Updated November 2020

Processor Binding Corporate Rules

ARTICLE I.
OVERVIEW, OBJECTIVE AND SCOPE

1. Workday's service

Workday, Inc. and its subsidiaries listed on Schedule 1 hereto (collectively the "**Workday Group**") provide software-as-a-service offerings where customers can load and Process data on the systems of the Workday Group. The Workday Group does not select or control the customers' data or Processing. The Workday Group only provides the technology platform and applications on which customers' Process data and provides ancillary support for the application on the customer's behalf and for the customer's benefit.

2. BCR as additional compliance option

The Workday Group is committed to offering its customers state of the art software-as-a-service solutions, data security standards and support with respect to the customer's data privacy compliance needs. The Workday Group does and will continue to offer its customers adequate data transfer and processing agreements and compliance options based on Workday, Inc.'s certification under the EU/CH-U.S. Privacy Shield Programs. To provide an alternative route to achieve compliance with data protection and data privacy laws, the Workday Group implements these Processor Binding Corporate Rules ("**BCR**"). Customers of the Workday Group that prefer the BCR approach can contract with members of the Workday Group to cover their Personal Data under these BCR, as further specified in the contractual agreement between such member of the Workday Group and the customer ("**Service Agreement**"). These BCR achieve an adequate level of protection for Personal Data, as required by the General Data Protection Regulation (EU) 2016/679 ("**GDPR**") and also satisfy requirements under other jurisdictions' laws.

3. Scope

Hundreds of companies, ranging from medium-sized to the Fortune 50, are amongst the customers of the Workday Group, each with different compliance needs and preferences.

These BCR govern international transfers of Personal Data to and between members of the Workday Group when acting as Processors on behalf of a Controller. The Processing activities involve the storing of the Personal Data and the Processing necessary to operate and maintain the Service and implement the individual customer's instructions when using the Service.

The Personal Data Processed by the Workday Group on behalf of its customers pertains to their prospective, current and former employees and the dependents or beneficiaries of such employees, as necessary for the customers as part of their human resources and benefits Processing. Depending on the choice of the individual customer, the Personal Data contains, without limitation, name, contact information, personal status information, information pertaining to employment or similar contracts, information on work experience, education and training, and compensation, payroll and benefits information. Depending on the circumstances of the individual case, the Personal Data might also contain information on ethnicity, religious beliefs, disability or trade union membership.

As required to provide its services to its customers, the Workday Group may export the Personal Data to the countries in which the different members of the Workday Group have their place of business (see Schedule 1 to the BCR set forth in Article II).

The Workday Group will agree with each customer in a Service Agreement which categories of the customer's data shall be covered by these BCR, for example, only Personal Data of Data Subjects in the EEA or also Personal Data of Data Subjects in other jurisdictions. Once such agreement has been reached, the Workday Group and its employees and contractors will comply with these BCR with respect to the data identified in the Service Agreement. Additional privacy compliance laws and requirements may apply to specific data, locations or functions.

4. Definitions

Notwithstanding the potentially broader scope of these BCR, as specified in a Service Agreement with a particular customer, certain terms shall bear the following meanings in these BCR:

Controller	means the natural or legal person which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data. In these BCR, the "Controller" shall be a legal entity with whom a member of the Workday Group has entered into a Service Agreement which incorporates by reference these BCR;
Data Subject	means an identified or identifiable natural person;
European Economic Area or EEA	means the member states of the European Union (including the UK) plus Iceland, Liechtenstein and Norway;
EU	means the member states of the European Union (including the UK);
Personal Data	means any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an 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. In these BCR, the term "Personal Data" refers to any Personal Data submitted electronically into a Service;
Personal Data Breach	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed;
Processing	means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated 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;
Processor	means a natural or legal person which Processes Personal Data on behalf of a Controller;
Service	means the Workday software-as-a-service applications.
Sub-processor	means a natural or legal person engaged by a Processor to Process Personal Data on behalf of itself and a Controller; and
Supervisory Authority	means an independent public authority, which is established by a member state pursuant to Article 51 GDPR.

ARTICLE II.
BINDING CORPORATE RULES

1. Binding nature

1.1 The duty to respect the BCR

All members of the Workday Group and their employees have the duty to respect the BCR and the instructions regarding the Personal Data Processing and the security and confidentiality measures as provided in the Service Agreement.

1.2 Means by which the BCR are made binding on the Workday Group and its employees

All members of the Workday Group have signed an intra-group agreement that obligates each member to comply with the BCR. Each employee of a member of the Workday Group is subject to an individual and separate agreement, a clause in an employment contract, and/or internal policies, in each case providing for sanctions in case of non-compliance.

1.3 Third-party beneficiary rights for Data Subjects

1.3.1 Each Data Subject whose Personal Data is covered by the BCR pursuant to a Service Agreement shall have the right to enforce the following elements of the BCR as a third-party beneficiary directly against each member of the Workday Group involved in the Processing of the Data Subject's Personal Data:

- Duty to respect the instructions from the Controller regarding the Personal Data Processing including for transfers to third countries (Art. 28.3.a, 28.3.g., 29 GDPR and Sections 1.1, 6.1.ii and 6.1.iv of these BCR),
- Duty to implement appropriate technical and organizational security measures (Art. 28.3.c and 32 GDPR and Section 6.1.iv of these BCR) and duty to notify any Personal Data Breach to the Controller (Art. 33.2 GDPR and Section 6.1.iv of these BCR),
- Duty to respect the conditions when engaging a Sub-processor either within or outside the Workday Group (Art. 28.2, 28.3.d, 28.4, 45, 46, 47 GDPR and Sections 6.1.vi and 6.1.vii of these BCR),
- Duty to cooperate with and assist the Controller in complying and demonstrating compliance with the law such as for answering requests from Data Subjects in relation to their rights (Art. 28.3.e, 28.3.f, 28.3.h GDPR and Sections 3.2, 6.1.i, 6.1.iii, 6.1.iv, 6.1. v and 6.1. 2 of these BCR),
- Easy access to the BCR (Art. 47.2.g GDPR and Section 1.8 of these BCR),
- Right to complain through internal complaint mechanisms (Art. 47.2.i GDPR and Section 2.2 of these BCR),
- Duty to cooperate with the Supervisory Authority (Art. 31, 47.2.l GDPR and Section 3.1 of these BCR),
- Liability, compensation and jurisdiction provisions (Art. 47.2.e, 79, 82 GDPR and Sections 1.3, 1.5 and 1.7 of these BCR),
- National legislation preventing respect of the BCR (Art. 47.2.m GDPR and Section 6.3 of these BCR).

1.3.2 Each Data Subject whose Personal Data is covered by the BCR pursuant to a Service Agreement shall have the right to enforce the BCR as a third-party beneficiary against each member of the Workday Group involved in the Processing of the Data Subject's Personal Data in case the Data Subject is not able to bring a claim against the

Controller because the Controller has factually disappeared or ceased to exist in law or has become insolvent, unless any successor entity has assumed the entire legal obligations of the Controller by contract or by operation of law, in which case the Data Subject can enforce its rights against such entity. In such a case, the Data Subject shall be able to enforce against the respective member of the Workday Group the following sections set out in these BCR: Article II, Sections 1.1, 1.3, 1.5, 1.7, 1.8, 2.2, 3.1, 3.2, 6.1, 6.2 and 6.3.

1.3.3 The Data Subjects' rights as mentioned in the preceding Sections 1.3.1 and 1.3.2 shall cover the judicial remedies for any breach of the third-party beneficiary rights guaranteed and the right to obtain redress and where appropriate receive compensation for any damage (material harm but also any distress). In particular, Data Subjects in the EU shall be entitled to lodge a complaint before the competent Supervisory Authority; the Data Subject shall have a choice between the Supervisory Authority of the EU Member State of his/her habitual residence, place of work or place of alleged infringement. Data Subjects in the EU shall be entitled also to lodge a complaint before the competent court, with a choice for the Data Subject to act before the courts where the Controller or Processor has an establishment or where the Data Subject has his or her habitual residence pursuant to Article 79 of the GDPR.

1.3.4 Where a member of the Workday Group and the Controller involved in the same Processing are found responsible for any damage caused by such Processing, the Data Subject shall be entitled to receive compensation for the entire damage directly from the respective member of the Workday Group (Art. 82.4 GDPR).

1.4. Responsibility towards the Controller

The BCR shall be made binding toward the Controller through a specific reference to it in the Service Agreement. If and to the extent provided in the Service Agreement, the Controller shall have the right to enforce the BCR against (a) any member of the Workday Group for breaches such member caused, (b) the member of the Workday Group referred under Section 1.5 of these BCR in case of a breach of the BCR or of the Service Agreement by members of the Workday Group established outside of the EEA or a breach of the written agreement referred under Section 6.1.vii of these BCR by any external Sub-processor established outside of the EEA. The Controller's rights shall cover the judicial remedies and the right to receive compensation, as further specified in the applicable Service Agreement.

1.5 The Workday Group accepts liability for paying compensation and to remedy breaches of the BCR

1.5.1 The Workday Group has appointed Workday Limited, Kings Building, May Lane, Dublin 7, Ireland to accept responsibility for and agrees to take the necessary action to remedy the acts of other members of the Workday Group established outside of the EEA or breaches caused by any external Sub-processor established outside of the EEA and to pay compensation for any damages resulting from the violation of the BCR to the Controller pursuant to the Service Agreement.

1.5.2 Workday Limited will accept liability as if the violation had taken place by itself in the EEA member state in which it is based instead of the member of the Workday Group outside the EEA or the external Sub-processor established outside of the EEA. Workday Limited may not rely on a breach by a Sub-processor (internal or external of the Workday Group) of its obligations in order to avoid its own liabilities.

1.6 Members of the Workday Group accepting liability have sufficient assets

The Workday Group will ensure that Workday Limited has sufficient assets to pay compensation for damages resulting from the breach of the BCR.

1.7 The burden of proof lies with the Workday Group not the individual Data Subject

1.7.1 Workday Limited will have the burden of proof that the member of the Workday Group outside of the EEA or the external Sub-processor is not liable for any violation of the BCR which has resulted in the Data Subject claiming damages.

1.7.2 Where the Controller can demonstrate that it suffered damage and establish facts which show it is likely that the damage has occurred because of the breach of the BCR, it will be for Workday Limited to prove that the member of the Workday Group outside of the EEA or the external Sub-processor was not responsible for the breach of the BCR giving rise to those damages or that no such breach took place.

1.7.3 If Workday Limited can prove that the member of the Workday Group outside the EEA or the external Sub-processor is not responsible for the act, it may discharge itself from any responsibility/liability.

1.8 Easy access to the BCR and third-party beneficiary rights for the Data Subjects

If a Controller agrees in a Service Agreement that the BCR are part of the contract with one or more members of the Workday Group, then the BCR will be annexed to the Service Agreement or a reference to it will be made with a possibility of electronic access. The Controller shall, in particular, provide all Data Subjects benefiting from the third-party beneficiary rights with the information on their third-party beneficiary rights with regard to the Processing of their Personal Data and on the means to exercise those rights. Every Data Subject shall have easy access to the BCR. The Workday Group will publish Sections 1.1, 1.3, 1.4, 1.6, 1.7, 2.2, 3.1, 3.2, 4.1, 4.2, 6.1, 6.2, 6.3 of the BCR on a website of the Workday Group in a way easily accessible to Data Subjects.

2. Effectiveness

2.1 Training program

The Workday Group will ensure that its personnel who are regularly engaged in the Processing of Personal Data or in the development of tools used to Process Personal Data are informed of the confidential nature of Personal Data and have received appropriate training on their responsibilities under the BCR. Specifically, the Workday Group provides privacy and security training to all employees during their onboarding process and also provides annual privacy and security training to personnel of the Workday Group with access to unencrypted Personal Data.

2.2 Complaint handling process

The Workday Group has delegated the Chief Privacy Officer as the specific point of contact who can be reached at privacy@workday.com in the event that Data Subjects contact the Workday Group directly. However, in accordance with the Service Agreement of the Workday Group with Controllers, the Workday Group will, without undue delay, forward complaints related to the Processing of or access to Personal Data from Data Subjects to the respective Controller, provided that the Data Subject has given sufficient information for the Workday Group to identify the Controller.

The Workday Group will handle complaints from Data Subjects where the responsible Controller has disappeared factually or has ceased to exist in law or become insolvent. In such cases, and provided that the Workday Group still maintains the Data Subjects' Personal Data (*i.e.*, it has not been deleted following termination of the Service Agreement), these complaints shall be timely handled by the Workday Group's Chief Privacy Officer or another clearly identified department or person who has an appropriate level of independence in the exercise of his/her functions.

If and when the conditions in this section are met, Data Subjects who contact the Workday Group at privacy@workday.com will be informed where to complain, in which form, the timescale for the reply on the complaint, consequences in case of rejection of the complaint, consequences in case the complaint is considered as justified, and consequences if the Data Subject is not satisfied by the replies (right to lodge a claim before the competent court/Supervisory Authority). In the event that the Workday Group no longer maintains the Personal Data, the Data Subject will be informed accordingly.

2.3 Audit program

The Workday Group conducts data protection audits on a regular basis by internal and external accredited auditors as well as on specific requests from the Chief Privacy Officer or the Workday Group's internal audit department. The audit program covers all aspects of the BCR, including methods of ensuring that corrective actions will take place. The Workday Group's Chief Privacy Officer and Workday, Inc.'s board of directors have access to audit reports.

Controllers have access to third-party audit reports of the Workday Group and may conduct their own audit in accordance with the Customer Audit Program and the applicable Service Agreement of the Workday Group.

Supervisory Authorities have the power to audit members of the Workday Group under applicable law. Upon request, The Workday Group will make available to the competent Supervisory Authority any audit reports that the Workday Group issues generally to all Controllers. With respect to Controller-specific audit reports, Supervisory Authorities with jurisdiction over the Controller can request access to the results of the Workday Group's audit reports from the Controller and carry out data protection audits themselves if required and legally possible. The Workday Group will also comply with any court order or other formal order that compels the Workday Group to make Controller-specific audit reports available to the competent Supervisory Authority.

The Workday Group will accept, at the request of a Controller and in accordance with the Service Agreement and the Customer Audit Program of the Workday Group, to submit their data processing facilities for audit of the Processing activities relating to that Controller. Any audits of Sub-processors with access to Personal Data will be coordinated through the Workday Group and in accordance with the Service Agreement and the Customer Audit Program of the Workday Group.

2.4 Network of privacy personnel for handling complaints and compliance

The Workday Group has appointed, and will continue to appoint, a data protection officer (DPO) where required in line with Art. 37 GDPR, as well as a Chief Privacy Officer (CPO) and appropriate staff in the privacy compliance team. These individuals benefit from the support of the Workday Group's highest management. Along with a network of privacy contacts at key locations and subsidiaries within the Workday Group, the privacy compliance team is responsible for reporting complaints and compliance issues to the Workday Group's DPO and CPO and assisting the DPO and CPO with local fact-finding, investigations, and implementation of and training on data privacy measures.

The Workday Group's DPO and CPO advise the executives of the Workday Group as appropriate and work with the privacy compliance team to deal with Supervisory Authorities' investigations, annually report on compliance, and ensure compliance at a global level.

3. Cooperation duty

3.1 Duty to cooperate with Supervisory Authorities

All members of the Workday Group shall cooperate with, and accept to be audited by, the Supervisory Authorities competent for the relevant Controller and comply with applicable law and the advice of these Supervisory Authorities on any issue related to the BCR.

3.2 Duty to cooperate with Controllers

The Workday Group and any Sub-processor shall cooperate and assist Controllers to comply with data protection law, such as the Controller's duty to respect the Data Subject rights or to handle their complaints, or to be in a position to reply to an investigation or inquiry from Supervisory Authorities, subject to the applicable Service Agreement. This shall be done in a reasonable time and to the extent reasonably possible and as agreed upon in the applicable Service Agreement.

4. Description of processing and data flows

4.1 Transfers and material scope covered by the BCR

All members of the Workday Group listed on Schedule 1 have agreed to the BCR within the scope and for the types of transfers of Personal Data specified in Article I of these BCR.

4.2 Geographical scope of the BCR (nature of Personal Data, type of Data Subjects, countries)

The structure and contact details of the Workday Group and its individual members is specified in Schedule 1. It is up to the Controller to require that the BCR apply to (i) all Personal Data Processed for Processor activities and that are submitted to EU law (for instance, data has been transferred from the European Union), or to (ii) all Processing of Personal Data Processed for Processor activities within the Workday Group whatever the origin of the Personal Data, subject to the terms of the Service Agreement.

5. Mechanisms for reporting and recording changes

5.1 A process for updating the BCR

The BCR can be modified, for instance, to take into account modifications of the regulatory environment or the company structure. The Workday Group shall report changes to all members of the Workday Group, the Supervisory Authority that approved the BCR and the Controllers whose Service Agreements include the BCR. Where a change affects the Processing conditions, the Workday Group will notify the Controllers through a communication to Workday's general customer base such as notification through Workday's community portal in such a timely fashion that Controllers have the possibility to object to the change or to terminate the Service Agreement in accordance with its terms.

The Workday Group's privacy compliance team keeps a fully updated list of the members of the Workday Group and of the Sub-processors involved in the Personal Data Processing activities for each Controller which shall be made accessible to each covered Controller, Data Subject and Supervisory Authority. In accordance with the Privacy and Compliance Policy of the Workday Group, the Workday Group's privacy compliance team will keep track of and record any updates to the BCR and provide the necessary information systematically to Controllers and upon request to competent Supervisory Authorities. With respect to Personal Data covered by the BCR, no transfer is made to a new member of the Workday Group until the new member is effectively bound by the BCR and can deliver compliance. Any changes to the BCR or to the list of members of the Workday Group shall be reported once a year to the Supervisory Authorities granting authorizations to the Workday Group with a brief explanation of the reasons justifying the update. Where a modification would affect the level of the protection offered by the BCR or significantly affect the BCR (i.e. changes in the bindingness), it must be promptly communicated to the relevant Supervisory Authorities via the competent Supervisory Authority granting authorizations to the Workday Group.

6. Data protection safeguards

6.1 Privacy principles

The BCR include the following principles, applicable to any member of the Workday Group with respect to Personal Data and Controllers covered by the BCR in accordance with the applicable Service Agreement which addresses procedural, operational and commercial arrangements, such as compensation for additional services that a Controller may request as part of assistance with the Controller's compliance obligations under these privacy principles and applicable law. The privacy principles describe obligations of a Processor and Sub-processor in the Workday Group as well as obligations of a Controller, i.e. a customer of the Workday Group. Controllers, i.e. customers of the Workday Group, are not directly bound by these principles (only members of the Workday Group are directly bound), but if a Controller agrees to transfer Personal Data to the Workday Group under a Service Agreement that refers to these BCR, then the Controller agrees also to its obligations under these BCR.

i) Transparency, fairness and lawfulness: The Workday Group and any applicable Sub-processors will have a general duty to help and assist Controllers to comply with the law (for instance, to be transparent about Sub-processor activities in order to allow the Controller to correctly inform the Data Subject).

ii) Purpose limitation: The Workday Group and any applicable Sub-processors shall Process Personal Data only on behalf of the Controller and in compliance with its instructions including with regard to transfers of Personal Data to a third country, unless required to do so by Union or Member State law to which the Workday Group or its Sub-processor is subject. In such a case, the Workday Group or its Sub-processor shall inform the Controller of that legal requirement before Processing takes place, unless that law prohibits such information on important grounds of public interest (Art. 28-3-a GDPR). In other cases, if the Workday Group or its Sub-processor cannot provide such compliance for whatever reasons, they will promptly inform the Controller of their inability to comply, in which case the Controller is entitled to suspend the transfer of Personal Data.

On the termination of the provision of data processing services, the Workday Group and its Sub-processors shall, at the choice of the Controller and in accordance with the terms of the applicable Service Agreement, delete or return all Personal Data to the Controller (for example, by way of providing the Controller with administrative access to the databases of the Workday Group) and delete the copies thereof, unless legislation imposed upon them requires storage of the Personal Data. In that case, the Workday Group and its Sub-processors will inform the Controller and warrant that they will safeguard the confidentiality of the Personal Data and will not actively Process the Personal Data anymore, except as otherwise instructed by the Controller.

iii) Data quality: The Workday Group and any applicable Sub-processors shall assist the Controller to comply with the law, in particular:

- The Workday Group will, when asked by a Controller, at the election of the Workday Group and as necessary under applicable law, either (1) provide the Controller with the ability to update, correct or delete Personal Data; or (2) make such updates, rectifications or deletions on the Controller's behalf. If any rectification or deletion of Personal Data is not reflected in the service of the Workday Group, the Workday Group and its Sub-processors will inform - or enable Controllers to inform - each member of the Workday Group to whom the Personal Data have been disclosed of such rectification, or deletion of the Personal Data.

- When asked by a Controller, the Workday Group and its Sub-processors will execute necessary measures in accordance with the Service Agreement to enable or assist the Controller to have Personal Data deleted or anonymized when the Personal Data is no longer needed in a form that identifies the Data Subjects. If any deletion or anonymization of Personal Data is not reflected in the service of the Workday Group, the Workday Group and its Sub-processors will communicate - or enable Controllers to communicate - to each member of the Workday Group to whom the Personal Data have been disclosed of any deletion or anonymization of the Personal Data.

iv) Security: The Workday Group and any applicable Sub-processors comply with the Workday Group's security and organizational measures set forth in the Service Agreement to ensure a level of security appropriate to the risks

presented by the Processing as provided by Art. 32 GDPR. The Workday Group and its Sub-processors will assist Controllers in ensuring compliance with the obligations as set out in Art. 32 to 36 GDPR taking into account the nature of Processing and information available to the Workday Group and its Sub-processors (Art. 28.3.f GDPR) in accordance with the Service Agreement. The Workday Group shall inform Controllers without undue delay after becoming aware of any Personal Data Breach affecting the Personal Data Processed on their behalf. In addition, the Sub-processors of the Workday Group shall inform Workday Group without undue delay after becoming aware of any Personal Data Breach affecting the Personal Data Processed on their behalf.

v) Data Subject rights: When asked by a Controller, the Workday Group and any applicable Sub-processors will execute any appropriate technical and organizational measures, insofar as this is possible and as agreed in the Service Agreement, for the fulfilment of the Controller's obligations to respond to requests for exercising the Data Subjects rights as set out in Chapter III of the GDPR (Art. 28.3.e GDPR) ("**Data Subject Request**") including by communicating any useful information in order to help the Controller to comply with the duty to respect the rights of the Data Subjects. If a Data Subject submits a Data Subject Request to the Workday Group or a Sub-processor and the Workday Group can identify the Controller, the Workday Group shall transmit such requests to the responsible Controller. The Workday Group shall not respond to any such Data Subject Request except to confirm to the Data Subject that the request relates to that Controller.

vi) Sub-processing within the Group: Personal Data may be sub-processed by other members of the Workday Group bound by the BCR only with the prior informed specific or general written authorization of the Controller. The Service Agreement will specify if a general prior authorization given at the beginning of the service would be sufficient or if a specific authorization will be required for each new Sub-processor. If a general authorization is given, the Controller will be informed by Workday Group of any intended changes concerning the addition or replacement of a Sub-processor in such a timely fashion that the Controller has the possibility to object to the change or to terminate the contract before the Personal Data are communicated to the new Sub-processor.

vii) Onward transfers to external Sub-processors: Personal Data may be sub-processed by non-members of the Workday Group only with the prior informed specific or general written authorization of the Controller. The Service Agreement will specify if a general prior authorization given at the beginning of the service would be sufficient or if a specific authorization will be required for each new Sub-processor. If a general authorization is given, the Controller will be informed by the Workday Group of any intended changes concerning the addition or replacement of Sub-processors in such a timely fashion that the Controller has the possibility to object to the change or to terminate the Personal Data Processing by the Workday Group before the Personal Data are communicated to the new Sub-processor.

Where the member of the Workday Group bound by the BCR subcontracts its obligations under the Service Agreement, with the authorization of the Controller, it shall do so only by way of a written contract or other legal act under Union or Member State law with the Sub-processor which ensures that adequate protection is provided as set out in Art. 28, 29, 32, 45, 46 GDPR and that either (i) the same data protection obligations as set out in the Service Agreement between the Controller and the Workday Group and Sections 1.3, 1.4, 3 and 6 of these BCR are imposed on the Sub-processor, or that (ii) other appropriate safeguards referred to in Art. 46.2 GDPR (including, without limitation, standard data protection clauses adopted by the European Commission per Art. 46.2.c GDPR) are properly implemented with the Sub-processor, in particular providing, in either case, sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the Processing will meet the requirements of the GDPR (Art. 28.4 GDPR).

6.1.2 Accountability and other tools

The Workday Group shall, in accordance with the Service Agreement and the Customer Audit Program of the Workday Group, make available to Controllers all information necessary to demonstrate compliance with its obligations as provided by Article 28.3.h GDPR and allow for and contribute to audits, including inspections conducted by the respective Controller or another auditor mandated by the Controller. In addition, the Workday Group shall immediately inform a Controller if, in its opinion, an instruction infringes the GDPR or other Union or Member State data protection provisions.

In order to demonstrate compliance with these BCR, members of the Workday Group maintain records of all categories of Processing activities carried out on behalf of Controllers in line with the requirements as set out in Art. 30.2 GDPR.

The members of the Workday Group shall also assist the Controller in implementing appropriate technical and organizational measures to comply with data protection principles and facilitate compliance with the requirements set up by the BCR in practice such as data protection by design and by default (Art. 25 and 47.2.d GDPR) by implementing the controls set forth in Workday's third-party audit reports.

6.2 The list of entities bound by BCR

Schedule 1 lists the members of the Workday Group bound by the BCR.

6.3 Transparency regarding conflicts between national legislation and the BCR

Where a member of the Workday Group has reasons to believe that the existing or future legislation applicable to it may prevent it from fulfilling the instructions received from the Controller or its obligations under the BCR or the Service Agreement, it will promptly notify this to (i) the Chief Privacy Officer of the Workday Group, who shall promptly inform the Controller, which is entitled to suspend the transfer of Personal Data and/or terminate the contract (or affected portions of a contract, as applicable and subject to the terms of the Service Agreement), and to (ii) the Supervisory Authority competent for the member of the Workday Group making the notification.

Any legally binding request for disclosure of the Personal Data by a law enforcement authority or a state security body shall be communicated to the Controller unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation. If communication with the Controller is prohibited, the member of the Workday Group shall inform its competent Supervisory Authority about the request, including information about the Personal Data requested, the requesting body and the legal basis for disclosure (unless otherwise prohibited).

If in specific cases the suspension and/or notification are prohibited, the requested member of the Workday Group will use its best efforts to obtain the right to waive this prohibition in order to communicate as much information as it can and as soon as possible, and be able to demonstrate that it did so.

In any case, transfers of Personal Data by a member of the Workday Group to any public authority cannot be massive, disproportionate and indiscriminate in a manner that would go beyond what is necessary in a democratic society.

6.4 The relationship between national laws and BCR

Where local legislation, for instance EU legislation, requires a higher level of protection for Personal Data it will take precedence over the BCR. At all times, Personal Data shall be Processed in accordance with applicable law. The Controller shall notify the Workday Group about any additional or higher data protection law requirements applicable to the Controller and its Personal Data.

7. Schedules incorporated into these BCR

Schedule 1 lists the members of the Workday Group bound by these BCR, as amended from time to time in accordance with the BCR.

Schedule 2 describes Workday's technical and organizational data security measures.

Schedule 1

Members of the Workday Group bound by the BCR (as of May 29, 2020, as amended from time to time)

1. The Workday Group can be contacted via its privacy compliance team using the following contact details:

Workday Limited
Attn.: Privacy
Kings Building
May Lane
Dublin 7 Ireland

privacy@workday.com

2. The individual members of the Workday Group and their respective contact details are set forth in the table below:

Member	Country	Contact Details
Workday, Inc.	USA	6110 Stoneridge Mall Road Pleasanton, CA 94588 USA
Canada Workday ULC	Canada	1515 Douglas Street Suite 600 Victoria, BC V8W 1P6 Canada
Workday Asia Pacific Limited	Hong Kong	Suite 3301-04, 33/F, Tower One Times Square 1 Matheson St., Causeway Bay, Hong Kong
Workday Australia Pty Ltd	Australia	Level 12 100 Pacific Highway North Sydney NSW 2060, Australia
Workday Austria GmbH	Austria	Regus Opera Kärntner Ring 5-7, 7th floor 1010 Vienna Austria
Workday B.V.	Netherlands	Gustav Mahlerplein 82 1082 MA Amsterdam The Netherlands
Workday (Beijing) Co. Ltd.	People's Republic China	1133, 11/F Beijing Kerry Center North Tower, 1 Guang Hua Rd, Chaoyang District, Beijing, People's Republic of China 100020 China
Workday Belgium SPRL	Belgium	Spaces Mercier Square Kardinaal Mercierplein 2 Mechelen, 2800 Belgium
Workday CZ s.r.o	Czech Republic	Italská 2584/69 Vinohrady 120 00 Prague 2

		Czech Republic
Workday Denmark ApS	Denmark	Harsdorffs Hus Office Club Kongens Nytorv 5 1050 Copenhagen Denmark
Workday España SL	Spain	Torre Espacio Paseo de la Castellana No. 259D Floor 21N Madrid 28046 Spain
Workday Finland Oy	Finland	Mikonkatu 9 00100 Helsinki Finland
Workday France	France	7-11 boulevard Haussmann 75009 Paris France
Workday Global, Inc.	USA	6110 Stoneridge Mall Road Pleasanton, CA 94588 USA
Workday GmbH	Germany	Streitfeldstrasse. 19 81673 Munich Germany
Workday India Private Limited	India	CoWrks 3rd Floor, Prudential Building Prudential IT Park, Central Avenue, Powai Mumbai, Maharashtra 400076 India
PT Workday Indonesia Services	Indonesia	c/o JustCo The Plaza Office Tower Level 7 Jalan MH Thamrin Kav 28 – 30 Jakarta 10350
Workday International Limited	Ireland	6th Floor 2 Grand Canal Square Dublin 2 Ireland
Workday Italy S.r.l.	Italy	Bastioni di Porta Nuova, 21 Milan 20121 Italy
Workday K.K.	Japan	Shin-Aoyama Tokyu Building 7F 3-11-13 Minami-Aoyama Minato-ku Tokyo 107-0062 Japan
Workday Korea Limited	South Korea	14F Gangnam N Tower, 129, Teheran-ro, Gangnam-gu, Seoul, 06133 South Korea
Workday Latvia SIA	Latvia	Riga Marijas iela 13 k-2 - 3 LV-1050

		Latvia
Workday Limited	Ireland	Kings Building May Lane Dublin 7 Ireland
Workday Malaysia Sdn.Bhd.	Malaysia	Level 35-02 (East Wing), Q Sentral, 2A Jalan Stesen Sentral 2, Kuala Lumpur Sentral, 50470 Kuala Lumpur, Malaysia
Workday Mexico S. de R.L. de C.V.	Mexico	375 Lago Alberto, Suite 18-103 Ciudad de México, CDMX 11320 Mexico
Workday Norway AS	Norway	Dronning Eufemias gate 16, 7th floor 0191 Oslo Norway
Workday Polska sp. Z o.o.	Poland	Varso Tower Chmielna 73 00-801 Warszawa Poland
Workday Singapore Pte. Ltd.	Singapore	1 Wallich Street #09-01 Guoco Tower Singapore 078881
Workday South Africa (Pty) Ltd	South Africa	9th Fl., 5th Street, Sandton Johannesburg, 2146 South Africa
Workday Sweden Aktiebolag	Sweden	Östra Järnvägsgatan 27, 9th floor 111 20 Stockholm Sweden
Workday Switzerland GmbH	Switzerland	Bleicherweg 10 8002 Zurich Switzerland
Workday (NZ) Unlimited	New Zealand	Level 2 152 Fanshawe St, Westhaven, Auckland 1010 New Zealand
Workday (Thailand) Co., Ltd	Thailand	8, T-One Building, Floor 20, Sukhumvit Rd. Soi 40, Phra Khanong, Khlong Toei, Bangkok, 10110 Thailand
Workday (UK) Limited	United Kingdom	Finsbury Circus House, 3rd Floor, 15 Finsbury Circus and 10 South Place London, EC2M 7EB United Kingdom
Adaptive Insights Co., Ltd.	Japan	Shin-Aoyama Tokyu Building 7F 3-11-13 Minami-Aoyama, Minato-ku Tokyo, 107-0062 Japan
Adaptive Insights Limited	United Kingdom	Finsbury Circus House, 3rd Floor 15 Finsbury Circus and 10 South Place

		London EC2M7EB United Kingdom
Adaptive Insights LLC	USA	2300 Geng Road, Suite 100 Palo Alto, CA 94303 USA
Adaptive Insights, Ltd.	Canada	1515 Douglas Street Victoria BC V8W 1P6 Canada
Adaptive Insights Pty Ltd.	Australia	Level 8, 140 Ann Street Brisbane QLD 4000 Australia

Schedule 2
Workday's technical and organizational data security measures

WORKDAY UNIFIED SECURITY EXHIBIT

This Workday Unified Security Exhibit applies to the Covered Service and Covered Data. Capitalized terms used herein have the meanings given in the Agreement, including attached exhibits, that refers to this Workday Unified Security Exhibit.

Workday maintains a comprehensive, written information security program that contains administrative, technical, and physical safeguards that, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing of Covered Data as well as the associated risks, are appropriate to (a) the type of information that Workday will store as Covered Data; and (b) the need for security and confidentiality of such information. Workday's security program is designed to:

- Protect the confidentiality, integrity, and availability of Covered Data in Workday's possession or control or to which Workday has access;
- Protect against any anticipated threats or hazards to the confidentiality, integrity, and availability of Covered Data;
- Protect against unauthorized or unlawful access, use, disclosure, alteration, or destruction of Covered Data;
- Protect against accidental loss or destruction of, or damage to, Covered Data; and
- Safeguard information as set forth in any local, state or federal regulations by which Workday may be regulated.

Without limiting the generality of the foregoing, Workday's security program includes:

1. Security Awareness and Training. Mandatory employee security awareness and training programs, which include:

a) Training on how to implement and comply with its information security program; and

b) Promoting a culture of security awareness.

2. Access Controls. Policies, procedures, and logical controls:

a) To limit access to its information systems and the facility or facilities in which they are housed to properly authorized persons;
b) To prevent those workforce members and others who should not have access from obtaining access; and
c) To remove access in a timely basis in the event of a change in job responsibilities or job status.

3. Physical and Environmental Security. Controls that provide reasonable assurance that access to physical servers at the data centers housing Covered Data is limited to properly authorized individuals and that environmental controls are established to detect, prevent and control destruction due to environmental extremes.

4. Security Incident Procedures. A security incident response plan that includes procedures to be followed in the event of any security breach of any application or system directly associated with the accessing, processing, storage, communication, or transmission of Covered Data.

5. Contingency Planning. Policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, pandemic flu, and natural disaster) that could damage Covered Data or production systems that contain Covered Data.

6. Audit Controls. Hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic information.

7. Data Integrity. Policies and procedures to ensure the confidentiality, integrity, and availability of Covered Data and to protect it from disclosure, improper alteration, or destruction.

8. Storage and Transmission Security. Security measures to guard against unauthorized access to Covered Data that is being transmitted over a public electronic communications network or stored electronically.

9. Secure Disposal. Policies and procedures regarding the secure disposal of tangible property containing Covered Data, taking into account available technology so that such data cannot be practicably read or reconstructed.

10. Assigned Security Responsibility. Assigning responsibility for the development, implementation, and maintenance of its information security program, including:

a) Designating a security official with overall responsibility;
b) Defining security roles and responsibilities for individuals with security responsibilities; and
c) Designating a Security Council consisting of cross-functional management representatives to meet on a regular basis or other appropriate oversight.

11. Testing. Regularly testing the key controls, systems and procedures of its information security program to validate that they are properly implemented and effective in addressing the threats and risks identified.

12. Monitoring. Network and systems monitoring, including error logs on servers, disks and security events for any potential problems. Such monitoring includes:

a) Reviewing changes affecting systems handling authentication, authorization, and auditing;
b) Reviewing privileged access to Workday production systems processing Covered Data; and
c) Engaging third parties to perform network vulnerability assessments and penetration testing on a regular basis.

13. Change and Configuration Management. Maintaining policies and procedures for managing changes Workday makes to production systems, applications, and databases processing Covered Data. Such policies and procedures include:

a) A process for documenting, testing and approving the patching and maintenance of the Covered Service;
b) A security patching process that requires patching systems in a timely manner based on a risk analysis; and
c) A process for Workday to utilize a third party to conduct web application level security assessments.

These assessments generally include testing, where applicable, for:

i. Cross-site request forgery
ii. Services scanning
iii. Improper input handling (e.g. cross-site scripting, SQL injection, XML injection, cross-site flashing)

iv. XML and SOAP attacks
v. Weak session management
vi. Data validation flaws and data model constraint inconsistencies
vii. Insufficient authentication
viii. Insufficient authorization

14. **Program Adjustments.** Workday monitors, evaluates, and adjusts, as appropriate, the security program in light of:

a) Any relevant changes in technology and any internal or external threats to Workday or the Covered Data;
b) Security and data privacy regulations applicable to Workday; and
c) Workday's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to information systems.