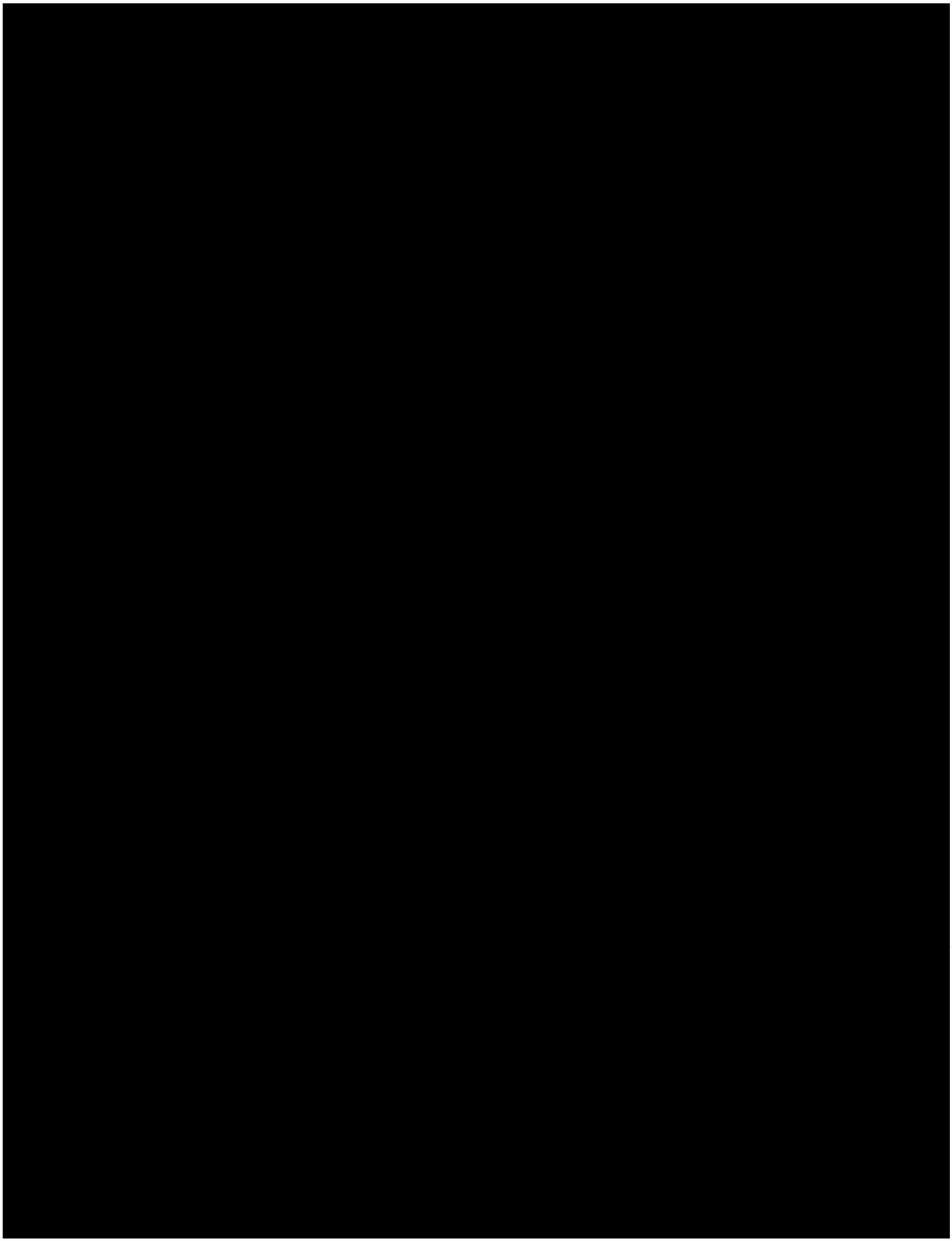
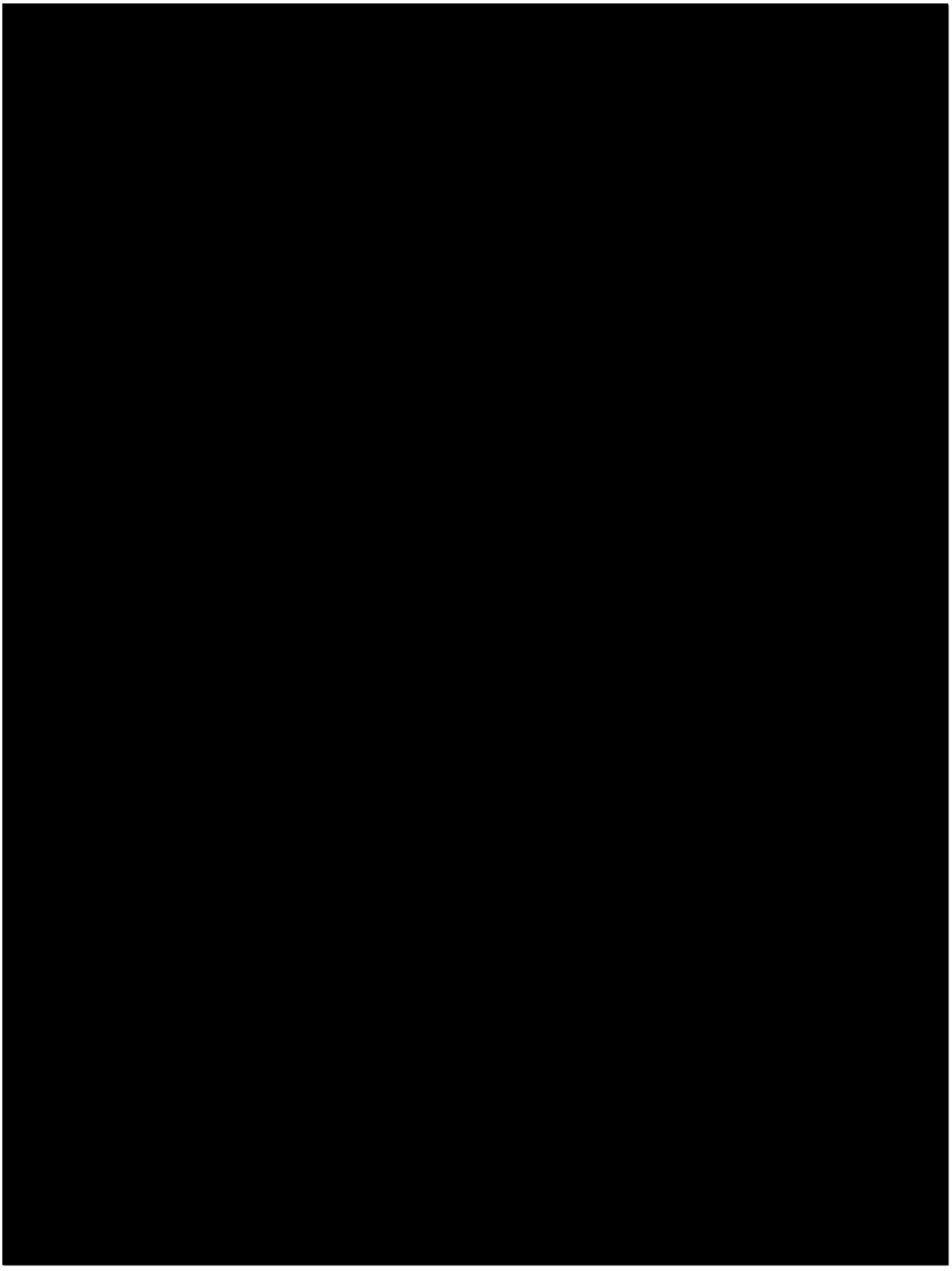
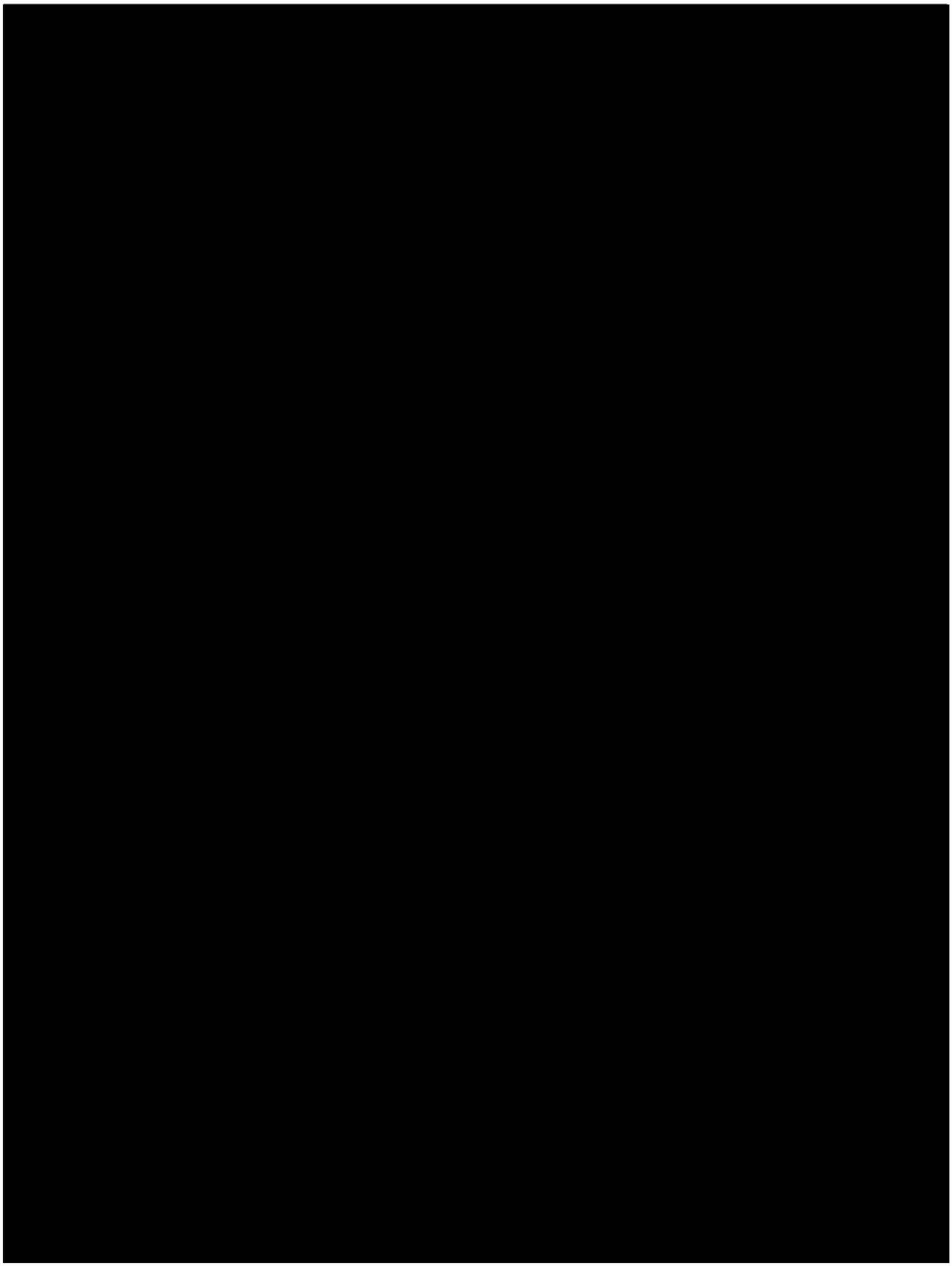
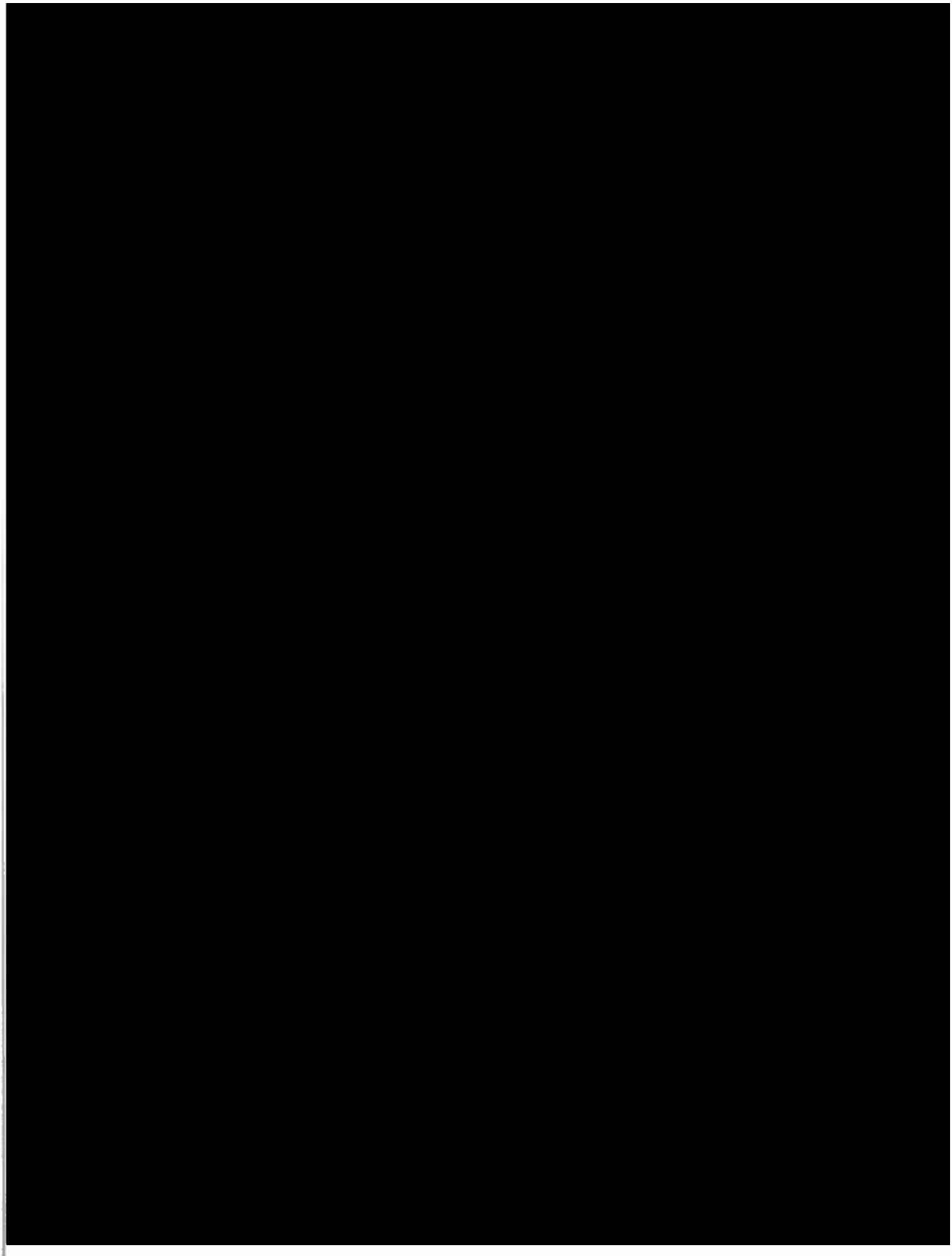
[redacted]









workday.

UNIVERSAL DATA PROCESSING EXHIBIT

This Universal Data Processing Exhibit ("**DPE**") is an exhibit to the Agreement between Workday and Customer and sets forth the obligations of the parties with regard to the Processing of Personal Data pursuant to such Agreement.

1. Definitions

Unless otherwise defined below, all capitalized terms have the meaning given to them in the applicable Agreement and/or exhibits thereto.

"**Agreement**" means the MSA, the Professional Services Agreement, and Order Forms, including any exhibits or attachments applicable to the Covered Service.

"**Covered Data**" means (i) Customer Data, (ii) Professional Services Data, and (iii) any other electronic data or information submitted by or on behalf of Customer to a Covered Service.

"**Covered Service**" means (i) any Service provided under an Order Form that specifically refers to this DPE, and/or, (ii) any Professional Services.

"**Customer Audit Program**" means Workday's optional, fee-based customer audit program as described in the Customer Audit Program Order Form for Covered Services.

"**Data Controller**" means the entity which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

"**Data Processor**" means the entity which Processes Personal Data on behalf of the Data Controller.

"**Data Protection Laws**" means all data protection laws applicable to the Processing of Personal Data under this DPE, including local, state, national and/or foreign laws, treaties, and/or regulations, the GDPR, and implementations of the GDPR into national law.

"**Data Subject**" means the person to whom the Personal Data relates.

"**GDPR**" means the General Data Protection Regulation (EU) 2016/679.

"**Personal Data**" means any Covered Data that relates to an identified or identifiable natural person.

"**Personal Data Breach**" means (i) a 'personal data breach' as defined in the GDPR affecting Personal Data, and (ii) any Security Breach affecting Personal Data.

"**Processing**" or "**Process**" means any operation or set of operations performed on Personal Data or sets of Personal Data, such as collecting, recording, organizing, structuring, storing, adapting or altering, retrieving, consulting, using, disclosing by transmission, disseminating or otherwise making available, aligning or combining, restricting, erasing or destroying.

"**Professional Services**" means the professional or consulting services provided to Customer under a Professional Services Agreement.

"**Professional Services Agreement**" means any agreement between the parties for the provision of consulting or professional services, including but not limited to the following agreements or terms: the Foundation Tenant Service Terms, the Professional Services Agreement, the Delivery Assurance terms, the Professional Services Addendum, and/or the Consulting and Training Addendum and Amendment.

"**Professional Services Data**" means electronic data or information that is provided to Workday under a Professional Services Agreement for the purpose of being input into a Service, or Covered Data accessed within or extracted from the Customer's tenant or instance to perform the Professional Services.

"**Subprocessor**" means a Workday Affiliate or third-party entity engaged by Workday or a Workday Affiliate as a Data Processor under this DPE.

"Subprocessor List" means the subprocessor list identifying the Subprocessors that are authorized to Process Personal Data, accessible through Workday's website (currently located at: https://www.workday.com/en-us/legal/subprocessors.html).

"Workday BCRs" means Workday's Processor Binding Corporate Rules. The Workday BCRs are accessible through Workday's website (currently located at https://workday.com/en-us/why-workday/security-trust.html).

2. Processing Personal Data

2.1 Scope and Role of the Parties. This DPE applies to the Processing of Personal Data by Workday to provide the Covered Service. For the purposes of this DPE, Customer and its Affiliates are the Data Controller(s) and Workday is the Data Processor.

2.2 Instructions for Processing. Workday shall Process Personal Data in accordance with Customer's documented instructions. Customer instructs Workday to Process Personal Data to provide the Covered Service in accordance with the Agreement (including this DPE) and as further specified via Customer's use of the Covered Service. Customer may provide additional instructions to Workday to Process Personal Data, however Workday shall be obligated to perform such additional instructions only if they are consistent with the terms and scope of the Agreement and this DPE.

2.3 Compliance with Laws. Workday shall comply with all Data Protection Laws applicable to Workday in its role as a Data Processor Processing Personal Data. Customer shall comply with all Data Protection Laws applicable to Customer as a Data Controller and shall obtain all necessary consents, and provide all necessary notifications, to Data Subjects to enable Workday to carry out lawfully the Processing contemplated by this DPE.

3. Subprocessors

3.1 Use of Subprocessors. Customer hereby agrees and provides a general prior authorization that Workday and Workday Affiliates may engage Subprocessors. Workday or the relevant Workday Affiliate engaging a Subprocessor shall ensure that such Subprocessor has entered into a written agreement that is no less protective than this DPE. Workday shall be liable for the acts and omissions of any Subprocessors to the same extent as if the acts or omissions were performed by Workday.

3.2 Notification of New Subprocessors. Workday shall make available to Customer a Subprocessor List and provide Customer with a mechanism to obtain notice of any updates to the Subprocessor List. At least thirty (30) days prior to authorizing any new Subprocessor to Process Personal Data, Workday shall provide notice to Customer by updating the Subprocessor List.

3.3 Subprocessor Objection Right. This Section 3.3 shall apply only where and to the extent that Customer is established within the European Economic Area, the United Kingdom or Switzerland or where otherwise required by Data Protection Laws applicable to Customer. In such event, if Customer objects on reasonable grounds relating to data protection to Workday's use of a new Subprocessor then Customer shall promptly, and within fourteen (14) days following Workday's notification pursuant to Section 3.2 above, provide written notice of such objection to Workday. Should Workday choose to retain the objected-to Subprocessor, Workday will notify Customer at least fourteen (14) days before authorizing the Subprocessor to Process Personal Data and Customer may terminate the relevant portion(s) of the Covered Service within thirty (30) days. Upon any termination by Customer pursuant to this Section, Workday shall refund Customer any prepaid fees for the terminated portion(s) of the Covered Service that were to be provided after the effective date of termination.

4. Rights of Data Subjects

4.1 Assistance with Data Subject Requests. Workday will, in a manner consistent with the functionality of the Covered Service and Workday's role as a Data Processor, provide reasonable support to Customer to enable Customer to respond to Data Subject requests to exercise their rights under applicable Data Protection Laws (**"Data Subject Requests"**).

4.2 Handling of Data Subject Requests. For the avoidance of doubt, Customer is responsible for responding to Data Subject Requests. If Workday receives a Data Subject Request or other complaint from a Data Subject regarding the Processing of Personal Data, Workday will promptly forward such request or complaint to Customer, provided the Data Subject has given sufficient information for Workday to identify Customer.

workday.

5. Workday Personnel

Workday shall require screening of its personnel who may have access to Personal Data, and shall require such personnel (i) to Process Personal Data in accordance with Customer's instructions as set forth in this DPE, (ii) to receive appropriate training on their responsibilities regarding the handling and safeguarding of Personal Data; and (iii) to be subject to confidentiality obligations which shall survive the termination of employment.

6. Personal Data Breach

In the event Workday becomes aware of a Personal Data Breach it shall without undue delay notify Customer in accordance with the Security Breach provisions of the MSA. To the extent Customer requires additional information from Workday to meet its Personal Data Breach notification obligations under applicable Data Protection Laws, Workday shall provide reasonable assistance to provide such information to Customer taking into account the nature of Processing and the information available to Workday.

7. Security of Processing

Workday shall implement and maintain appropriate technical and organizational measures to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data as described in the Universal Security Exhibit.

8. Audit

Customer agrees that, to the extent applicable, Workday's then-current SOC 1 and SOC 2 audit reports (or comparable industry-standard successor reports) and/or Workday's ISO 27001 and ISO 27018 Certifications will be used to satisfy any audit or inspection requests by or on behalf of Customer, and Workday shall make such reports available to Customer. In the event that Customer requires additional information, including information necessary to demonstrate compliance with this DPE, or an audit related to the Covered Service, such information and/or audit shall be made available in accordance with Workday's Customer Audit Program.

9. Return and Deletion of Personal Data

Upon termination of the Covered Service, Workday shall return and delete Personal Data in accordance with the relevant provisions of the Agreement.

10. Additional European Terms

10.1 Data Transfers. Workday makes available the transfer mechanisms listed below which shall apply to all transfers of Personal Data from the European Economic Area and/or its member states, the United Kingdom and Switzerland to countries which do not ensure an adequate level of data protection within the meaning of Data Protection Laws of the foregoing countries.

i. **Binding Corporate Rules.** For the Covered Services identified in Addendum B, the Workday BCRs apply to the Processing of Personal Data of a Customer or Customer affiliate established in the European Economic Area, the United Kingdom or Switzerland. In this event, all provisions of the Workday BCRs are incorporated by this reference and shall be binding and enforceable for Customer according to Section 1.4 of the Workday BCRs as if they were set forth in this DPE in their entirety. In the event of any conflict or inconsistency between this DPE and the Workday BCRs, the Workday BCRs shall prevail.

ii. **Standard Contractual Clauses.** The Standard Contractual Clauses set out in Addendum A shall apply between Customer and the Customer Affiliates established within the European Economic Area, the United Kingdom, and Switzerland (each as "data exporter") and Workday, Inc. (as "data importer"), subject to the requirements of Section 11.

iii. **Order of precedence.** Where more than one transfer mechanism applies, the transfer of Personal Data will be subject to a single transfer mechanism in accordance with the following order of precedence: (i) the Workday BCRs, and (ii) the Standard Contractual Clauses.

10.2 Subject-Matter, Nature, Purpose and Duration of Data Processing. Workday will Process Personal Data to provide the Covered Service. The duration of Processing Personal Data shall be for the term of the Agreement.

10.3 Types of Personal Data and Categories of Data Subjects. The types of Personal Data and categories of Data Subjects are set forth in Appendix 1 to the Standard Contractual Clauses, which is hereby incorporated into this DPE by this reference and shall be binding as if it was set forth in this DPE in its entirety.

10.4 Data Protection Impact Assessments and Prior Consultations. Customer agrees that, to the extent applicable, Workday's then-current SOC 1 and SOC 2 audit reports (or comparable industry-standard successor reports) and/or Workday's ISO 27001 and ISO 27018 Certifications will be used to carry out Customer's data protection impact assessments and prior consultations, and Workday shall make such reports available to Customer. To the extent Customer requires additional assistance to meet its obligations under Article 35 and 36 of the GDPR to carry out a data protection impact assessment and prior consultation with the competent supervisory authority related to Customer's use of the Covered Service, Workday will, taking into account the nature of Processing and the information available to Workday, provide reasonable assistance to Customer through the Customer Audit Program.

11. Clarifications to the Standard Contractual Clauses

If Customer executes the Standard Contractual Clauses, the terms in this Section will apply.

11.1 Audits. For the purposes of Clause 5 (f) of the Standard Contractual Clauses, audits will be performed in accordance with Section 8 of this DPE.

11.2 Subprocessors. For the purposes of Clause 11 of the Standard Contractual Clauses, Customer consents to Workday appointing Subprocessors in accordance with Section 3 of this DPE.

11.3 Return and Deletion of Personal Data. For purposes of Clause 12 (1) of the Standard Contractual Clauses, Workday shall return and delete Data Exporter's data in accordance with Section 9 of this DPE.

11.4 Conflict. For the avoidance of doubt, the parties agree that the terms of this Section are not intended to amend or modify the Standard Contractual Clauses. These provisions provide clarity in terms of Workday's business processes for complying with the Standard Contractual Clauses. In the event of any conflict between the terms of this DPE and the provisions of the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail

12. General Provisions

12.1 Customer Affiliates. Customer is responsible for coordinating all communication with Workday on behalf of its Affiliates with regard to this DPE. Customer represents that it is authorized to issue instructions as well as make and receive any communications or notifications in relation to this DPE on behalf of its Affiliates.

12.2 Termination. The term of this DPE will end simultaneously and automatically at the later of (i) the termination of the Agreement or, (ii) when all Personal Data is deleted from Workday's systems.

12.3 Conflict. This DPE is subject to the non-conflicting terms of the Agreement. With regard to the subject matter of this DPE, in the event of inconsistencies between the provisions of this DPE and the Agreement, the provisions of this DPE shall prevail with regard to the parties' data protection obligations.

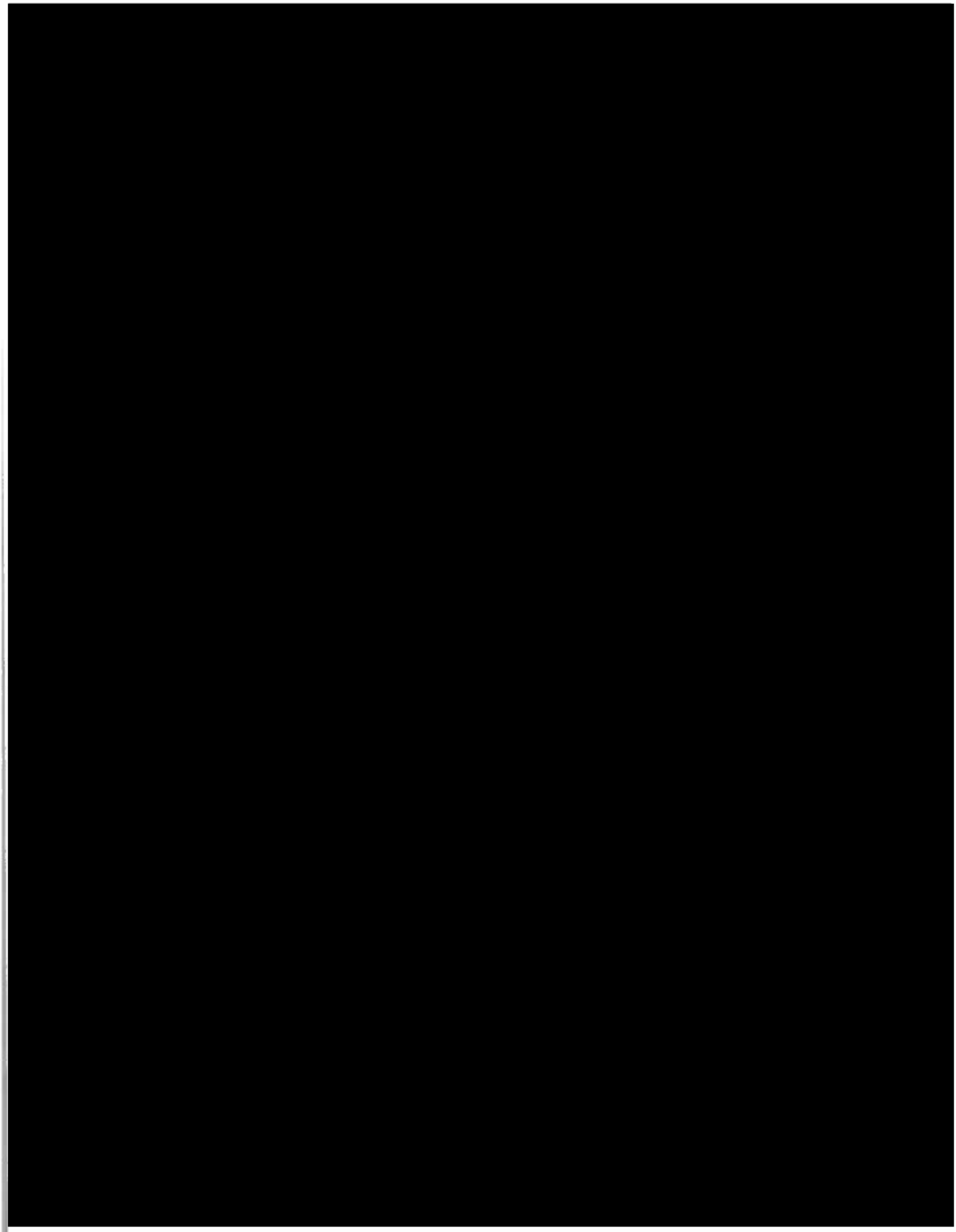
12.4 Customer Affiliate Enforcement. Customer's Affiliates may enforce the terms of this DPE directly against Workday, subject to the following provisions:

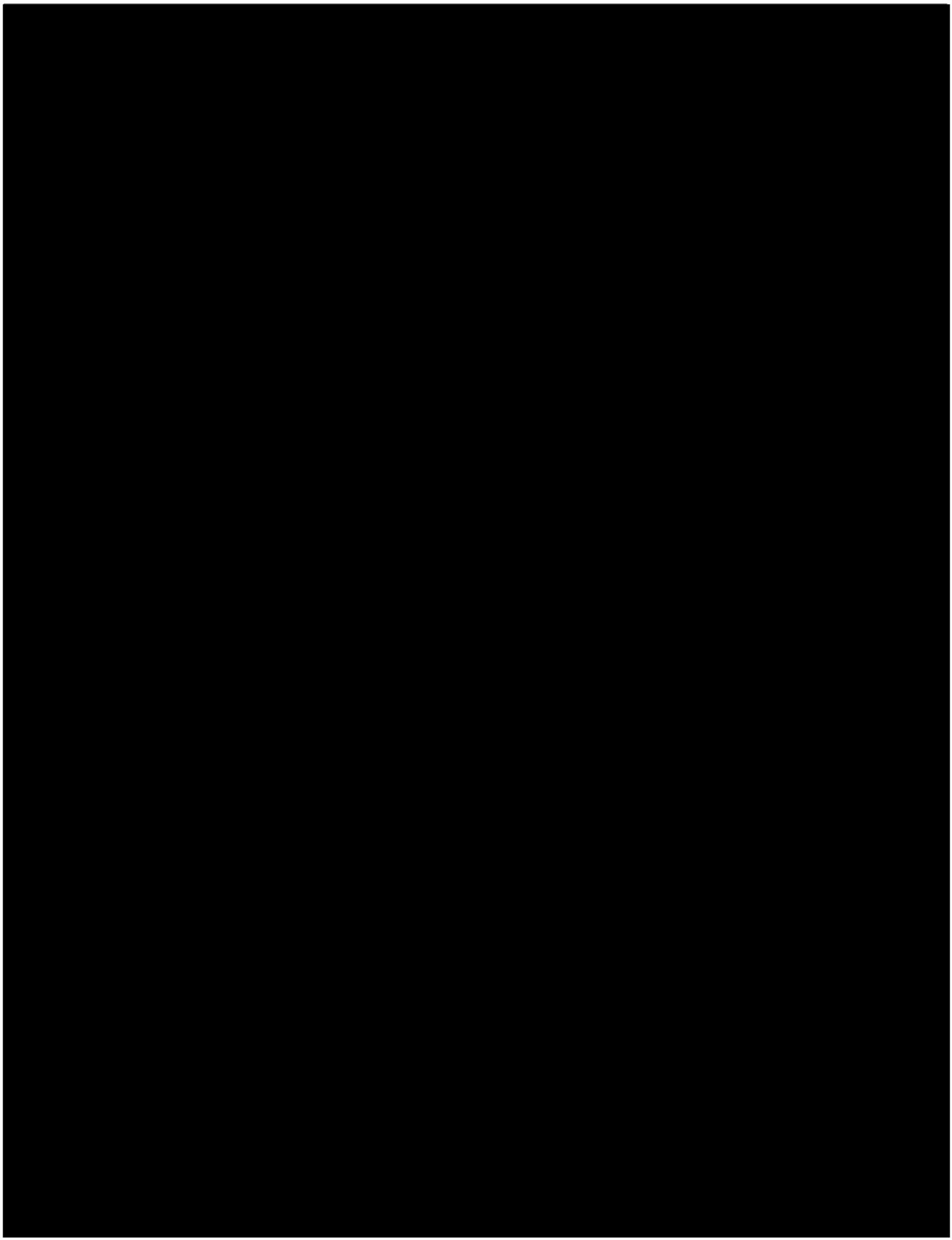
i. Customer will bring any legal action, suit, claim or proceeding which that Affiliate would otherwise have if it were a party to the Agreement (each an "**Affiliate Claim**") directly against Workday on behalf of such Affiliate, except where the Data Protection Laws to which the relevant Affiliate is subject require that the Affiliate itself bring or be party to such Affiliate Claim; and

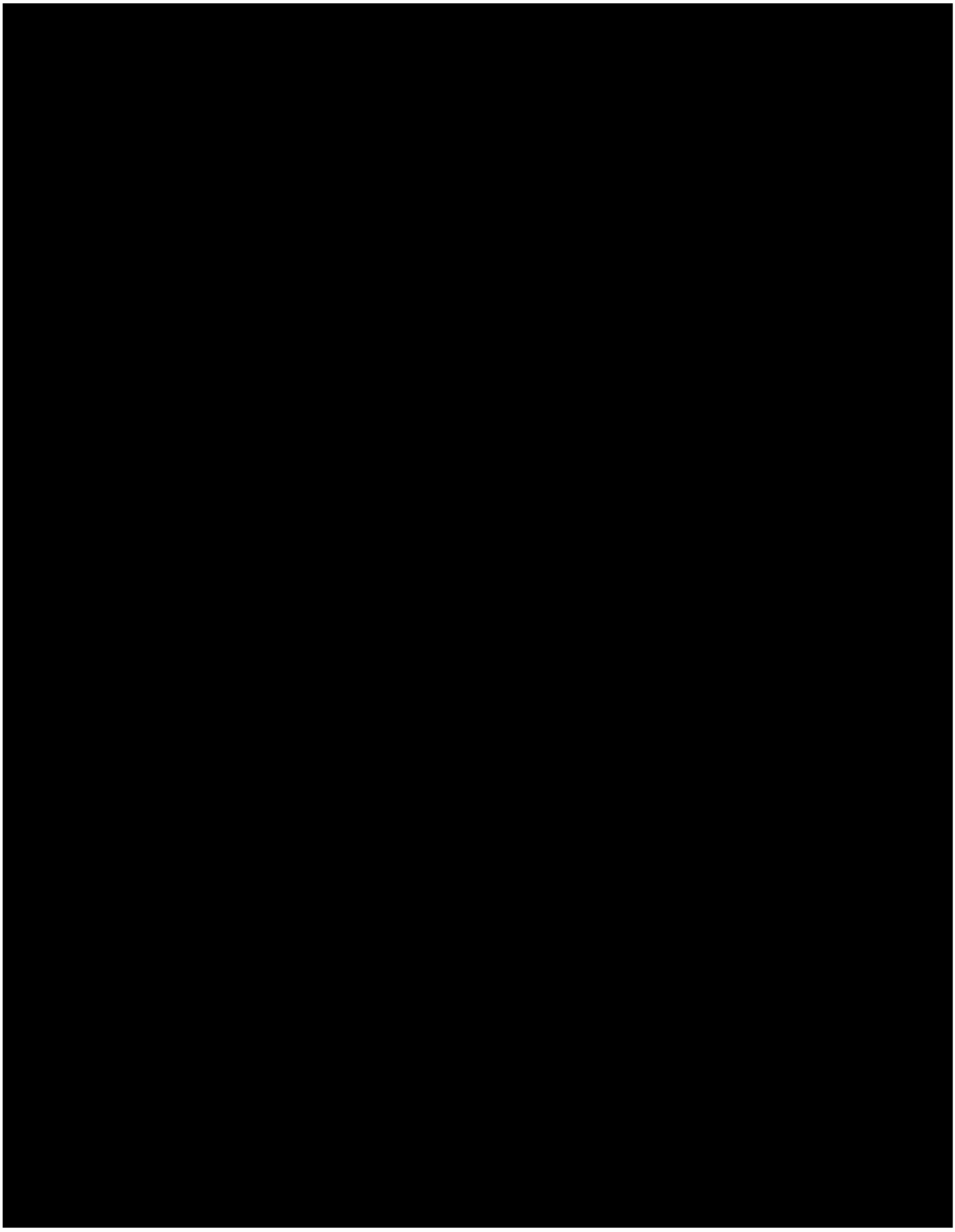
ii. for the purpose of any Affiliate Claim brought directly against Workday by Customer on behalf of such Affiliate in accordance with this Section, any losses suffered by the relevant Affiliate may be deemed to be losses suffered by Customer.

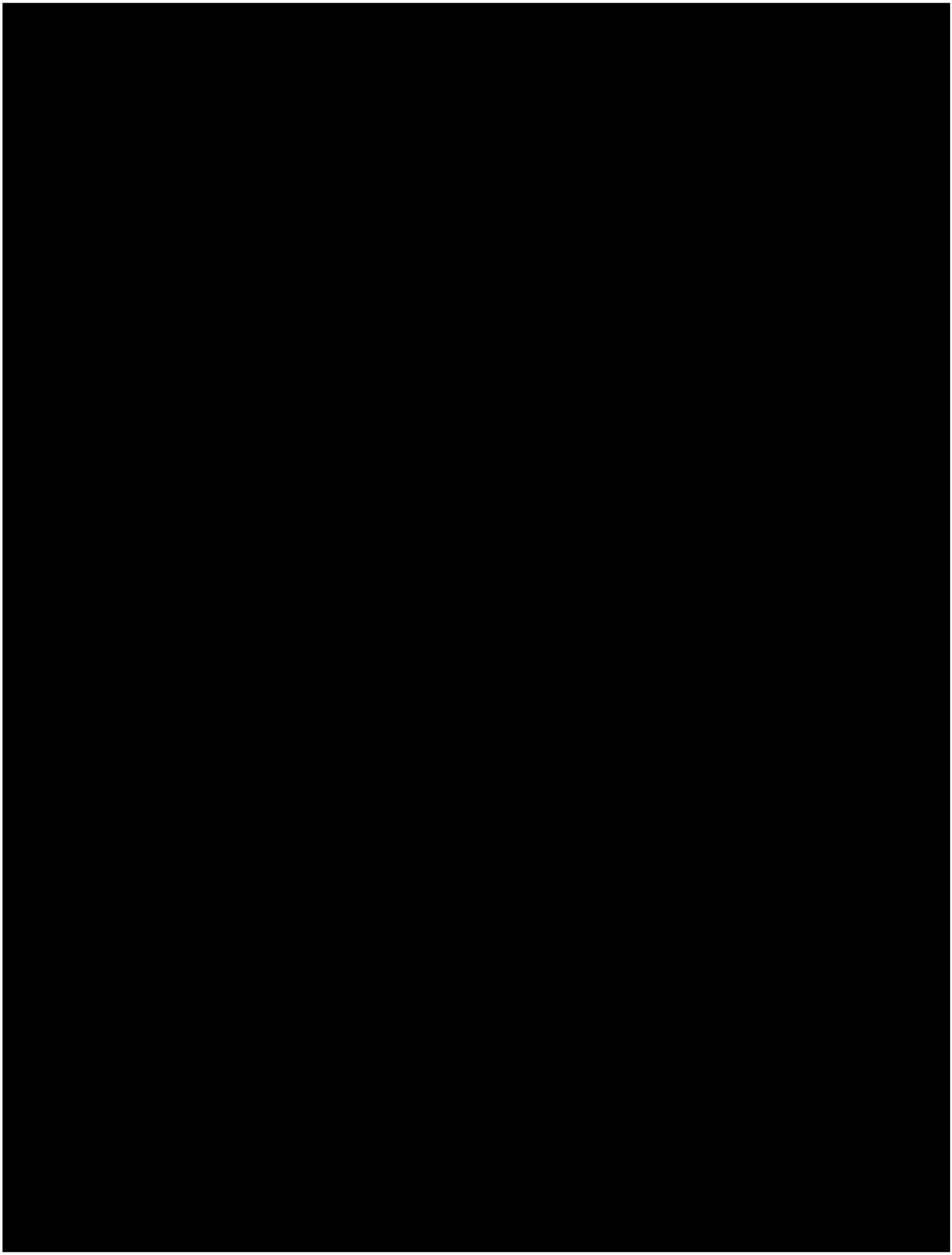
12.5 Remedies. Customer's remedies (including those of its Affiliates) with respect to any breach by Workday or its Affiliates of the terms of this DPE (including the Standard Contractual Clauses), and the overall aggregate liability of Workday and its Affiliates arising out of, or in connection with the Agreement (including this DPE) will be subject to any aggregate limitation of liability that has been agreed between the parties under the Agreement (the "**Liability Cap**"). For the avoidance of doubt, the parties intend and agree that the overall aggregate liability of Workday and its Affiliates arising out of, or in connection with the Agreement (including this DPE) shall in no event exceed the Liability Cap.

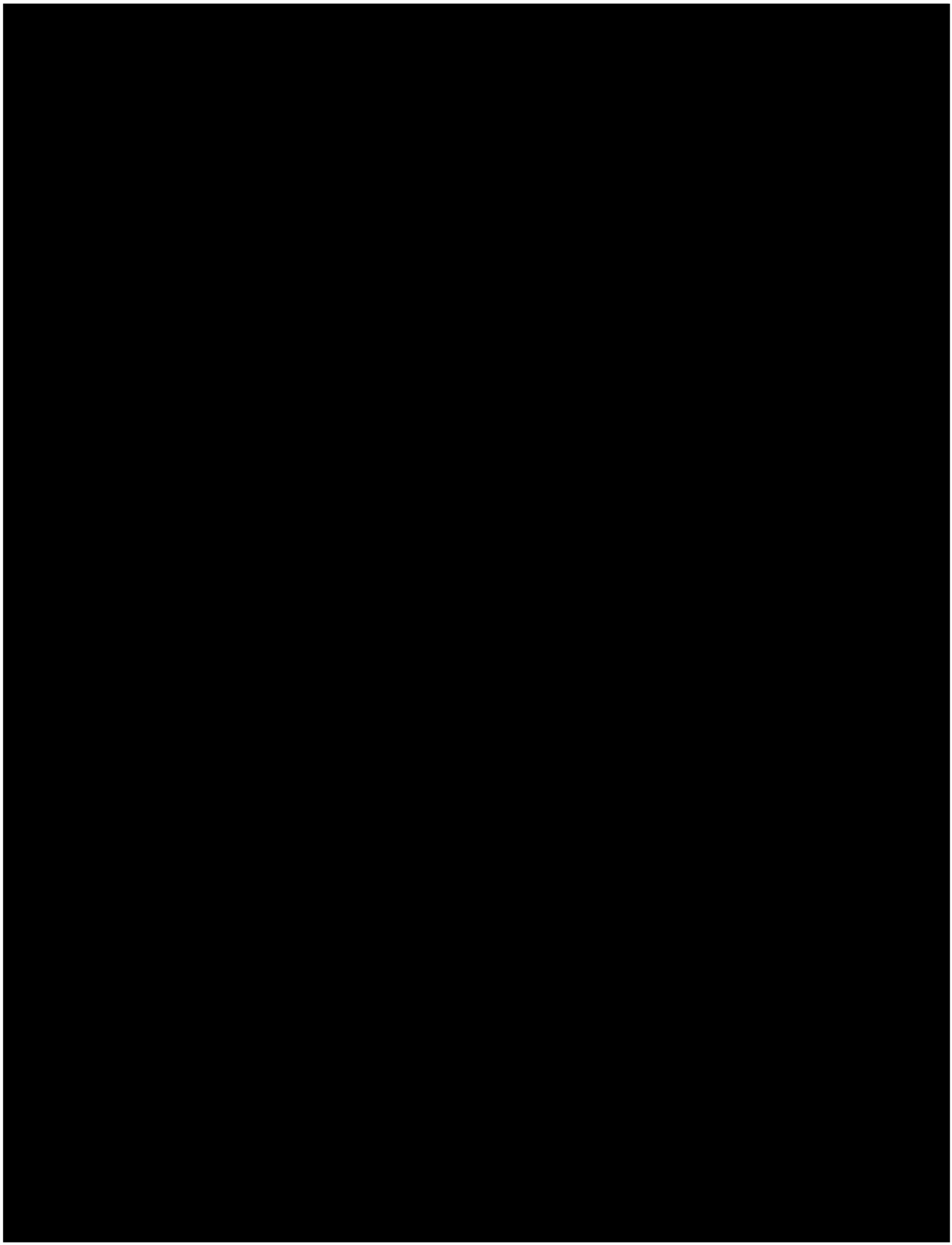
12.6 Miscellaneous. The section headings contained in this DPE are for reference purposes only and shall not in any way affect the meaning or interpretation of this DPE.

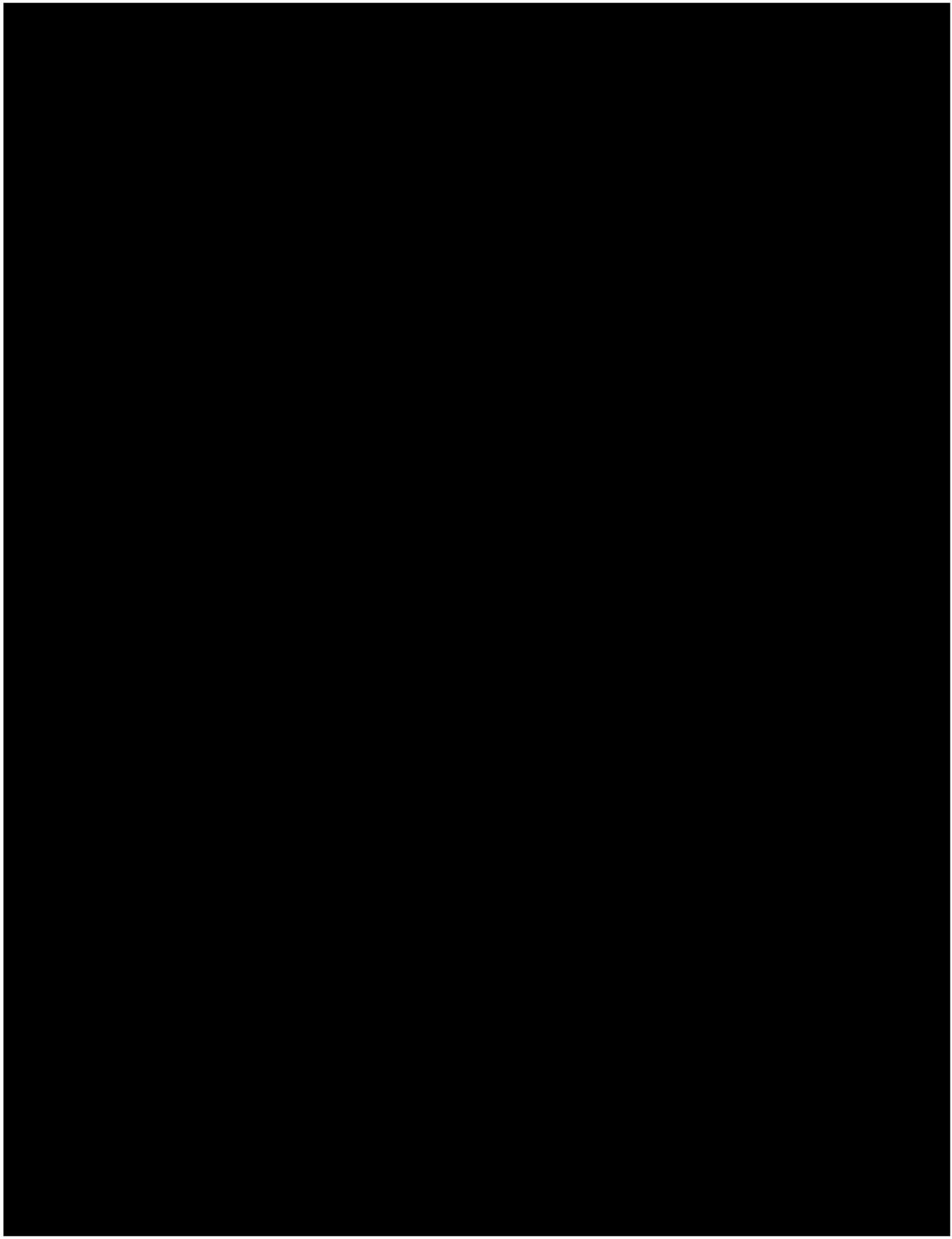












workday.

00250058.0 - **Confidential**

UNIVERSAL SECURITY EXHIBIT

This Workday Universal 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 Universal 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 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**. Technical or procedural mechanisms put in place to promote efficient and effective operations, as well as compliance with policies.

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.

UNIVERSAL SECURITY EXHIBIT

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; and

    b) Defining security roles and responsibilities for individuals with security responsibilities.

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.

workday.

Confidential

Workday Production Support and Service Level Availability Policy (SLA)

Workday's Service is based on a multi-tenanted operating model that applies common, consistent management practices for all customers using the service. This common operating model allows Workday to provide the high level of service reflected in our business agreements. This document (the "SLA") communicates Workday's Production Support and Service Level Availability Policy for its customers. Capitalized terms, unless otherwise defined herein, shall have the same meaning as in the primary Service subscription agreement between Workday and Customer ("MSA").

1. Support Terms:

Workday will provide Customer with support 24x7x365 (24 hours a day, 7 days a week, 365 days a year) in accordance with this SLA.

2. Service Availability:

Workday's Service Availability commitment for a given calendar month is 99.7%.
Service Availability is calculated per month as follows:

$$\left(\frac{\text{Total} - \text{Unplanned Outage} - \text{Planned Maintenance}}{\text{Total} - \text{Planned Maintenance}}\right) \quad X\ 100\% \geq 99.7\%$$

Definitions:

- **Total** is the total minutes in the month
- **Unplanned Outage** is total minutes that the Service is not available in the month outside of the Planned Maintenance window
- **Planned Maintenance** is total minutes of planned maintenance in the month.

Currently, Planned Maintenance is four (4) hours for weekly maintenance, plus four (4) hours for monthly maintenance, plus four (4) hours for quarterly maintenance. The Planned Maintenance windows can be found at Workday Scheduled Maintenance (https://community.workday.com/articles/521701). All times are subject to change upon 30 days' notice provided at https://community.workday.com ("Workday Community") and any such change shall not lengthen the duration of the associated maintenance window.
If actual maintenance exceeds the time allotted for Planned Maintenance, it is considered an Unplanned Outage. If actual maintenance is less than time allotted for Planned Maintenance, that time is not applied as a credit to offset any Unplanned Outage time for the month.

The measurement point for Service Availability is the availability of the Production Tenants at the Workday Production data center's Internet connection points. Upon Customer request not more than once per month via the Workday case management system ("Customer Center"), Workday will provide a Service Availability report.

3. Workday Feature Release and Service Update Process:

Periodically, Workday introduces new features in the Service with enhanced functionality across Workday applications. Features and functionality will be made available as part of a major feature release ("Feature Release") or as part of weekly service updates ("Service Updates"). Feature Releases will take place approximately twice per year. The frequency of Feature Release availability may be increased or decreased by Workday at Workday's discretion with at least 30 days' prior notice to Customer on Workday Community. Specific information and timelines for Feature Releases and Service Updates can be found on Workday Community. Feature Releases will be performed during a weekend within any Planned Maintenance.

4. Service Response:

Workday's Service Response commitment is: (1) not less than 50% of online transactions in one second or less and (2) not more than 10% in 2.5 seconds or more. "Service Response" means the processing time of the

Workday Production Support and Service Level Availability Policy (SLA)

Workday Production Tenants in the Workday Production data center to complete transactions submitted from a web browser. This Service Response commitment excludes online requests processed via background jobs, Workday Web Services, or as analytics.

The time required to complete the request is measured from the point in time when the request has been fully received by the encryption endpoint in the Workday Production data center, until the response begins to be returned for transmission to Customer. Customer may request a Service Response report not more than once per month via the Customer Center.

Customers may impact their own Service Response time by launching custom reports and integrations in excess of the limits set forth in Workday Community. Workday may enforce reasonable and documented system limits to serve as guardrails for the Service where these reports and integrations negatively impact Service Response.

5. Production Data Center Disaster Recovery:

Workday will maintain a disaster recovery plan for the Workday Production Tenants in conformance with Workday's most current Disaster Recovery Summary, the current version of which can be viewed on the Workday Community. Workday commits to a recovery time objective of 12 hours - measured from the time that the Workday Production Tenant becomes unavailable until it is available again. Workday commits to a recovery point objective of 1hour - measured from the time that the first transaction is lost until the Workday Production Tenant becomes unavailable.

Workday will test the disaster recovery plan once every six months and will make available a written summary of the results of the most recent test available to Customers in Workday Community.

6. Case Submittal and Reporting:

Customer's Named Support Contacts may submit cases to Workday Support via the Customer Center. Named Support Contacts must be trained on the Workday products for which they initiate support requests. Each case will be assigned a unique case number. Workday will respond to each case in accordance with this SLA and will work diligently toward resolution of the issue taking into consideration its severity and impact on the Customer's business operations. Actual resolution time will depend on the nature of the case and the resolution itself. A resolution may consist of a fix, workaround, delivery of information or other reasonable solution to the issue. Case reporting is available on demand via the Customer Center.

7. Severity Level Determination:

Customer shall reasonably self-diagnose each support issue and shall recommend to Workday an appropriate Severity Level designation. Workday shall validate Customer's Severity Level designation or notify Customer of a proposed change in the Severity Level designation to a higher or lower level with justification for the proposal. In the event of a conflict regarding the appropriate Severity Level designation, each party shall promptly escalate such conflict to its management team for resolution through consultation between the parties' management. In the rare case a conflict requires a management discussion, both parties shall make a representative available within one hour of the escalation.

8. Support Issue Production Severity Levels - Response and Escalation:

"Workday Response Commitment" means the period of time from when Customer logs the Production case in the Customer Center until Workday responds to Customer or escalates within Workday, if appropriate. Because of the widely varying nature of issues, it is not possible to provide specific resolution commitments.

If Customer is not satisfied with the progress of a Severity Level 1 or 2 issue, Customer may escalate the case to Workday support management using the escalation process defined for Named Support Contacts. Upon

escalation, Workday shall notify support senior management and shall assign a Workday escalation manager to work with Customer until the escalation is resolved.

Severity Level 1:

- Definition: The Service is unavailable or a Service issue prevents timely payroll processing, tax payments, entry into time tracking, financials closing (month-end, quarter-end or year-end), payment of supply chain invoices or creation of purchase orders, processing of candidate applications, issues that prevent financial aid disbursements, admissions, and registration activity of students. No workaround exists.
- Workday Response Commitment: Workday will respond within 30 minutes after receiving the case and will remain accessible for troubleshooting from the time a Severity 1 issue is logged until it is resolved.
- Resolution: Workday will work to resolve the problem until the Service is returned to normal operation and will notify Customer of status changes.
- Escalation: If the problem has not been resolved within one hour, Workday will escalate the problem to the appropriate Workday organization. The escalated problem will have higher priority than ongoing support, development or operations initiatives.
- Customer Response Commitment: Customer shall remain accessible for troubleshooting from the time a Severity 1 issue is logged until it is resolved.

Severity Level 2:

- Definition: An issue with the Service that prevents Customer from completing one or more critical business processes with a significant impact. No workaround exists.
- Workday Response Commitment: Workday will respond within one hour after receiving the case and shall remain accessible for troubleshooting from the time a Severity 2 issue is logged until it is resolved.
- Resolution: Workday will work to resolve the problem until the Service is returned to normal operation and will notify Customer of status changes.
- Escalation: If the problem has not been resolved within four hours, Customer may request that Workday escalate the problem to the appropriate Workday organization where the escalated problem will have higher priority than ongoing development or operations initiatives.
- Customer Response Commitment: Customer shall remain accessible for troubleshooting from the time a Severity 2 issue is logged until it is resolved.

Severity Level 3:

- Definition: An issue with the Service that prevents Customer from completing one or more important business processes that impact Customer's business operations. A workaround exists but is not optimal.
- Workday Response Commitment: Workday will respond within four hours after receiving the case.
- Resolution: If resolution requires a Workday issue fix, Workday will add the issue fix to its development queue for future Service Updates and will suggest a potential workaround until the problem is resolved in a future Service Update. Workday will notify Customer of status changes.
- Escalation: If progress is not being made to Customer's satisfaction, Customer may request that Workday escalate the problem to the appropriate Workday organization
- Customer Response Commitment: Customer will respond to Workday requests for additional information and will implement recommended solutions in a timely manner.

Severity Level 4:

- Definition: An issue with the Service that delays Customer from completing one or more non-critical business processes that are not imperative to Customer's business operations. A workaround exists.
- Workday Response Commitment: Workday will respond within 24 hours after receiving the case.
- Resolution: If resolution requires a Workday issue fix, Workday will add the issue fix to its development

queue for future Service Updates and will suggest potential workarounds until the problem is resolved in a future Service Update. Customer will be notified of status changes.

- Escalation: If progress is not being made to Customer's satisfaction, Customer may request that Workday escalate the problem to the appropriate Workday organization.
- Customer Response Commitment: Customer will respond to Workday's requests for additional information and will implement recommended solutions in a timely manner.

Severity Level 5 (Including Customer Care and Operations Requests):

- Definition: Non-system issues and requests such as Named Support Contact changes, SLA report, or general Service inquiries. Questions about product configuration and functionality should be addressed to the Workday Community.
- Workday Response Commitment: Workday will respond within 24 hours after receiving the case.
- Resolution Commitment: Workday will respond to the request and will notify Customer of status changes.
- Escalation: If progress is not being made to Customer's satisfaction, Customer may request that Workday escalate the problem to the appropriate Workday organization.
- Customer Commitment: Customer will respond to Workday requests for additional information in a timely manner.

9. Workday Support Scope:

Workday will support functionality that is delivered by Workday as part of the Service. For all other functionality, and for issues or errors in the Service caused by issues, errors, or changes in Customer's information systems, customizations, and third-party products or services, Workday may assist Customer and its third-party providers in diagnosing and resolving issues or errors but Customer acknowledges that these matters are outside of Workday's support obligations. Failure to meet obligations or commitments under this SLA that are attributable to (1) Customer's acts or omissions; and (2) force majeure events shall be excused.

10. Workday Web Services API Support:

Workday recommends using the most recent version of the Workday Web Services ("WWS") APIs in order to receive optimum performance and stability. Prior versions of WWS APIs are updated to support backward-compatibility for all prior versions of WWS APIs that have not reached an end-of-life status. Workday will make end-of-life announcements no less than 18 months before the end-of-life of each WWS API. Workday will make announcements surrounding the WWS APIs through Workday Community or, for Workday Extend APIs, through the Workday Extend developer site.

Backward compatibility means that an integration created to work with a given WWS API version will continue to work with that same WWS API version even as Workday introduces new WWS API versions. With the exception of backward-compatibility updates, prior versions of WWS APIs are not enhanced.

11. Workday Cloud Platform Support:

For customers subscribing to Workday Extend ("Extend") under an Order Form, Workday will support Extend in Production Tenants. All Extend Applications, whether created by a customer, Workday or others, are expressly not covered by this SLA. Workday will not be responsible for any Service Availability downtime or delayed Service Response times caused by use of any Extend Applications. Workday may modify or deprecate Extend APIs, features and services in accordance with the Extend Availability Statuses posted on the Workday Extend developer site at developer.workday.com. Use of the developer site and all materials therein is governed by the Extend Developer Program Agreement. "Extend Applications" means the customizations, add-ons, extensions and/or other software solutions developed by or for a customer using Extend developer materials.

2020004-RFP Schedule 8

Respondent Instructions

1. Failure to follow these instructions and other instructions/requirements described in Part 3, Section 3.4 of the RFP Particulars (Appendix B) may result in disqualification of the proposal
2. Provide the Cost and Financial Proposal in this Excel Form. All costs are in Canadian Dollar. Pricing includes all applicable duties and taxes except HST.
3. Upon request, at any time prior to the award of a contract, Respondent must provide the University with any additional information and documentation to support the cost or pricing information in this Form
4. Year 1 starts upon contract award for Phase 1 Clarification Contract, which is expected to be May 1, 2021. uOttawa fiscal year is from May 1 to April 30.
5. Each of Tabs A, B, C, D and E must be completed. Tab A is a summary of Tabs B to E. The Tab A must not be modified.
6. Tab B - provide costs and pricing by category by completing the cells in white for the Deliverables associated with Phase I - Clarification
7. Tab C - provide implementation and integration costs pricing by category completing the cells in white
8. Tab D - Provide pricing for each module of the Pre-qualified ERP Software needed for the Deliverables and to meet requirements set out in RFSQ# 2020003-RFSQ. Costs are to be provided for the next ten (10) years and include the functions/modules listed in the Software Costs tab and based on the applicable metrics provided in the RFSQ# 2020003-RFSQ. The total price must include the cost of maintenance and support and any costs associated with new components/technology that are imposed by the proposed software application and not included in the University of Ottawa's current technical architecture. The total price must include the cost of licenses required for development, testing and training environments. The total software cost cannot be higher than the cost proposal received in the RFSQ submitted by the Pre-qualified ERP Software provider in response to RFSQ # 2020003-RFSQ-ERP

9. Tab E - provide the hourly rate based on the different type of resource category. Rates would be for authorized changed orders during implementation.
10. Describe the pricing methodology used to calculate the proposed pricing.