Data Processing Agreement

1. Purpose and background

This Data Processing Agreement concerns Planday´s processing of Personal Data on behalf of the Controller and this Data Processing Agreement sets out the terms and conditions which apply to the Processor's Processing of Personal Data.

2. Definitions and interpretation

The following words and expressions have the meanings stated below, unless the context requires otherwise.

Appendix/Appendices	Means appendices to this Data Processing Agreement.
Business Day	A day other than Saturday, Sunday or public holiday
Business Hours	9:00 am to 5:00 pm on a Business Day
Contract	Means the customer agreement between the Processor and Customer regarding delivery of services, and Processor's general terms, including any schedules, appendices and amendments hereto
Controller	The Customer as defined in the Contract and in accordance with the definition in the applicable Data Protection Law.
Data Processing Agreement	This agreement with Appendices.
Data Processing Services	The services described in Appendix A
Data Protection Law	The legislation, as amended, protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the Processing of Personal Data applicable to a Controller: in the EEA country where the Controller is established, including the GDPR, the United Kingdom Data Protection Act 2018, the Privacy and Electronic Communications Directive 2002/58/EC (as updated by Directive 2009/136/EC) and the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426). A reference to Data Protection Law is a reference to it as amended, extended or reenacted from time to time.

Data Subject	An identified or identifiable natural person (an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person).
Destroy/Destruction	Means that Personal Data is irrevocably deleted from all storage media on which it has been held and that the Personal Data cannot in any way be restored, including by any Sub-processors.
EEA	The European Economic Area.
GDPR	Regulation (EU) 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)
Personal Data	Any information, in whatever form, relating to the Data Subject and as further defined in Data Protection Law.
Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.
Process/Processing	Any operation or set of operations which is performed upon Personal Data or on sets of Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Processing Operations	As defined in Appendix A
Processor	Means Planday as defined in the Data Processing Agreement and in accordance with the definition in the applicable Data Protection Law.
Return	Means that all Personal Data is returned physically or electronically to the Controller and that any copies thereof etc. which may be in the

	Processor's possession, or which the Processor may have at its disposal, including Personal Data handed over to Sub-processors, is subject to Destruction.
Sub-processor	Means another processor engaged by the Processor with the purpose of carrying out specific processing activities on behalf of the Controller.
Planday System	Any information technology system or systems on which the Data Processing Services are performed in accordance with this Data Processing Agreement.

2.2 Any exclusion or cap on liability in the Contract shall also apply to the Processor's liability under this Data Processing Agreement.

3. Scope

3.1 The Data Processing Agreement applies to any Processing of Personal Data performed by the Processor in connection with the performance of the Data Processing Services to the Controller as defined in Appendix A (the subject-matter).

3.2 The Customer and Planday acknowledge that the Customer is the Controller and Planday is the Processor in respect of any Personal Data supplied to Planday by or on behalf of Customer, including Personal Data described in Appendix A, in the course of the supply of the Data Processing Services.

3.3 The nature and purpose of the Processing, the types of Personal Data and categories of Data Subjects are set out in Appendix A.

4. Obligations of the Processor

4.1 The Processor shall:

a) process Personal Data only on documented instructions from the Controller as specified in this Data Processing Agreement and for the purposes set out in Appendix A;
b) discharge its operations under this Data Processing Agreement with due skill, care and diligence;
c) keep a record as described in art. 30 of the GDPR at its normal place of business of any Processing of the Personal Data carried out in the course of the Data Processing Services and of its compliance with its obligations set out in this Data Processing Agreement ("Records");
d) ensure that persons authorised to Process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
e) implement appropriate technical and organisational measures to protect Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and against all other unlawful forms of Processing as specified in clause 6;
f) only make copies of the Personal Data to the extent reasonably necessary, which among other things may include back-up, mirroring, security, disaster recovery and testing of the Personal Data;
g) only subcontract with Sub-processors in accordance with the requirements of clause 7;
h) immediately inform the Controller if, in its opinion, an instruction infringes Data Protection Law;
i) assist the Controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to requests for exercising the Data

Subject's non-exclusive rights to access, rectification, erasure and data portability, as these are stated in the Data Protection Law;

j) at the choice of the Controller Destroy or Return all the Personal Data to the Controller either during or after the term of this Data Processing Agreement, cf. clause 11;
k) make available to the Controller all information necessary to demonstrate compliance with the Data Protection Law, e.g. annual ISO27001 compliance certificate, if any;

l) in connection with clause 4.1(k), if legally and technically possible allow for and contribute to audits, including inspections conducted by the Controller or another mandated by the Controller as set out in clause 8;
m) comply with its obligations under Data Protection Law.

4.2 If the Processor receives any complaint, notice or communication which relates directly or indirectly to the Processing of Personal Data or to either party's compliance with Data Protection Law, it shall immediately notify the Controller and it shall provide the Controller with full cooperation and assistance in relation to any such complaint, notice or communication.

4.3 The Processor's liability under the Contract, including the Data Processing Agreement, is capped and disclaimed according to the terms of the Contract.

4.4 The Processor shall inform the Controller without undue delay if the Processor knows / becomes aware of any Personal Data Breach.

4.5 The Processor shall be entitled to charge the Controller separately for any cost (including internal resources at the Processor' standard rates) that may incur in relation to assistance as referred to in clause 4.1(a)-(m).

5. Obligations of the Controller

5.1 The Controller will be solely responsible and liable for its compliance with applicable law as Controller. The Controller will ensure before using the software and receive the services under the Contract in a way that includes Processing of Personal Data that it complies with all Data Protection Law, e.g. in relation to the provision of required information/notification to and/or approvals from Data Subjects and/or regulatory authorities related to the Processing.

5.2 The Controller will promptly notify the Processor if it becomes aware that Processing of the Controller's Personal Data may be contrary to Data Protection Law.

5.3 The Controller warrants that the Processor's strict compliance with any instruction from the Controller with respect to the Processing of Personal Data, shall not result in a violation of applicable Data Protection Law.

5.4 The Controller will indemnify the Processor from any loss resulting from the Controller's failure to comply with its obligations hereunder.

6. Security measures

6.1 The Processor must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks, that are presented by Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise Processed, 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 risks of varying likelihood and severity for the rights and freedoms of natural persons, including inter alia as appropriate:

a) the pseudonymisation and encryption of Personal Data;
b) the ability to ensure the 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.

6.2 The specific technical and organisational security measures implemented by the Processor are set out in Appendix B (Security Measures).

7. Sub-processors

7.1 The Controller hereby authorises the Processor to engage Sub-processors, including without limitation the Sub-processors as stated in Appendix A, to perform Processing of Personal Data, provided that the Processor enters into a written agreement with each Sub-processor which imposes the same obligations on the Sub-processors as are imposed on the Processor under this Data Processing Agreement. The Controller will at any time upon reasonable prior written notice be entitled to receive a copy of the Processor's data processing agreement with each Sub-processor.

7.2 The Processor will inform the Controller by email about any intended addition or replacement of a sub-processor in advance allowing the Controller/Data Subject the opportunity to object and/or render its informed consent, such not to be unreasonably withheld. The controller cannot object without a bona fide and objective reason, unless required by mandatory law. If the Controller objects to any addition or replacement of any sub-processor, provided that such objection is based on a bona fide and objective reason, the Processor is entitled to terminate the Data Processing Agreement with immediate effect by written notice.

7.3 Where a Sub-processor fails to fulfil its data protection obligations under the Data Processing Agreement referred to in clause 7.1, the Processor shall remain fully liable to the Controller for the performance of the Sub-processor's fulfilment of its data protection obligations in general.

8. Audits

8.1 For the purpose of auditing the Processor's compliance with its obligations under this Data Processing Agreement, the Processor shall allow for the Controller, on reasonable written notice of not less than thirty (30) days to the Processor during Business Hours, to perform an Audit, including but not limited to a) gain access to inspect the records and any other information held at the Processor's premises or on the Processor System related to the Data Processing Services, and; b) gain access to inspect the Processor System.

8.2 The written notice shall include a proposed audit plan. If part of the requested audit scope is covered by the scope of an audit report by a qualified third party auditor within the last 12 months, the Processor may request the Controller to consider whether it could rely on such a report instead of an audit. The Processor will be entitled to suggest the date and time of the audit to minimise business disruption and may suggest the audit to be combined with audits from other Controllers. The Controller cannot deny such suggestions from the Processor, unless it has a bona fide objective reason to do so.

8.3 At the written request of Controller according to Clause 8.1 and 8.2, the Controller (or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality appointed by the Controller or Regulator) will be entitled to perform audits of the Processor's facilities and security practices directly related to the Processing of Personal Data under the Contract in order to monitor compliance with this Data Processing Agreement. Unless in case of any reasonable suspected breach of this Data Processing Agreement or as otherwise permitted by mandatory law, such audit shall be limited to 1 audit per 12 months' period.

8.4 The Controller will bear any costs related to audits and the Processor shall be entitled to charge the Controller separately for any reasonable cost (including internal resources at the Processor's standard rates) that the Processor may incur in relation to its assistance with such audits.

8.5 Any audit shall be conducted in accordance with the Processor's internal policies and all participants shall be subject to adequate written confidentiality obligations. To the extent allowed under applicable law, the Controller shall deliver to the Processor a copy of the audit report and, subject to removing any Confidential Information, the Processor shall be entitled to use such report free of charge in relation to other Controllers.

8.6 The Controller may use the information obtained during any audit, including any audit report, only for the purpose of meeting its audit obligations under Data Protection Law. For the avoidance of doubt, the Controller is not allowed to disclose to the public any parts of the audit report, without prior written consent from the Processor, unless required by mandatory law.

8.7 The Processor shall give all necessary assistance to the conduct of such audits during the term (as set out in clause 10) of this Data Processing Agreement.

8.8 The Controller, or its third-party representatives as specified in clause 8.3, is allowed to conduct audits with the Processor's Sub-processors to the extent this is possible according to the terms and conditions in the then currently valid and applicable version of the Sub-processor's terms and conditions.

9. Third country transfers

9.1 The Processor may only transfer the Personal Data to countries outside the EEA subject to documented instructions from the Controller as specified in Appendix A.

9.2 If the Processor transfers Personal Data to any third country (being a country outside the EEA when the Controller is located in the EEA) the Processor will inform the Controller of such intended transfer in advance allowing the Controller the opportunity to object and will ensure that the following conditions are fulfilled:

a) the Processor has provided appropriate safeguards (including any appropriate legal mechanisms) in place in relation to the transfer;
b) the Data Subject has enforceable rights and effective legal remedies;
c) the Processor provides an adequate level of protection to any Personal Data that is transferred; and
d) the Processor complies with reasonable instructions notified to it in advance by the Controller with respect to the processing of the Personal Data.

10. Term and termination

10.1 This Data Processing Agreement will take effect from the effective date as specified in the Contract, and shall continue in force during the Term as defined in the Contract.

10.2 Upon termination of the Contract, this Data Processing Agreement shall also terminate.

10.3 In continuation of clause 10.2, The Processor shall, upon instruction from the Data Controller, either delete or anonymize the personal data processed under this Agreement. If no such instruction is received within 120 days after the termination of the service contract, the Processor shall have the right to choose either deletion or anonymization. The Processor shall confirm the action taken to the Data Controller in writing. The Processor shall ensure that any deletion or anonymization is carried out in compliance with applicable data protection laws and regulations

10.4 Any provision of this Data Processing Agreement that expressly or by implication is intended to come into or continue in force or after termination of this Data Processing Agreement shall remain in full force and effect.

10.5 Termination of this Data Processing Agreement, for any reason, shall not affect the accrued rights, remedies, obligations or liabilities of the Parties existing at termination.

11. Changes

11.1 If there are changes in mandatory Data Protection Law, the Processor is entitled to change this Data Processing Agreement accordingly without notice and without the possibility for the Controller to terminate the Data Processing Agreement or the Contract.

11.2 Notwithstanding clause 7.2 and 11.1, the Processor reserves the right to modify this Data Processing Agreement at any time according to the procedure for changes in the Contract.

12. Governing law and disputes

12.1 This Data Processing Agreement is governed by and will be interpreted in accordance with Danish law. However, the conflict of laws rules must be disregarded to the extent that such rules are non-mandatory.

12.2 Any dispute arising out of this Data Processing Agreement, including any dispute concerning the existence or validity of this Data Processing Agreement shall be brought before the Danish courts.

Appendix A to Data Processing Agreement

In connection with the Processor's provision of services and hosting the Personal Data on behalf of the Controller, the Controller gives the Processor the instruction and grants consent to Process the following Personal Data for the purposes set out below:

1. General description and purpose of the Processing Operations Processing Operations:

The Processor processes the Personal Data of the Controller for the purpose of delivering an available and operational workforce management service/product. This includes providing customized user experiences within our product and service and when needed performing troubleshooting, ongoing maintenance and improvements.

The Controller provides the Processor with access to pseudo- and anonymise data to support the delivery and fulfillment of the purposes provided.

2. Categories of Data Subjects

The Data Subject categories may be adjusted from time to time, to the extent that the processing of Personal Data and the purposes thereof continue to fall under the general description.

- *Employees*
- *Potential employees*
- *Former employees*

3. Types of Personal Data

Description of the types of Personal Data for each category of Data Subjects:

Full name & initials, address, email address, telephone, gender, Tax ID, bank details, birth date, relative or next of kin full name & telephone, payroll details, photograph, employee contract information, employee payslip information, data entered into custom fields created by Customer which may contain sensitive Personal Data including medical data.

4. Who at the Processor has access to Personal Data?

Only persons engaged with the purposes for which the Personal Data is Processed will be authorised to access and Process the Personal Data. This e.g. includes employees providing:

- *Support services,*
- *Maintenance and backup,*
- *Operational system/support staff*

5. Which external parties have access to all or part of the Personal Data (sub-processors), for which purpose(s) and their geographical location?

Sub Processor	Description	Physical Address	Contact
Salesforce	**Customer records management processor, required for Sales and Support Activities**	**Floor 26 Salesforce Tower 110 Bishopsgate London United Kingdom EC2N 4AY**	**privacy@salesforce.com**
Intercom	**Real-time chat support within product to customers and in-product notifications**	**3rd Floor, Stephens Ct.18-21 St. Stephen's Green Dublin 2, Ireland**	**compliance@intercom.com**
Microsoft Azure	**Infrastructure Hosting Services and in-product services**	**One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland**	**https://azure.microsoft.com/en-gb/support/options/**
Kombo Technologies Gmbh	**Integrations Platform, Automatic synchronization, transfer and integration of data between HR, ATS and payroll systems**	**Rosenthaler Str. 72A 10119 Berlin Germany**	**Support@kombo.dev**

Appendix B to the Data Processing Agreement

Security measures

The Processor will implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk of the processing. These measures include but are not limited to:

1. Access control to premises and facilities (physical)

1.1 Processor will ensure a contractual commitment to commercially reasonable physical security systems at all sub-processor or hosted data centres and administration sites which are used to Process Personal Data;

1.2 Processor will ensure a contractual commitment that physical access control is implemented for all sub-processor or hosted data centers (including, by way of example only, by verifying access control to the data centres with the sub-processor, for example whether unauthorised access to data centres is prohibited by onsite staff, or that biometric scanning or security camera monitoring is in place as required, or that turnstiles are integrated with access control readers to control physical access at all sites at all times by requiring staff to present a photo identity card prior to entering such site);

1.3 Processor will review whether sub-processor or hosted data centres maintain procedures for issuing identification badges to authorised staff and controlling physical access to systems under its control;

1.4 Processor will verify with the sub-processor or hosted data centre whether visitors are pre-approved before coming to Processor sites which are used to Process Personal Data, required to present identification and/or sign a visitor log, and escorted at all times while on the sites.

2. Access control to systems (virtual)

2.1 Processor will establish and maintain commercially reasonably safeguards against accidental or unauthorised access to, destruction of, loss of, or alteration of the Personal Data on the systems which are used to Process Personal Data:

2.1.1 access will be granted to personnel on the basis of least privilege and specific roles, through documented access request procedures;

2.1.2 access controls are enabled at the operating system, database, or application level;

2.1.3 administrative access will be restricted to prevent changes to systems or applications;

2.1.4 users will be assigned a single account with multi-factor authentication where possible and prohibited from sharing accounts.

3. Access control to devices and laptops

3.1 Processor will implement and maintain commercially reasonable security measures with respect to mobile devices and laptops that are used to Process Personal Data.

4. Access control to Personal Data

4.1 Access will be granted only after successful completion of an approved process, i.e. LAN Logon ID, application access ID, or other similar identification.

4.2 Unique User IDs and passwords will be issued to the users.

4.3 Users, once authenticated, will be authorised for access levels based on their specific role and on the basis of least privilege.

5. Transmission and disclosure control

5.1 Processor will implement and maintain commercially reasonable measures to prevent Personal Data from being read, copied, modified or removed without authorisation during electronic

transmission or transport and to enable Processor to check and establish to which bodies the transfer of Personal Data by means of data transmission facilities is envisaged.

5.2 Processor will maintain technology and processes designed to minimise access for illegitimate Processing, including technology for the encryption of Personal Data.

6. Input control

6.1 Processor will maintain system and database logs for access to all Personal Data under its control;

6.2 All Processor systems must be configured to provide event logging to identify a system compromise, unauthorised access, or any other security violation. Logs must be protected from unauthorised access or modification;

6.3 Customer/Processor will maintain input controls on its systems.

7. Job control

7.1 Processor will implement procedures to ensure the reliability of its employees and any other person acting under its supervision that may come into contact with, or otherwise have access to and Process, Personal Data, such as completing background checks prior to the commencement of employment.

7.2 Processor will implement procedures to ensure that its personnel are aware of its responsibilities under the Agreement. Processor shall instruct and train all persons it authorises to have access to the Personal Data on the Data Protection Legislation as well as on all relevant security standards and shall commit them in written form to comply with the data secrecy, the Data Protection Legislation and other relevant security standards.

7.3 Processor will promptly act to revoke access to Personal Data of Customer/Processor due to termination, a change in job function, or in observance of user inactivity or extended absence.

7.4 Processor shall have in place a data protection policy and a document retention policy, with which its personnel must comply.

8. Incident management

8.1 Processor will implement, maintain an incident management procedure that allows the processor to inform the Controller within the required time frame of any relevant incident, as appropriate.

8.2. Should an incident (potentially) affect personal data, the Processor shall notify the Controller in accordance with Clause 4 in the Data Processing Agreement.

8.3 The incident management procedure includes periodic evaluation of recurring issues that might indicate a security breach.

8.4 Processor will periodically review any previous incidents to see what it can learn.

9. Availability control

9.1 Processor will protect Personal Data against accidental destruction or loss by ensuring:

9.1.1 Workstations will be protected by commercial anti-virus and malware prevention software receiving regular definition updates;

9.1.2 Upon detection of a virus or malware, Processor will take immediate steps to arrest the spread and damage of the virus or malware and to eradicate the virus or malware.

9.1.3 Servers will be protected by commercial firewalls and intrusion protection prevention systems.

10. Business continuity and change management

10.1 Processor will implement, maintain and regularly review a business continuity plan and disaster recovery plan that will, inter alia, allow the Processor to restore the availability and access to the Personal Data in a timely manner to be agreed upon by the parties involved in the event of a physical or technical event.

10.2 Processor will implement change management to control the organisation, business processes, systems and sub-processor relationships that affect information security.

10.3 As part of the change management procedure, the Processor reviews any potential impact on the security of personal data to see what it can learn.

11. Control of instructions

11.1 Processor will implement and maintain procedures to ensure that Personal Data is processed only in accordance with Controller's instructions.

12. Separation control

12.1 Processor will implement and maintain procedures to ensure that personal data collected for different purposes will be processed separately to the extent that Processor has been expressly notified about such different purposes and requested to do so and under the condition that Processor may invoice its time and expenses for complying with this request.

13. Regular testing of security measures

13.1 Processor will frequently test, assess and evaluate the effectiveness of its technical and organisational security measures.