Customer to send out SMS' to the Customer's employees.

Compaya A/S
Palægade 4, 2.tv
1261 København K

The Supplier cooperates with the Danish postal operator. The cooperation makes it possible to distribute pay slips via the digital mailbox (e-Boks) if this has been agreed with the Customer.

PostNord Strålfors A/S
Hedegaardvej 88
2300 København S
Denmark

Appendix 3

Introduction

The Supplier has implemented a risk-based approach to IT security and the protection of personal data processed on our customers and our customer's employees. The Supplier has implemented the below-mentioned technical and organizational measures to mitigate the risks relating to the processing of personal data in Danløn, where the Supplier acts as processor on behalf of the Customer. The Supplier will always as a minimum employ the below-mentioned security measures but can at any time upgrade the level of security and the corresponding measures, if the Supplier identifies a change in the risk scenario.

Physical security at the Supplier's premises

The Supplier has established physical access control to ensure that only authorized persons are able to access the premises, where storage and processing of personal data is taking place.
The Supplier's facilities are subject to video surveillance.
Alarm systems are implemented at the Supplier's premises, and there is only access with a key or a keycard with access code.

Logging

All network traffic and all server logs are monitored and logged.
The following activities are logged in systems, databases and networks:

- All access attempts;
- All searches;
- Activities carried out by system administrators and others with special rights;
- Security incidents, including (i) deactivation of logging, (ii) changes to system rights, and (iii) failed log-on attempts

The Supplier does not operate with shared log-ins so the Supplier will always be able to identify which employee performed a specific activity.
The relevant log files are stored and protected against manipulation and technical errors. The log files are continuously reviewed to ensure normal operation and to examine unintended incidents.

Antivirus and firewalls

All external access to systems and databases where processing of personal data takes place is filtered through a secure firewall with a restrictive protocol.
The Supplier has implemented port- and IP address filtration to ensure limited access to ports and specific IP addresses.
Antivirus software and Intrusion Prevention System (IPS) is installed on all systems and databases where processing of personal data takes place, to protect against hostile attacks.

The antivirus software is continuously updated.
Protection against XSS and SQL injections is implemented in all services.
The Suppliers internal networks are only accessible for authorized persons.

Encryption

Effective and strong encryption based on a recognized algorithm is used for transmission of personal data though the internet and/or email.
The Customer's UserID (username) and password is encrypted using a commonly recognized algorithm.

Back up and availability

The technical measures and the Supplier's systems are continuously reviewed using vulnerability scans and penetration tests.
All changes to systems, databases and networks are carried out in accordance with predefined Change Management procedures, to ensure maintenance with relevant updates and patches, including security patches.
System monitoring is taking place on all systems where personal data is processed.
The data environment is monitored for vulnerabilities and identified problems are solved.
Back-up is established to ensure that all systems and data, including personal data, can be restored if they are lost or altered.

Authorization, access control and security

Only employees with a work-related demand for personal data are granted access to personal data. The assessment of an employee's work-related demands is carried out from a "need-to-have" perspective, to ensure compliance with the principle of data minimization.
Employees are subject to continuous awareness training in relation to IT security and the security of processing of personal data. All employees are informed about the management approved information security policy.
All potential new employees are subject to screening. When employed, the new employee signs a confidentiality agreement. Furthermore, all new employees are introduced to the information security policy and the procedures for processing of personal data pertaining to the work-related responsibilities of the employee.
Specific procedures are in place to ensure that the access user rights of terminated employees are removed.
The Supplier has implemented a password policy to (i) ensure that the passwords of employees are not disclosed to unauthorized persons, and (ii) that only passwords with the necessary level of complexity are approved and (iii) to ensure that passwords are regularly changed.
The Supplier has implemented protection of moveable assets. The security of employees'

laptop computers include protection with commonly recognized encryption, and the use of passwords on the hard disc drive level. Furthermore, VPN connection and two factor identification are used for remote access.
If external persons are allowed access to the Supplier's premises, and thus within a proximity of where processing of personal data is taking place, they are informed of the Supplier's security guidelines and asked to sign a confidentiality agreement.

Controls

The Supplier performs an internal audit and control of the implemented technical and organizational security measures using controls from the ISO 27002 standard. The ISO 27002 standard is used to ensure control with the implementation of the Information Security Management System ("ISMS") used by the Supplier for risk management in the process of determining the necessary security measures.
Furthermore, a yearly ISAE 3402 statement is carried out by an independent auditor. The ISAE 3402 statement is focused on ensuring that the Supplier has implemented and maintained a sufficient and adequate level of security.