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 personal data in the Agreement about Danløn.

The following data processing agreement ("the Agreement") is hereby entered between "the Customer" (the legal entity called the Customer in the Agreement about Danløn) and Danske Lønsystemer A/S, VAT no. 15611472, Engholm Parkvej 8, DK-3450 Allerød (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 provides for the processing of personal data carried out by the Supplier on behalf of the Customer as data processor.

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 ("General data protection regulation").

2 Processing of Personal Data

2.1 The Supplier will 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 organization, unless required to do so by Union or Member State law to which the Supplier is subject. In this case, the Supplier informs the Customer of this legal requirement before processing, unless the legal provision in question 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 informs the Customer immediately, 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 guarantees that the Supplier has sufficient right to process personal data covered by the Agreement and to let the Supplier process these personal data on behalf of the Customer, inter alia by obtaining relevant consents.

3 Requirement for the Supplier

3.1 The Supplier must process personal data in compliance with applicable Danish data protection regulations including the General Data Protection 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.

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 the legislation including the General Data Protection Regulation.

3.4 The Supplier must also comply with the legal standards on security measures, which bind the Supplier directly, including the 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 defined in consideration of

(i) the current technical level,

(ii) the implementation costs,

(iii) the character, the extent, the context and the purpose of the processing as well as the risks of varying probability and seriousness related to the rights and freedoms of natural persons.

3.6 The Supplier must in ensuring the above-mentioned security measures as a minimum implement the technical and organizational measures specified in Appendix 3 of 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 Data Processing Agreement and allow for and contribute to audits in accordance with the Data Processing 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 on the Supplier's website www.danlon.dk once each year. By written notification to the Customer, the Supplier is entitled to change the website on which the declaration must be uploaded.

3.9 In addition, the Customer is entitled to appoint an independent expert at his own expense who must have access to those parts of the physical facilities of the Supplier in which the processing of personal data takes place and receive necessary information for analyzing whether the Supplier has taken the technical and organizational security measures mentioned. The independent expert of the Customer cannot get access to information on 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 an undertaking of secrecy and in any event treat any information gathered or received from the Supplier confidentially and only share information with the Customer. The Customer is not entitled to pass on information or to use the information for any other purposes than for the assessment of whether the Supplier has implemented the necessary technical and organizational security measures.

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

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

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

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

3.11 The Supplier must, taking into account the nature of the processing, assist the Customer by appropriate technical and organizational measures, for the fulfillment of the Customer's obligation to respond to requests for exercising the data subjects' 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 32-36 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 in particular, upon request, the provision of all 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 location of servers, service centers etc. which form part of the data processing is stated in Appendix 1. The Supplier is obliged to warn the Customer before changing the physical location. This does not require a formal amendment of Appendix 1. A prior written notice is sufficient.

3.14 The Customer pays the Supplier separately for the time and material spent on the handling of enquiries and tasks according to paragraph 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 www.danlon.dk or any other website selected by the Supplier.

4 Sub-processors

4.1 The Customer gives to the Supplier a prior written consent to use sub-processors. At the time of the conclusion of the Agreement, the Supplier uses the sub-processors specified in Appendix 2. The Supplier must inform the Customer in writing of any planned changes concerning addition or replacement of sub-processors no later than two months beforethe amendment enters into force. The Customer is entitled within two weeks following the provision of the amendment, without giving any reasons, to object to the amendment by refusing to use the new sub-processor. In this case, the Supplier is entitled to terminate all agreements with the Customer according to which the Supplier processes personal data on behalf of the Customer by serving a notice of one month.

4.2 Before using a sub-processor, the Supplier must conclude a written agreement with the sub-processor in which at least the same obligations are imposed on the sub-processor as assumed by the Supplier at the time of the conclusion of the Agreement, 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 the parts of the Supplier's agreement with a sub-processor which relate to data protection obligations and are mandatory under clause 4.2.

4.4 If a sub-processor fails to fulfill its data protection obligations, the Supplier remains fully liable to the Customer of the performance of the 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 can transfer his rights and obligations according to the Agreement without a consent of the Customer, provided that the person to whom rights and/or obligations are transferred is obliged to process personal data in accordance with the requirements applicable to the Supplier according to the Agreement.

6 Duration and Termination of the Agreement

6.1 The Agreement comes into force at the same time as the Agreement about Danløn and will apply until the Agreement about Danløn terminates.

6.2 Each party is entitled to terminate the Agreement on the same terms as those applicable to Agreement about Danløn.

6.3 Regardless of the formal agreement period, the Agreement applies as long as the Supplier as data processor processes personal data for the customer which the customer controls.

6.4 In case of termination of the Agreement, the Supplier is obliged, upon request, to help to ensure that the data processing is passed on to another supplier or transferred back to the Customer, sincerely.

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

7 Notifications

7.1 If a Party according to the Agreement has to forward a written message to the other Party, the obligation can be fulfilled by sending an email to the most recent email address of the other Party. The Supplier may also fulfill the obligation to make a written notification by posting messages directly in the system, to which the Customer has received a license of use under 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 must 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 is an integral part of the Agreement.

Instruction and description of the processing of Personal Data in Danløn

Purpose and character of the data processing

The purpose of entrusting data processing activities to the Supplier is to let the Customer use Danløn which is an IT system accessed by the Customer online and hosted and operated 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 pay etc. This also includes the transfer of data on behalf of the Customer, e.g. to the Danish Tax Agency, Nets, pension companies, Statistics Denmark etc.

Categories of data subjects

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

Categories of personal data

For the above-mentioned categories of registered data subjects, name, address, personal ID number and employment date will be processed. Furthermore, information regarding the data subjects' payroll details such as pay, taxes, pension, holiday, disbursements, mileage allowances etc. including the information registered by the Customer about the data subjects in Danløn. For optimal use of Danløn, email address, mobile phone number and bank account details will also be processed.

For the data subjects in category III, the resignation date will be processed as well.

Special categories of personal data

Based on the recipient, to which the holiday pay of the data subject is settled, it is possible to determine the union membership of the data subject.

Location(s) including the country in which the processing takes place

DK-3450 Allerød
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. the Danish Tax Agency, pension companies, Nets, Statistics Denmark etc.

APPENDIX 2

Use of sub-processors

All data are hosted by the Supplier's affiliated company, Lessor A/S. Lessor A/S owns and runs the data centers, in which the Customer's information is hosted.

Lessor A/S
Engholm Parkvej 8
DK-3450 Allerød

The Supplier cooperates with Compaya A/S. The cooperation makes it possible to send out SMS messages to the Customer's employees, if this has been agreed with the Customer.

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

The Supplier cooperates with PostNord Strålfors A/S if this has been agreed with the Customer. The cooperation makes it possible to distribute pay slips via e-Boks.

PostNord Strålfors A/S
Hedegaardvej 88
DK-2300 København S

The Supplier cooperates with Db2Data ApS. This company assists the Supplier in deleting, compressing and indexing on the Supplier's servers in the Supplier's data center.

Db2Data ApS
Svejgårdsvej 14
DK-2900 Hellerup

The Supplier cooperates with Bogholdergruppen.dk. This company assists the Supplier in supporting the Customer in writing and by telephone via the Danløn services 'Kontakt support' and 'Danløn Direkte'.

Bogholdergruppen.DK
Gammel Køge Landevej 55,4
DK-2500 Valby

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 customers' employees. The Supplier has implemented the below-mentioned technical and organizational measures to mitigate the risks related to the processing of personal data in Danløn where the Supplier acts as processor on behalf of the Customer. The Supplier will, as a minimum, always employ the below-mentioned security measures, but may at any time upgrade the security level and the corresponding measures in case of a change of 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 personal data are stored and processed.

The Supplier's facilities are subject to video surveillance.

Alarm systems are implemented in the Supplier's premises. Access requires a key or a key card with access code.

Logging

Al 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 and
- 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 work with shared log-ins. Therefore, it will always be possible 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.

Anti-virus and firewalls

All external access to systems and databases where processing of personal data takes places, is filtered through a secure firewall with a restrictive protocol.

A port and IP address filtration has been implemented to ensure limited access to ports and specific IP addresses.
Anti-virus software and Intrusion Prevention System (IPS) have been installed on all systems and databases where processing of personal data take place, to protect against hostile attacks. The anti-virus software is continuously updated.
Protection against XSS and SQL injections is implemented in all services. The internal network of the Supplier can only be accessed by authorized persons.

Encryption

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

Backup and availability

The technical measures and the Supplier's systems are continuously tested by means of vulnerability scans and penetration tests.
All changes to systems, databases and networks are carried out in accordance with predefined Change Management procedures, which ensure maintenance with relevant updates and patches, including security patches.
System monitoring is taking place on all systems, in which personal data are processed. The data environment is monitored for vulnerabilities, and identified problems, if any, are solved.
Backup 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 are granted access to personal data. All assessments of an employee's work-related demand are carried out from a 'need to have' perspective in order to ensure compliance with the principle of data minimization. The employees' access is reassessed regularly.
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 written information security policy approved by the management.
All new employees are subject to screening. When employed, the employees sign a confidentiality agreement. Furthermore, new employees are introduced to the information security policy and procedures for processing of personal data within the employee's field of work.
Specific procedures are implemented to ensure that the user rights of resigning employees are deactivated.

The Supplier has implemented a password policy to ensure that the employees' passwords do not fall into any unauthorized person's hands, that only passwords with the necessary level of complexity can be approved and that passwords are changed regularly.
The protection of movable devices is established. The employees' laptop computers are i.a. protected with a recognized encryption protocol and passwords on hard disc drive level. Furthermore, VPN connection and a two-factor authentication are used for remote access.
Outside personnel with access to the Supplier's premises and thus potentially to personal data is informed about the Supplier's security guidelines and asked to sign a confidentiality agreement.

Checks

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 connection with the determination of the necessary security measures.
Furthermore, an annual ISAE 3402 statement is drawn up by an independent auditor. The ISAE 3402 statement is focused on ensuring that the Supplier has implemented and maintained a sufficient level of security.