TermTrax

Software Review Report

Slack

Generated: 2026-08-06T08:37:42.144Z
Schema Version: 1.2.0

Table of Contents

Review Summary

Review ID: woe43khscpmy7rit61uxst4k
Status: ANALYSIS
Decision: Pending
Created At: 2026-07-14T09:11:50.684Z
Submitted At: Not submitted
Submitted By: N/A
Analysis Completed At: 2026-08-06T08:26:49.641Z
General Notes: None
Usage Conditions: None
AI Jurisdiction: Contingent on Customer domicile — three possible governing laws apply: (1) California + controlling U.S. federal law [US/Canada domicile]; (2) England [Rest of World, except Japan]; (3) Japan [Japan domicile]. Most probable governing law for a standard US-domiciled team chat deployment: California.
Human Jurisdiction: N/A

Intake Form

Purpose: App for team to chat
Risk Concerns: None
Review Priorities: None

Playbook Items

Name	Category	Weight	AI Color	Human Color
Termination for Convenience	Termination	ACCEPTABLE_TO_DEVIATE	Needs Review	Unaddressed
Authorized Equipment & Software	Access & Personnel	HIGH	Needs Review	Unaddressed
Data Ownership	Data Handling	CRITICAL	Needs Review	Unaddressed
Data Backup & Restoration	Business Continuity	HIGH	Aligned	Unaddressed
Data Segregation	Data Handling	HIGH	Aligned	Unaddressed
Arbitration or other dispute resolution process	Legal & Compliance	MEDIUM	Needs Review	Unaddressed
Breach Indemnification	Governance & Risk Transfer	HIGH	Needs Review	Unaddressed
Subprocessor Agreements	Subprocessors	CRITICAL	Needs Review	Unaddressed

Name	Category	Weight	AI Color	Human Color
Modification of Terms	Legal & Compliance	HIGH	Needs Review	Unaddressed
Processing Location Restrictions	Data Handling	HIGH	Needs Review	Unaddressed
Audit Logging	Security Operations	HIGH	Needs Review	Unaddressed
Data Processing Security Policies	Security Operations	HIGH	Aligned	Unaddressed
Security Certifications	Governance & Risk Transfer	HIGH	Aligned	Unaddressed
Anti-Virus Solution	Security Operations	HIGH	Needs Review	Unaddressed
Password Encryption	Encryption	HIGH	Needs Review	Unaddressed
Termination for Cause	Termination	ACCEPTABLE_TO_DEVIATE	Aligned	Unaddressed
Breach Notification Timeline	Breach & Incident Response	CRITICAL	Needs Review	Unaddressed
Termination Obligations	Termination	MEDIUM	Aligned	Unaddressed
Compliance Monitoring	Governance & Risk Transfer	HIGH	Needs Review	Unaddressed
Publicity	Publicity	HIGH	At Risk	Unaddressed
Cybersecurity Prevention Systems	Security Operations	HIGH	Aligned	Unaddressed
Regulatory Disclosure Procedure	Breach & Incident Response	HIGH	Needs Review	Unaddressed
Security Training	Access & Personnel	MEDIUM	Needs Review	Unaddressed
Disaster Recovery Testing	Business Continuity	HIGH	Needs Review	Unaddressed
Data Subject Rights Assistance	Governance & Risk Transfer	HIGH	Aligned	Unaddressed
Our liability	Limitation of Liability	ACCEPTABLE_TO_DEVIATE	Aligned	Unaddressed
Data Retention & Deletion	Data Handling	HIGH	Aligned	Unaddressed
Vendor Audit Rights	Governance & Risk Transfer	HIGH	Needs Review	Unaddressed
User Authentication Policies	Security Operations	HIGH	Needs Review	Unaddressed
Employee Confidentiality Agreements	Access & Personnel	HIGH	Aligned	Unaddressed
Employee Access Control	Access & Personnel	HIGH	Aligned	Unaddressed
Employee Offboarding Access	Access & Personnel	HIGH	Needs Review	Unaddressed
Confidentiality	Confidentiality	HIGH	Aligned	Unaddressed
Physical Security Controls	Security Operations	HIGH	Aligned	Unaddressed
Compliance with Referenced Laws	Legal & Compliance	HIGH	Needs Review	Unaddressed
Vendor's liability	Limitation of Liability	HIGH	Needs Review	Unaddressed
License Grant to Data – Our Company to Vendor	License Grant	CRITICAL	Needs Review	Unaddressed
Retention of our Rights to our Property	Intellectual Property	CRITICAL	Aligned	Unaddressed
No AI/ML Training on Our Data	Data Handling	CRITICAL	At Risk	Unaddressed
Processing Limitation	Data Handling	CRITICAL	Needs Review	Unaddressed
Insurance	Commercial Terms	ACCEPTABLE_TO_DEVIATE	Needs Review	Unaddressed
Ownership of Custom Deliverables	Intellectual Property	HIGH	At Risk	Unaddressed
Governing Law	Legal & Compliance	ACCEPTABLE_TO_DEVIATE	Aligned	Unaddressed

Name	Category	Weight	AI Color	Human Color
Encryption at Rest	Encryption	HIGH	Needs Review	Unaddressed
Subprocessor Change Notification	Subprocessors	HIGH	Aligned	Unaddressed
Assignment	Legal & Compliance	ACCEPTABLE_TO_DEVIATE	Aligned	Unaddressed
Cyber Risk Insurance	Governance & Risk Transfer	MEDIUM	Needs Review	Unaddressed
Warranty & Remedy	Commercial Terms	ACCEPTABLE_TO_DEVIATE	Aligned	Unaddressed
Automatic Renewal	Commercial Terms	ACCEPTABLE_TO_DEVIATE	Aligned	Unaddressed
Restrictions on Use	Operations	HIGH	Aligned	Unaddressed
Indemnification – Vendor to Our Company	Indemnification	MEDIUM	Needs Review	Unaddressed
License Grant – Vendor to Our Company	License Grant	HIGH	Needs Review	Unaddressed
Exclusivity	Operations	HIGH	Aligned	Unaddressed
Non-Solicitation of Employees	Operations	MEDIUM	Aligned	Unaddressed
Subprocessor Audit Rights	Subprocessors	MEDIUM	Needs Review	Unaddressed
Encryption in Transit	Encryption	HIGH	Needs Review	Unaddressed
Indemnification – Our Company to Vendor	Indemnification	MEDIUM	Needs Review	Unaddressed
Payment Terms	Commercial Terms	HIGH	Aligned	Unaddressed
Data Protection Officer (DPO)	Governance & Risk Transfer	MEDIUM	Aligned	Unaddressed

Termination for Convenience

AI Comment: Slack's contractual framework (Salesforce MSA + Slack Supplemental Terms) does not provide Customer with a general right to terminate for convenience during a subscription term. MSA §11.3 restricts termination for both parties to for-cause scenarios only — uncured material breach after 30 days' notice, or insolvency events. This directly fails the playbook's first requirement that "We can terminate for convenience."

Second, MSA §5.1 explicitly declares payment obligations non-cancelable and fees paid non-refundable. This provision directly contradicts the playbook's requirement that Customer receive a pro-rata refund of remaining unused fees upon a convenience termination. A partial carve-out to this non-refundable rule exists in §11.4 (refund upon Customer's for-cause termination), but this applies only when Customer exercises the §11.3 cause-termination right — a scenario wholly distinct from the convenience termination the playbook requires.

The one element of the playbook position that is met is the vendor's inability to terminate paid subscriptions for convenience — MSA §11.3 equally limits SFDC's termination rights for paid services to for-cause scenarios. This is consistent with the playbook requirement. However, MSA §2.7 grants SFDC an unrestricted termination for convenience right over the free services tier (for any or no reason, without prior notice), which partially conflicts with the vendor-cannot-terminate-for-convenience requirement.

Customer does possess a term-end exit mechanism under §11.2 (non-renewal with 30 days' notice), and a narrow change-of-control triggered termination with refund under §12.8. Neither constitutes a mid-term termination for convenience right, and neither triggers a pro-rata refund in the way the playbook describes.

Given the playbook weight of Acceptable to Deviate, these gaps are informational rather than blocking. The absence of a Customer termination for convenience right is standard market practice in enterprise SaaS subscriptions; annual/multi-year subscription commitments with non-cancelable fees are the commercial norm. The most significant conflict with the playbook position is the explicit non-cancelability and non-refundability of fees under §5.1, which would preclude a pro-rata refund even if a convenience termination right were negotiated into an Order Form without a corresponding §5.1 carve-out.

— Superseding reasoning —
Within the MSA, §11.4 (refund upon Customer's for-cause termination) creates a specific exception to §5.1's general rule that fees paid are non-refundable. Under the specific-over-general drafting canon, §11.4 controls the refund question when Customer exercises for-cause termination rights under §11.3. §5.1's general non-refundable rule remains fully operative in all other scenarios — including, critically, any hypothetical convenience termination (which does not exist under the contract). This superseding determination does not assist with the playbook's convenience termination analysis; it only clarifies which provision governs within the for-cause termination context.

— Note —
The AI cited 5 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "A party may terminate this Agreement for cause (i) upon 30 days written notice to the other party of a material breach if such breach remains uncured at the expiration of such period, or (ii) if the o…"
2. "Except as otherwise specified herein or in an Order Form, (i) fees are based on Services subscriptions purchased and not actual usage, (ii) payment obligations are non-cancelable and fees paid are non…"
3. "Customer agrees that SFDC, in its sole discretion and for any or no reason, may terminate Customer's access to the Free Services or any part thereof. Customer agrees that any termination of Customer's…"
4. "If this Agreement is terminated by Customer in accordance with the 'Termination' section above, SFDC will refund Customer any prepaid fees covering the remainder of the term of all Order Forms after t…"
5. "Except as otherwise specified in an Order Form, subscriptions will automatically renew for additional one year terms, unless either party gives the other written notice (email acceptable) at least 30 …"

> *"Notwithstanding the foregoing, if a party is acquired by, sells substantially all of its assets to, or undergoes a change of control in favor of, a direct competitor of the other party, then such other party may terminate this Agreement upon written notice. In the event of such a termination, SFDC will refund Customer any prepaid fees covering the remainder of the term of all subscriptions for the period after the effective date of such termination."*
> — https://www.salesforce.com/en-us/wp-content/uploads/sites/4/documents/legal/salesforce_MSA.pdf

Authorized Equipment & Software

AI Comment: The playbook item requires (1) that vendor employees process Customer Data only on authorized business equipment, and (2) that the vendor prevents use or installation of unauthorized hardware and software on systems processing Customer Data. These controls address the risk of data exfiltration or compromise via unmanaged endpoints and rogue software — a material concern for a SaaS team-chat platform handling potentially sensitive internal communications.

Across the full document set, no provision explicitly addresses either requirement. The analysis reveals layered but incomplete coverage.

WHAT IS COVERED: MSA §2.2 commits SFDC to "appropriate administrative, physical, and technical safeguards" including measures against unauthorized access — general language theoretically encompassing endpoint controls, but not specific to authorized-equipment-only processing or unauthorized software prohibition. This provision is superseded on the subject of technical/organizational measures for Personal Data processing by DPA §6.1 (see Superseding). DPA §4.1 addresses personnel security controls: confidentiality training, reliability assurance, and limitation of access to authorized personnel only. This governs who may access Customer Data, but is silent on what equipment or software those personnel use to do so. DPA §6.1 is the governing provision for technical and organizational security measures for Personal Data processing, incorporating by reference the Security, Privacy and Architecture Documentation (SPARC) as the authoritative source for the applicable controls. The standard used is "appropriate measures" — not benchmarked to the specific controls the playbook item requires. The SPARC (Document 9) provides the most granular contractual detail: (a) alignment with ISO 27001, ISO 27002, and ISO 27018 (which encompass endpoint device and software installation controls); (b) automated vulnerability scanning of production hosts; and (c) strict employee access controls with audit logging.

WHAT IS ABSENT: No explicit contractual commitment that employees process Customer Data only on authorized business equipment (no MDM requirement, device enrollment policy, BYOD restriction, or equivalent is stated). No explicit prohibition on unauthorized hardware or software installation on systems processing Customer Data. Slack's internal endpoint security program — if any MDM, device allowlisting, or software control program exists — is not disclosed in the available contractual documents. The Acceptable Use Policy (Document 3) references a Salesforce AUP PDF not included in the current document set; AUPs typically govern customer/user behavior rather than vendor-internal security controls, making it an unlikely source for these commitments, but this cannot be confirmed without the full text.

ISO 27001 INFERENCE: The SPARC's commitment to align with ISO 27001/27002/27018 provides the strongest indirect assurance. ISO 27001:2022 Annex A controls A.8.1 (User endpoint devices) and A.8.19 (Installation of software on operational systems) directly address the playbook requirements. However, the specific controls are not contractually enumerated, "align with" is a weaker standard than "certified to," and the certification scope for Slack's specific services is not confirmed in the documents.

CLASSIFICATION RATIONALE: Under the acceptable position for this High-weight item, YELLOW is appropriate. General safeguards language and ISO 27001 alignment provide some indirect assurance that endpoint and software controls exist, meaning the contract is not silent. However, the explicit, specific commitments the playbook item requires — authorized-equipment-only processing and prevention of unauthorized hardware/software on data-processing systems — are absent from the contractual text. The protection provided is weaker and less specific than the playbook requires.

— Superseding reasoning —
DPA §6.1 (PIF index 2) supersedes MSA §2.2 (PIF index 0) on the subject of technical and organizational security measures applicable to Customer Data / Personal Data processing. The DPA is the specific data processing instrument incorporated by reference into the MSA (MSA §2.2 expressly states "The terms of the data processing addendum… are hereby incorporated by reference"), and DPA §6.1 addresses the same subject matter — security safeguards protecting Customer Data — with greater specificity: it is scoped to Personal Data processing, expressly names the Security, Privacy and Architecture Documentation as the authoritative source for the applicable controls, and includes a non-degradation obligation. Under the general-over-specific principle, the more specific DPA provision governs on this topic for Personal Data processing contexts.

— Note —
The AI cited 2 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "SFDC shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibiliti…"
2. "SFDC shall maintain appropriate technical and organizational measures for protection of the security (including protection against unauthorized or unlawful Processing and against accidental or unlawfu…"

> *"SFDC will maintain appropriate administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Customer Data, as described in the Documentation. Those safeguards will include, but will not be limited to, measures designed to prevent unauthorized access to or disclosure of Customer Data (other than by Customer or Users)."*
> — https://www.salesforce.com/en-us/wp-content/uploads/sites/4/documents/legal/salesforce_MSA.pdf
> *"At a minimum, Salesforce will align with prevailing*
> *industry standards such as ISO 27001, ISO 27002, and ISO 27018."*
> — Security, Privacy and Architecture Report
> *"Security Controls"*
> — Security, Privacy and Architecture Report
> *"We place strict controls over employee access to Customer Data. There are technical controls and audit policies in place to ensure that access to Customer Data is logged."*
> — Security, Privacy and Architecture Report

Data Ownership

AI Comment: The playbook item requires that "as between the parties, all Personal Data remains sole property of our company." Analysis of this Critical-weight item across the full Slack/Salesforce contract stack produces a YELLOW classification: the core ownership language is explicit and strong across multiple documents, but the Slack Supplemental Terms AI/ML provisions introduce a meaningful limitation on the "sole" property standard in the contract's default state.

Core Ownership Confirmed (GREEN elements): Multiple documents establish Customer ownership of Customer Data, which encompasses Personal Data submitted to the Services. The User Terms state Customer Data is "owned by Customer." The MSA § 6.2 contains the most direct ownership disclaimer: "SFDC acquires no right, title or interest from Customer or its licensors under this Agreement in or to any Customer Data." The DPA § 2.2 confirms SFDC processes Personal Data as Confidential Information only under Customer's documented instructions, and the Privacy Policy confirms "Slack is a processor of Customer Data and the Customer is the controller." These provisions are mutually consistent and satisfy the ownership element of the playbook requirement.

The license SFDC holds over Customer Data (MSA § 6.2) is a "worldwide, limited-term license to host, copy, use, transmit, and display" Customer Data "as appropriate for SFDC to provide and ensure proper operation of the Services" — a service delivery license expressly disclaimed as not an ownership transfer in the same section.

'Sole Property' Limitation (YELLOW elements): The Slack Supplemental Terms' "Slack Search, Learning and Artificial Intelligence" section creates a material gap from the "sole property" standard. By default — without requiring any Customer action — the contract authorizes SFDC to use Customer Data (including Personal Data) "to train models for use by the services and features that Customer has access to" and for product R&D across SFDC's customer base. Critically, the same section bifurcates ownership: while "Customer retains all ownership of its Customer Data," "SFDC retains all ownership in and to aggregated machine learning results." This creates a regime in which Personal Data is used as training input for Slack's ML models, and Slack owns the resulting commercial products derived from that data.

An opt-out from global ML model training is available per the Privacy Principles page (referenced by the Supplemental Terms), but it requires the Primary Owner to proactively contact Slack's Customer Experience team. The default contractual position is model training — the opt-out is not automatic.

Additionally, the Privacy Policy separately identifies Slack as the *controller* of "Other Information" — including usage metadata, log data, and device information that may constitute personal data relating to identified users — meaning this category of personal data is not within Customer's "sole property" rights at all. This is a secondary concern but reinforces the overall YELLOW posture.

Classification Rationale: For a Critical-weight data ownership playbook item requiring "sole property" status, the combination of (a) a default contractual authorization for ML training on Personal Data, (b) SFDC's ownership of aggregated ML results derived from that Personal Data, and (c) Slack's controller status over usage-related personal data, represents a material gap from the "sole property" standard in the contract's default state — even though the underlying Customer Data ownership is clearly and repeatedly confirmed. YELLOW reflects that the contract partially addresses the requirement with weaker protections than "sole property" demands. Remediating to GREEN would require, at minimum, negotiating removal of the ML training authorization or converting it to opt-in consent, and removing the aggregated ML results ownership carve-out from the Supplemental Terms.

— Note —
The AI cited 2 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "Customer grants SFDC, its Affiliates and applicable contractors a worldwide, limited-term license to host, copy, use, transmit, and display any Non-SFDC Applications and program code created by or for…"
2. "SFDC shall treat Personal Data as Confidential Information and shall Process Personal Data on behalf of and only in

accordance with Customer's documented instructions for the following purposes: (i) P…"

> *"you acknowledge and agree that the Customer Data is owned by Customer and the Contract provides Customer with many choices and control over that Customer Data."*
> — User Terms of Service | Legal | Slack
> *"Subject to the limited licenses granted herein, SFDC acquires no right, title or interest from Customer or its licensors under this Agreement in or to any Customer Data, Non-SFDC Application or such program code."*
> — https://www.salesforce.com/en-us/wp-content/uploads/sites/4/documents/legal/salesforce_MSA.pdf
> *"SFDC may access Customer Data in Slack for the following reasons, and Customer instructs SFDC to process its Customer Data for such purposes:*
>
> *1. to train models for use by the services and features that Customer has access to;*
> *2. to improve services and features that Customer has access to;*
> *3. to conduct research and development of products that Customer will have access to without additional cost;*
> *4. as otherwise provided in the MSA between SFDC and Customer."*
> — Slack Supplemental Terms | Legal | Slack
> *"Customer retains all ownership of its Customer Data and SFDC retains all ownership in and to aggregated machine learning results."*
> — Slack Supplemental Terms | Legal | Slack
> *"Slack is a processor of Customer Data and the Customer is the controller."*
> — Privacy Policy | Legal | Slack
> *"If you want to exclude your Customer Data from helping train Slack global models, you can opt out. If you opt out, Customer Data on your workspace will only be used to improve the experience on your own workspace and you will still enjoy all of the benefits of our globally trained ML models without contributing to the underlying models."*
> — Slack Privacy Principles
> *"Customer Data and Other Information"*
> — Slack Privacy Principles

Data Backup & Restoration

AI Comment: The playbook item requires two distinct obligations: (1) vendor creates backups of data, and (2) vendor regularly conducts restoration tests of those backups at minimum annually. Both elements are directly and explicitly addressed in the Security, Privacy and Architecture Report (SPARC), which constitutes "Documentation" incorporated by reference into the Main Services Agreement (MSA § 2.2) and the Data Processing Addendum (DPA § 6.1).

Backup creation: The SPARC states unambiguously that "Customer Data and our source code are automatically backed up every night." This establishes a daily automated backup cadence, clearly meeting the backup creation requirement. The SPARC further notes that Customer Data is stored redundantly in multiple locations and that Salesforce performs regular backups with rollbacks and replication as needed, providing additional layers of data protection.

Restoration testing: Most critically for the playbook item's "at minimum annually" testing requirement, the SPARC commits that "Backups are fully tested at least every 90 days to confirm that our processes and tools work as expected." Quarterly testing (4× per year) materially exceeds the minimum annual testing cadence. The SPARC reinforces this by confirming "well-tested backup and restoration procedures which allow recovery from a major disaster" and that the operations team tests disaster recovery measures regularly with a 24-hour on-call team.

Contractual force: Both the MSA (§ 2.2) and the DPA (§ 6.1) create general security safeguard obligations that expressly defer to the SPARC for specifics ("as described in the Documentation" and "as set forth in the Security, Privacy and Architecture Documentation," respectively). The SPARC's specific backup and restoration testing commitments therefore carry contractual weight through incorporation by reference. Under SPECIFIC_OVER_GENERAL superseding logic, the SPARC's express commitments govern over the general safeguard language in the MSA and DPA.

Note on documentation currency: The SPARC states it may be updated from time to time; reviewers should verify the current published version of the SPARC at contract execution. No material limitation is observed in the current version.

aiPreferenceMet is false because no ideal preference was specified in the playbook item — GREEN reflects that the acceptable threshold (backups created + at minimum annual restoration testing) is met and exceeded, but preference met requires an explicitly stated ideal.

— Superseding reasoning —
The SPARC (Security, Privacy and Architecture Documentation) contains the specific backup creation and restoration testing commitments, and is the operative control document for this playbook item. The MSA § 2.2 creates a general obligation to maintain safeguards "as described in the Documentation," explicitly deferring to the SPARC for the specifics of what those safeguards entail. DPA § 6.1 similarly requires technical and organizational measures "as set forth in the Security, Privacy and Architecture Documentation." Under the SPECIFIC_OVER_GENERAL principle, the SPARC's express commitments — daily automated backups and at-least-quarterly restoration testing — supersede and govern over the general safeguard language in the MSA and DPA. There is no conflict between the documents; the MSA and DPA establish the obligation while the SPARC defines its content.

— Note —
The AI cited 1 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "SFDC shall maintain appropriate technical and organizational measures for protection of the security (including protection against unauthorized or unlawful Processing and against accidental or unlawfu…"

> *"Customer Data and our source code are automatically backed up every night."*
> — Security, Privacy and Architecture Report
> *"Backups are fully tested at least every 90 days to confirm that our processes and tools work as expected."*
> — Security, Privacy and Architecture Report
> *"We have well-tested backup and restoration procedures which allow recovery from a major disaster."*
> — Security, Privacy and Architecture Report
> *"SFDC will maintain appropriate administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Customer Data, as described in the Documentation."*
> — https://www.salesforce.com/en-us/wp-content/uploads/sites/4/documents/legal/salesforce_MSA.pdf

Data Segregation

AI Comment: The playbook item requires physical and/or logical separation of Customer Data received from different controllers. The document set addresses this requirement, with the most specific and direct confirmation appearing in the Slack Security, Privacy and Architecture Report (SPARC). The SPARC — incorporated by reference as "Documentation" under the MSA — explicitly states that the Covered Services operate on "a multitenant architecture at both the platform and infrastructure layers that is designed to segregate and restrict Customer Data access based on business needs" and that "the architecture provides a logical data separation for each different customer via a unique ID." This directly and unambiguously satisfies the logical separation prong of the acceptable position. The contractual obligation is established in MSA §2.2 ("appropriate administrative, physical, and technical safeguards...as described in the Documentation") and reinforced in DPA §6.1 ("appropriate technical and organizational measures...as set forth in the Security, Privacy and Architecture Documentation"). Both provisions tie the contractual commitment to the SPARC, giving the segregation architecture described therein full contractual force. The Privacy Principles page provides corroborating evidence in the narrower AI/ML training context, confirming "data will not leak across workspaces." No physical separation between individual customers is explicitly described — but the "physical and/or logical" formulation in the acceptable position means logical separation alone is sufficient. The mechanism (unique customer ID enforcing logical separation at platform and infrastructure layers) is the standard SaaS multi-tenant architecture approach and is appropriate for a team chat deployment. No conflicting provisions exist across the document set — all relevant provisions are consistent and complementary. Classification is GREEN. aiPreferenceMet is false because no ideal preference was specified beyond the acceptable position.

— Note —
The AI cited 1 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "SFDC shall maintain appropriate technical and organizational measures for protection of the security (including protection against unauthorized or unlawful Processing and against accidental or unlawfu…"

> *"The Covered Services are operated on a multitenant architecture at both the platform and infrastructure layers that is designed to segregate and restrict Customer Data access based on business needs. The architecture provides a logical data separation for each different customer via a unique ID."*
> — Security, Privacy and Architecture Report
> *"SFDC will maintain appropriate administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Customer Data, as described in the Documentation. Those safeguards will include, but will not be limited to, measures designed to prevent unauthorized access to or disclosure of Customer Data (other than by Customer or Users)."*
> — https://www.salesforce.com/en-us/wp-content/uploads/sites/4/documents/legal/salesforce_MSA.pdf
> *"Data will not leak across workspaces."*
> — Slack Privacy Principles

Arbitration or other dispute resolution process

AI Comment: The acceptable position requires "no limitation as to method of dispute resolution." Across the Slack document set, dispute resolution is governed by a mandatory exclusive court jurisdiction framework rather than a discretionary, multi-method arrangement. For the most probable scenario — a US-domiciled Customer purchasing Slack online — the operative instrument is the Slack Supplemental Terms, which specifies California law and exclusive jurisdiction in San Francisco County, California courts. The substantively identical provisions in MSA §12.9 and §12.11 are superseded by the Supplemental Terms for online Slack orders per the Supplemental Terms' express "in place of" language.

This exclusive court jurisdiction regime constitutes a limitation on dispute resolution method: it forecloses arbitration, mediation, or litigation in alternative forums. This conflicts with the "no limitation" acceptable position. The limitation is materially less onerous than a mandatory arbitration clause — court proceedings preserve full judicial discovery, appellate rights, class action standing, and procedural due process protections that mandatory arbitration commonly eliminates.

A distinct RED-level concern exists for India-domiciled customers: MSA §12.16.1 imposes mandatory binding arbitration with cost-splitting and no guaranteed appeal. While not the primary scenario for this US-domiciled team chat deployment, the provision should be flagged for completeness and for any India-based team members or future expansion.

The User Terms' prevailing-party attorney-fee recovery provision adds a financial risk dimension: a losing party bears the winner's reasonable costs and fees. This creates an asymmetric deterrent that may discourage enforcement of smaller claims, effectively shaping dispute resolution in practice even if not in method.

Because the contract addresses dispute resolution but imposes limitations — exclusive court jurisdiction in a specific venue — that fall short of the "no limitation" acceptable position, yet do not rise to the level of mandatory arbitration for the primary US deployment scenario, a YELLOW classification is appropriate. Medium weight per the Review Specific Playbook; documented justification required if accepted as-is.

— Superseding reasoning —
The Slack Supplemental Terms explicitly state they apply "in place of the SFDC Contracting Entity, Notices, Governing Law, and Venue sections in the MSA" for online Slack orders. This express replacement language directly overrides MSA §12.9 for online Slack purchases. Because both provisions are substantively consistent for US-domiciled customers (California law; San Francisco-area courts), the superseding determination does not change the practical outcome for this deployment, but the Supplemental Terms are the controlling instrument.

> *"For an online order of Slack Services (a Slack plan purchased via the Slack website), the following applies in place of the SFDC Contracting Entity, Notices, Governing Law, and Venue sections in the MSA:"*
> — Slack Supplemental Terms | Legal | Slack
> *"Each party agrees to the applicable governing law above without regard to choice or conflicts of law rules, and to the exclusive jurisdiction of the applicable courts above."*
> — https://www.salesforce.com/en-us/wp-content/uploads/sites/4/documents/legal/salesforce_MSA.pdf
> *"The arbitration panel's decision shall be final, conclusive and binding on the parties to the arbitration. The Parties shall each pay one-half of the costs and expenses of such arbitration, and each shall separately pay its respective counsel fees and expenses."*
> — https://www.salesforce.com/en-us/wp-content/uploads/sites/4/documents/legal/salesforce_MSA.pdf
> *"Governing Law; Venue; Fees"*
> — User Terms of Service | Legal | Slack

Breach Indemnification

AI Comment: The playbook item requires indemnification from SFDC/Slack for (1) SFDC's own breaches of its contractual and data protection obligations and (2) breaches by subprocessors. "Indemnification" in its standard legal sense encompasses a defense obligation, a hold-harmless commitment, and compensation for losses — not merely general liability subject to a damages cap.

What the contract provides:

The MSA's indemnification framework (§9.1) is expressly and exclusively limited to intellectual property infringement claims brought by third parties against Customer. No indemnification provision anywhere in the document set extends to data breaches, security incidents, or violations of SFDC's data protection or confidentiality obligations. This is a deliberate structural choice: SFDC commits to defend and hold harmless Customer from IP infringement claims, but no equivalent defense obligation exists for breach-related third-party claims (e.g., regulatory enforcement actions or downstream customer lawsuits arising from a Slack data incident).

For subprocessor breaches, DPA §5.4 establishes general liability ("SFDC shall be liable for the acts and omissions of its Sub-processors to the same extent SFDC would be liable if performing the services of each Sub-processor directly under the terms of this DPA"). This is a liability provision, not an indemnification: it creates an obligation to compensate Customer for direct losses but includes no defense obligation for third-party claims. Moreover, DPA §11 explicitly subjects all DPA liability — including §5.4 subprocessor liability — to the MSA's limitation of liability cap (12 months of fees paid; consequential damages excluded under §10.2). In a material data breach scenario, the practical recovery ceiling would be significantly constrained.

DPA §7 establishes breach notification and reasonable remediation efforts, which are procedurally important but are not a substitute for indemnification.

Why YELLOW (not RED):

The contract is not silent — it provides partial protection through the DPA §5.4 subprocessor liability mechanism, robust security control obligations (DPA §6.1), breach notification procedures (DPA §7), and general liability recovery for direct damages (MSA §10.1). These provisions collectively establish a breach-response framework that provides more than nothing. YELLOW accurately reflects that the topic is addressed with materially weaker protection than the playbook item requires: liability exists but true indemnification (defend + hold harmless for third-party breach claims) does not.

Governing jurisdiction note:

For a US-domiciled team under California law, the consequential damages exclusion and 12-month liability cap are generally enforceable under California contract law. California courts routinely uphold sophisticated commercial liability caps. There is no statutory fill-in (e.g., CCPA/CPRA does not impose a vendor indemnification obligation on processors). The gap is therefore real and unmitigated by statute in the governing jurisdiction.

Practical risk for a team chat use case:

Slack processes all internal communications, file transfers, and potentially sensitive business data. A breach by SFDC or a subprocessor (e.g., AWS) affecting this workspace would expose the Customer organization to regulatory inquiry under CCPA, potential employee or client claims, and reputational harm — none of which SFDC would be obligated to defend against or indemnify Customer for under the current terms.

— Note —
The AI cited 6 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.

1. "SFDC will defend Customer against any claim, demand, suit or proceeding made or brought against Customer by a third party alleging that any Purchased Service infringes or misappropriates such third pa…"
2. "SFDC shall be liable for the acts and omissions of its Sub-processors to the same extent SFDC would be liable if performing the services of each Sub-processor directly under the terms of this DPA, unl…"
3. "Each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, and all DPAs between Authorized Affiliates and SFDC, whether in contract, tor…"
4. "IN NO EVENT SHALL THE AGGREGATE LIABILITY OF EACH PARTY TOGETHER WITH ALL OF ITS AFFILIATES ARISING OUT OF OR RELATED TO THIS AGREEMENT EXCEED THE TOTAL AMOUNT PAID BY CUSTOMER AND ITS AFFILIATES HERE…"
5. "IN NO EVENT WILL EITHER PARTY OR ITS AFFILIATES HAVE ANY LIABILITY ARISING OUT OF OR RELATED TO THIS AGREEMENT FOR ANY LOST PROFITS, REVENUES, GOODWILL, OR INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL…"
6. "SFDC maintains security incident management policies and procedures specified in the Security, Privacy and Architecture Documentation and shall notify Customer without undue delay after becoming aware…"

Subprocessor Agreements

AI Comment: The Salesforce/Slack DPA (Document ID: rztql8356vi4ymqu0aokqwuv) substantially addresses the playbook's primary requirement but leaves a material gap on its secondary privileged-access requirement.

Primary requirement — written agreements at least as protective as this DPA: FULLY MET. DPA §5.1 expressly states that "SFDC or an SFDC Affiliate has entered into a written agreement with each Sub-processor containing, in substance, data protection obligations no less protective than those in the Agreement with respect to the protection of Personal Data." Since the DPA is itself incorporated into and forms part of the Agreement (MSA §2.2, DPA §6.1), the standard "no less protective than those in the Agreement" is functionally equivalent to "at least as strict as this DPA." Additional reinforcing provisions exist: DPA §5.4 makes SFDC fully liable for subprocessor acts and omissions as if SFDC performed those services directly; DPA §8.2 requires subprocessors to be bound by the government-access-request commitments in the Standard Contractual Clauses and the Salesforce Processor BCR.

Secondary requirement — privileged-access subprocessors must be prohibited or subject to Customer's prior approval: NOT MET. The contract documents are completely silent on any differentiated treatment of subprocessors based on access privilege level. The notification-and-objection mechanism in DPA §5.2–5.3 provides only reactive, undifferentiated control over all new subprocessors: Customer must affirmatively subscribe to notifications and then object within 30 days of notice. This is meaningfully different from "prior approval" — it is opt-in, post-notification, and applies uniformly regardless of access tier. No provision prohibits high-privilege subprocessors, subjects their engagement to Customer pre-clearance, or even defines what constitutes "privileged access." The gap is complete for this sub-requirement.

Overall classification: YELLOW. The core written-agreement obligation is clearly met with strong supporting provisions (full liability pass-through, SCC/BCR obligations on subprocessors). However, for a Critical-weight item, the absence of any prior-approval or prohibition mechanism specifically for privileged-access subprocessors is a material gap. The notification/objection mechanism provides partial but insufficient mitigation for this specific requirement. Reviewing counsel should negotiate a contractual addendum or side letter requiring Slack to (a) notify Customer specifically when a proposed new subprocessor would have privileged access to Customer Data and (b) obtain Customer's written consent before onboarding such subprocessor.

— Note —
The AI cited 4 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "The Infrastructure and Sub-processor Documentation contains a mechanism to subscribe to notifications of new Sub-processors for each applicable Service, and if Customer subscribes, SFDC shall provide …"
2. "Customer may object to SFDC's use of a new Sub-processor by notifying SFDC promptly in writing within thirty (30) days of receipt of SFDC's notice in accordance with the mechanism set out in section 5…"
3. "SFDC shall be liable for the acts and omissions of its Sub-processors to the same extent SFDC would be liable if performing the services of each Sub-processor directly under the terms of this DPA, unl…"
4. "SFDC shall ensure that Sub-processors involved in the Processing of Personal Data are subject to the relevant commitments regarding Government Access Requests in the Standard Contractual Clauses and S…"

> *"SFDC or an SFDC Affiliate has entered into a written agreement with each Sub-processor containing, in substance, data protection obligations no less protective than those in the Agreement with respect to the protection of Personal Data to the extent applicable to the nature of the Services provided by such Sub-processor."*
> — Data Processing Addendum

Modification of Terms

AI Comment: The documents substantially but incompletely address modification-of-terms procedures across the Slack agreement hierarchy.

Acceptable Position Assessment — Substantially But Not Fully Met:

For material changes, the documents satisfy the core requirements of the acceptable position: (a) the Slack Supplemental Terms (§ Changes to Terms) require "reasonable notice prior to the change taking effect" before material changes to those terms become effective; (b) the User Terms (§ Modifications) require advance email or in-app notice before material changes take effect; (c) current versions are posted and accessible at all times with effective dates specified. These provisions collectively ensure material changes are ascertainable in advance of taking effect.

However, two meaningful gaps prevent a GREEN classification on the acceptable position:

1. **Non-material changes — advance notice gap:** The User Terms states that "all other changes [i.e., non-material] will become effective on the date we publish the change" (§ Modifications, sentence 2 of §1-45). Changes effective on the date of publication are technically ascertainable at the moment they take effect, but there is no prior notification window — a reviewer who does not actively monitor the posted page could miss a change before or at the moment it becomes binding. The Supplemental Terms do not specify the treatment of non-material changes at all, creating additional ambiguity.

2. **"Reasonable notice" — undefined period:** Neither the User Terms nor the Supplemental Terms specify a minimum notice period for material changes. "Reasonable notice" is vague and could, in practice, permit very short advance windows.

Preference Assessment — Not Met:

The ideal preference requires two elements: (a) advance written notice (partially satisfied for material changes only) and (b) an opportunity to terminate with a pro-rata refund upon disagreement with changed terms. Neither the Supplemental Terms nor the MSA provides a termination-with-refund mechanism tied to disagreement with term changes. The sole operative mechanism is "use = acceptance" (Supplemental Terms § Changes to Terms), which creates no meaningful exit right. The MSA's for-cause termination right (§ 11.3) requires a material uncured breach and does not apply to a Customer's mere disagreement with modified terms.

Favorable Signal — MSA Stability: The MSA, the primary governing document under the Slack Terms hierarchy, does not contain a visible clause reserving SFDC's right to unilaterally modify the MSA's terms. Absent such a clause, MSA changes would appear to require mutual written agreement. This is a positive structural signal, though assessed with moderate confidence given the MSA's online versioning with a "last updated" date.

Overall: YELLOW. The acceptable position is substantially met for material changes but has a real gap on non-material changes (no advance notice) and on the vagueness of the notice period. The ideal preference is unmet — no termination right with pro-rata refund is available upon disagreement with changed terms. For a High-weight item, this gap is meaningful.

> *"Modifications"*
> — User Terms of Service | Legal | Slack
> *"Any material revisions to these User Terms will become effective on the date set forth in our notice, and all other changes will become effective on the date we publish the change."*
> — User Terms of Service | Legal | Slack
> *"If we make a material change to these Supplemental Terms, we will provide Customer with reasonable notice prior to the change taking effect."*
> — Slack Supplemental Terms | Legal | Slack
> *"Customer understands and agrees that use of the Slack Services after the date on which these Supplemental Terms have changed will constitute acceptance of the updated Supplemental Terms."*
> — Slack Supplemental Terms | Legal | Slack
> *"If we make changes that materially alter your privacy rights, Slack will provide additional notice, such as via email or through the Services."*
> — Privacy Policy | Legal | Slack
> *"12.3 Entire Agreement and Order of Precedence. This Agreement is the entire agreement between SFDC and Customer regarding** Customer's use of Services and supersedes all prior and contemporaneous agreements, proposals or representations, written or oral, concerning its subject matter. The parties agree that any term or condition stated in a Customer purchase order or in any other Customer order documentation (excluding Order Forms) is void. In the event of any conflict or inconsistency among the following documents, the order of precedence shall be: (1) the applicable Order Form, (2) this Agreement, and (3) the Documentation. Titles and headings of sections of this Agreement are for convenience only and shall not affect the construction of any provision of this Agreement."*
> — https://www.salesforce.com/en-us/wp-content/uploads/sites/4/documents/legal/salesforce_MSA.pdf

Processing Location Restrictions

AI Comment: The playbook item imposes a disjunctive requirement: (Condition A) all Vendor processing must occur in the US, Canada, or the EU; OR (Condition B) processing must be completed under Standard Contractual Clauses. Neither condition is fully satisfied, yielding a YELLOW classification for this High-weight item.

Condition A — NOT MET: The Privacy Policy explicitly confirms that Slack transfers Personal Data to countries beyond US/Canada/EU, specifically identifying Australia, India, Japan, and South Korea as destination countries (in addition to the US). The SPARC commits to data-at-rest storage within "certain major geographic areas except as otherwise provided in your Order Form" — a vague commitment that defers geographic specificity to the individual Order Form, preventing public confirmation of restriction to US/Canada/EU. The DPA maintains a global sub-processor list; DPA §13 specifically references Slack's APEC PRP certification for APEC-country sub-processor transfers, confirming processing in those locations.

Condition B — PARTIALLY MET: SCCs are incorporated into the DPA (Revision April 2026) under §12 "Europe Specific Provisions" and Schedule 1 "Transfer Mechanisms for European Data Transfers." The MSA §2.2 also conditions SCC and Processor BCR application on data originating "from the European Economic Area (EEA), the United Kingdom and Switzerland." For a US-domiciled customer's data processed by sub-processors in Australia, India, Japan, or South Korea, no SCC mechanism applies under these documents. The Privacy Policy's SCC language could be read more broadly (as if SCCs apply to all Slack transfers to those countries), but this reading is superseded by the DPA's explicit EU-limited scope per document hierarchy (see superseding analysis).

Why YELLOW and not RED: (1) For a standard US-domiciled team chat deployment, primary service hosting runs

through Slack Technologies, LLC on AWS infrastructure — likely US-based for US customers, meaning the core message storage and processing for the primary use case falls within the acceptable geographic range; (2) APEC PRP certification (DPA §13) applies specifically to Slack entities and covers transfers among APEC economies (AU, JP, KR), providing a recognized — if not SCC-equivalent — cross-border privacy framework for a substantial portion of the identified gap countries; (3) DPA §5.1 requires all sub-processors to maintain data protection obligations "no less protective than those in the Agreement," providing contractual floor protections for international processing; (4) SCCs are fully operative for any EU-origin personal data flowing through Slack.

Key residual risk for a US customer: US-originated Customer Data transferred to sub-processors in non-EU, non-APEC jurisdictions (if any), or to APEC-country sub-processors where only the APEC PRP framework applies rather than the SCCs required by the playbook, remains without SCC coverage. Additionally, the Slack Supplemental Terms authorize AI/ML model training processing on Customer Data without specifying geographic constraints or requiring SCCs for that processing activity.

— Superseding reasoning —
The Privacy Policy's International Data Transfers section states that SCCs are used "for transfers to, among others, Australia, Canada, India, Japan, South Korea, and the United States" — language that, read in isolation, could suggest SCCs cover all Slack international transfers to those countries regardless of data origin, which would satisfy the playbook's Condition B. However, the DPA — which is an addendum that "forms part of the Agreement" (DPA §1, "How This DPA Applies") and thus holds contractual precedence over the Privacy Policy — explicitly scopes its SCC provisions within "12. EUROPE SPECIFIC PROVISIONS" and Schedule 1 titled "Transfer Mechanisms for European Data Transfers," applying only to "European Personal Data." Under the document hierarchy established in the User Terms §"Entire Agreement" (Contract prevails over User Terms which prevails over referenced pages including the Privacy Policy) and the MSA §12.3 order of precedence (Order Form > Agreement > Documentation), the DPA's contractual EU-limited SCC scope controls over the Privacy Policy's broader disclosure language. PIF 3 (DPA §12) supersedes PIF 1 (Privacy Policy SCC statement).

— Note —
The AI cited 2 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. ""European Personal Data" means the Personal Data subject to European Data Protection Laws and Regulations."
2. "Notwithstanding the foregoing, Slack Technologies, LLC and Slack Technologies Limited (collectively "Slack") have obtained PRP certification and shall Process Personal Data submitted to Services provi…"

> *"Slack may transfer your Personal Data to countries other than the one in which you live, including transfers to the United States."*
> — Privacy Policy | Legal | Slack
> *"Slack uses Standard Contractual Clauses approved by the European Commission (and the equivalent standard contractual clauses for the UK where appropriate) for transfers to, among others, Australia, Canada, India, Japan, South Korea, and the United States."*
> — Privacy Policy | Legal | Slack
> *"To the extent Personal Data from the European Economic Area (EEA), the United Kingdom and Switzerland are processed by SFDC, its Processor Binding Corporate Rules,, and/or the Standard Contractual Clauses shall apply, as further set forth in the DPA."*
> — https://www.salesforce.com/en-us/wp-content/uploads/sites/4/documents/legal/salesforce_MSA.pdf
> *"SFDC or an SFDC Affiliate has entered into a written agreement with each Sub-processor containing, in substance, data protection obligations no less protective than those in the Agreement with respect to the protection of Personal Data to the extent applicable to the nature of the Services provided by such Sub-processor."*
> — Data Processing Addendum
> *"Salesforce will store Customer Data at rest within certain major geographic areas except as otherwise provided in your Order Form."*
> — Security, Privacy and Architecture Report
> *"SFDC may access Customer Data in Slack for the following reasons, and Customer instructs SFDC to process its Customer Data for such purposes:*
>
> *1. to train models for use by the services and features that Customer has access to;*
> *2. to improve services and features that Customer has access to;*
> *3. to conduct research and development of products that Customer will have access to without additional cost;*
> *4. as otherwise provided in the MSA between SFDC and Customer."*
> — Slack Supplemental Terms | Legal | Slack

Audit Logging

AI Comment: The playbook item requires the ability to examine whether and by whom personal data has been entered into, modified, or removed from data processing systems — that is, comprehensive audit logging of PII access and manipulation operations. The documents collectively address audit logging, but with a meaningful gap between what is explicitly described and what the item requires.

What the contract addresses:
The Security, Privacy and Architecture Report (SPARC) is the most specific document on this topic. It confirms: (1) "Detailed access logs are available both to users and administrators of paid teams," with sign-in event logging (device type, IP address) as the explicitly described content; (2) team administrators of paid plans can review consolidated access logs for their whole workspace; and (3) an extensive centralised logging environment captures security, monitoring, availability, and access metrics. Both the Acceptable Use Policy (AUP) and the SPARC's "Digital Services Act and Other Acceptable Use

Information" section state: "There are technical controls and audit policies in place to ensure that access to Customer Data is logged" — a broad statement that, read generously, could encompass PII access events. The DPA (§ 6.1) requires appropriate technical and organisational measures protecting against unauthorised access to Customer Data and explicitly cross-references the SPARC as the operative specification.

Where the gap lies:
The only concretely described log content is authentication-level: sign-in events with device type and IP address. The SPARC does not explicitly confirm that granular data-manipulation operations — who entered, modified, or deleted specific personal data records — are logged and accessible to customer administrators. The phrase "detailed access logs" is promising but ambiguous: without further elaboration, it is unclear whether these logs capture read/write/delete operations on individual records (as the playbook requires) or are limited to session/authentication events. The statement "access to Customer Data is logged" is broad enough to cover the requirement in principle, but the contextual framing (appearing alongside employee-access controls) introduces ambiguity about whether it extends to customer-user-level PII manipulation logging. Additionally, the "detailed access logs" are explicitly available only to paid-plan administrators, which is appropriate for a typical enterprise Slack deployment but is a plan-level dependency.

Classification: YELLOW. The topic is addressed — audit logging exists, is referenced across multiple documents, and access logs are available to customer administrators — but the contract language does not explicitly confirm the level of granularity required (who entered/modified/deleted which specific personal data records). The acceptable position for a High weight item requires a clearer, more affirmative commitment than what the present language provides. The item is not RED because meaningful logging infrastructure and customer-administrator access to logs are confirmed.

— Superseding reasoning —
The AUP (PIF index 1) and the SPARC's "Digital Services Act and Other Acceptable Use Information" section (PIF index 2) contain identical language regarding employee access controls and audit logging. No conflict exists between these two references — they are consistent across documents. However, for security-specific matters, the SPARC is the authoritative technical document expressly referenced by the DPA (§ 6.1) as the operative specification for security controls, making the SPARC the primary reference. The AUP reference is supplementary context, not a controlling source on security architecture. Because the language is identical (no contradiction), formal superseding is not required, but the SPARC version is treated as the governing source for security classification purposes.

— Note —
The AI cited 2 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "Access Logging: Detailed access logs are available both to users and administrators of paid teams.

We log every time an account signs in, noting the type of device used and the IP address of the conn…"
2. "SFDC shall maintain appropriate technical and organizational measures for protection of the security (including protection against unauthorized or unlawful Processing and against accidental or unlawfu…"

> *"We place strict controls over employee access to Customer Data. There are technical controls and audit policies in place to ensure that access to Customer Data is logged."*
> — Acceptable Use Policy | Legal | Slack
> *"We place strict controls over employee access to Customer Data. There are technical controls and audit policies in place to ensure that access to Customer Data is logged."*
> — Security, Privacy and Architecture Report
> *"Systems used in the provision of the Covered Services log information to their respective system log facilities or a centralized logging service (for network systems) in order to enable security reviews and analysis. Salesforce maintains an extensive centralised logging environment in the production environment which contains information pertaining to security, monitoring, availability, access and other metrics about the Covered Services. These logs are analysed for security events via automated monitoring software, overseen by the security team."*
> — Security, Privacy and Architecture Report

Data Processing Security Policies

AI Comment: The playbook item requires (1) adequate security on data processing systems and (2) adequate policies to prevent unauthorized access to those systems. Both prongs are extensively addressed across the Slack/SFDC document set, at multiple layers — contractual obligation, contractual warranty, personnel controls, third-party certification commitments, and granular operational detail — producing a GREEN classification at HIGH confidence.

Prong 1 — Adequate security on data processing systems:
The MSA §2.2 commits to "appropriate administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Customer Data." The DPA §6.1 reinforces and expands this with enumerated protections against "unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Customer Data," paired with active compliance monitoring and a no-material-decrease guarantee. The SPARC (Security, Privacy and Architecture Report) operationalizes these commitments with specific technical controls: detailed access logging for paid-tier administrators, remote access management (instant session termination on demand), automated vulnerability scanning and remediation, mandatory security reviews for new features, automated static analysis of code, two-factor authentication across the production environment, firewalls configured to industry best practices, and intrusion detection by Salesforce or authorized external entities. The SPARC additionally commits to minimum alignment with ISO 27001, ISO 27002, and ISO 27018. The DPA §6.2 commits to maintaining ISO 27001 certification and SOC 2 (SSAE 18) reports for the duration of the Agreement — providing independent third-party verification that security controls meet those standards.

Prong 2 — Adequate policies to prevent unauthorized access:
The MSA §2.2 explicitly names prevention of unauthorized access as a specific inclusion within the safeguard commitment. The DPA §4.1 addresses the human-access vector through mandatory training, written confidentiality agreements with post-employment survival obligations, and a contractual requirement limiting SFDC personnel access to Personal Data strictly to those with a need to perform services under the Agreement. The AUP (and SPARC) additionally state that strict controls govern employee access to Customer Data, backed by technical controls and audit policies that ensure all access is logged. The DPA §8.1 addresses government access requests with detailed protections including notification to Customer, reasonable challenge obligations, and a certification that no back doors have been created.

No Silence Gap: Every aspect of the playbook item is explicitly addressed. The item is not silent.

No Superseding Conflict: The MSA, DPA, and SPARC are hierarchically consistent and additive. The MSA §12.3 establishes order of precedence as (1) Order Form, (2) MSA, (3) Documentation; the DPA is incorporated by reference into the MSA (MSA §2.2), and the SPARC is the "Security, Privacy and Architecture Documentation" explicitly referenced in both. There is no conflict among these provisions — each layer adds specificity without contradicting any other.

One Contextual Note (not classification-changing): The Slack Supplemental Terms §1 grants SFDC broad authorization to access Customer Data for model training and service improvement. This is a separately agreed processing purpose rather than a security vulnerability, and the Privacy Principles document clarifies that technical controls prevent individual Slack employees from accessing underlying Customer Data content during ML/AI model development. This does not alter the GREEN classification for this item but is relevant context for any AI/data-use playbook items.

Basis for GREEN: The contractual commitments are specific, binding, backed by an express warranty that security will not materially decrease during the subscription term, and externally verified through maintained ISO 27001 and SOC 2 certifications. The SPARC provides granular operational detail on specific preventive controls. Collectively, this substantially meets the acceptable position for a High-weight item requiring adequate security and unauthorized access prevention policies.

— Note —
The AI cited 4 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "SFDC warrants that during an applicable subscription term (a) this Agreement, the Order Forms and the Documentation will accurately describe the applicable administrative, physical, and technical safe…"
2. "SFDC shall maintain appropriate technical and organizational measures for protection of the security (including protection against unauthorized or unlawful Processing and against accidental or unlawfu…"
3. "SFDC shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibiliti…"
4. "SFDC has obtained the third-party certifications and audits set forth in the Security, Privacy and Architecture Documentation for each applicable Service. Where SFDC has obtained ISO 27001 certificati…"

> *"SFDC will maintain appropriate administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Customer Data, as described in the Documentation. Those safeguards will include, but will not be limited to, measures designed to prevent unauthorized access to or disclosure of Customer Data (other than by Customer or Users)."*
> — https://www.salesforce.com/en-us/wp-content/uploads/sites/4/documents/legal/salesforce_MSA.pdf
> *"Security Controls"*
> — Security, Privacy and Architecture Report
> *"At a minimum, Salesforce will align with prevailing*
> *industry standards such as ISO 27001, ISO 27002, and ISO 27018."*
> — Security, Privacy and Architecture Report
> *"Salesforce, or an authorized external entity, will monitor the Covered Services for unauthorized intrusions."*
> — Security, Privacy and Architecture Report
> *"We place strict controls over employee access to Customer Data. There are technical controls and audit policies in place to ensure that access to Customer Data is logged."*
> — Acceptable Use Policy | Legal | Slack

Security Certifications

AI Comment: The acceptable position requires (1) a current SOC 2 Type II report or ISO 27001 certification covering the services, and (2) availability of that report/certificate to the Customer on request. Both requirements are substantively met across the DPA and the Security, Privacy and Architecture Report (SPARC).

Certification existence and maintenance (requirement 1): DPA §6.2 expressly names ISO 27001 certifications and SSAE 18 SOC 2 reports among the certifications SFDC has obtained for the applicable services, and contractually commits to maintaining these certifications — or appropriate and comparable successors — for the duration of the Agreement. The SPARC independently confirms that certifications are performed on the Slack services and that copies are downloadable, and separately commits that Salesforce will align at minimum with ISO 27001, ISO 27002, and ISO 27018. Because the playbook requirement is satisfied by ISO 27001 *or* SOC 2 Type II, and ISO 27001 is explicitly committed to in both the DPA and the SPARC, the certification prong is met even setting aside the SOC 2 point addressed below.

SOC 2 Type II specificity gap (minor): The DPA refers to "SSAE 18 Service Organization Control (SOC) 2 reports" without expressly specifying "Type II." SSAE 18 covers both Type I (point-in-time design evaluation) and Type II (operating effectiveness over a period). For an enterprise SaaS platform of Slack/Salesforce's scale and the annual cadence

referenced in the SPARC, Type II is the standard industry form — the conditional framing ("Where SFDC has obtained…") simply allows for services that may not carry every certification. Because ISO 27001 alone satisfies the "or" in the acceptable position, this gap does not affect the overall classification, though reviewers should verify the specific SOC 2 Type II designation in any audit report actually provided.

Available on request (requirement 2): DPA §6.3.1 provides an explicit contractual mechanism: upon Customer's written request at reasonable intervals, SFDC shall make available copies of its most recent third-party audits or certifications set forth in the Security, Privacy and Architecture Documentation. The "reasonable intervals" qualifier is standard market practice for audit report access and does not materially restrict the right; it merely prevents requests at an impractical frequency. The SPARC further provides that customers may download copies of applicable certifications directly.

Contractual chain: The DPA is incorporated into the Main Services Agreement by reference at MSA §2.2, making its certification commitments part of the binding contractual framework governing the Slack deployment. The SPARC is covered by the MSA §8.2 warranty that the Documentation accurately describes applicable safeguards, giving the SPARC's certification statements additional contractual backing.

"Comparable successors" clause: DPA §6.2 permits replacement of ISO 27001 or SOC 2 with "appropriate and comparable successors." This is a standard and reasonable carve-out accommodating certification framework evolution and does not meaningfully weaken the protection.

Overall: The DPA's express naming of ISO 27001 and SOC 2, its maintenance commitment, and its Customer-access mechanism — corroborated by the SPARC's operational confirmation — collectively meet the acceptable position. Classification: GREEN.

— Superseding reasoning —
The Privacy Policy's general statement that "Slack has received internationally recognized security certifications" (PIF 4) is superseded by the DPA §6.2's specific enumeration of ISO 27001 certifications and SSAE 18 SOC 2 reports (PIF 0). The DPA is a legally binding data processing addendum to the main commercial agreement — it addresses certification obligations with contractual precision and named standards, whereas the Privacy Policy's security section is a public-facing disclosure document containing a general marketing-level statement. Under the specific-over-general drafting principle, the DPA's named certifications and maintenance commitment govern the classification.

— Note —
The AI cited 2 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "SFDC has obtained the third-party certifications and audits set forth in the Security, Privacy and Architecture Documentation for each applicable Service. Where SFDC has obtained ISO 27001 certificati…"
2. "Upon Customer's written request at reasonable intervals, and subject to the confidentiality obligations set forth in the Agreement, SFDC shall:

(i) the make available to Customer (or Customer's Third…"

> *"Certifications"*
> — Security, Privacy and Architecture Report
> *"At a minimum, Salesforce will align with prevailing industry standards such as ISO 27001, ISO 27002, and ISO 27018."*
> — Security, Privacy and Architecture Report
> *"Slack has received internationally recognized security certifications."*
> — Privacy Policy | Legal | Slack

Anti-Virus Solution

AI Comment: The vendor's terms across all provided documents are entirely silent on anti-virus or anti-malware software as an explicit, named contractual commitment. No document in the set directly states that authorized computer systems must have — or do have — an anti-virus solution. The phrase "anti-virus" does not appear anywhere in the document set.

Under the silence-handling framework, a High weight item defaults to RED when the contract is silent. However, a one-level downgrade to YELLOW is warranted on INDUSTRY_NORM grounds: Salesforce/Slack has contractually committed to maintaining ISO 27001 certification for the duration of the Agreement (DPA §6.2) and to aligning with ISO 27002 as a minimum standard (SPARC, Security Controls section). ISO 27002:2022 Control A.8.7 (Protection against malware) is a required control for ISO 27001 certified organizations and explicitly mandates anti-malware protection across systems. An ISO 27001-certified enterprise SaaS provider that does not implement anti-malware controls would be in breach of its certification obligations. The practical risk that Slack entirely lacks anti-virus controls is therefore low given these maintained certifications.

Nonetheless, the absence of an explicit contractual anti-virus clause means the item cannot be GREEN. Residual concerns include: (1) the SPARC addresses production host vulnerability scanning — a related but distinct control from endpoint anti-virus; (2) the scope of "all authorized computer systems" versus only production infrastructure is ambiguous and unaddressed; (3) the ISO 27001 pathway to anti-virus coverage is inferential, not express. This item should be flagged for follow-up: the reviewing team should request written vendor confirmation that anti-virus/anti-malware controls are deployed across all authorized systems, or obtain the relevant sections of the SOC 2 Type II report that address malware protection.

— Applied silence standard —
Basis: INDUSTRY_NORM

Citation: ISO 27002:2022 Control A.8.7 (Protection against malware) is a mandatory control for ISO 27001-certified organizations. Salesforce/Slack contractually commits to maintaining ISO 27001 certification (DPA §6.2) and aligning with ISO 27002 as a minimum standard (SPARC Security Controls section). An ISO 27001-certified enterprise SaaS provider must implement anti-malware controls as a certification requirement, making the practical risk of entirely absent anti-virus protection low. Industry practice for enterprise SaaS providers at this certification level universally includes anti-malware deployment.

— Note —
The AI cited 1 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "SFDC shall maintain appropriate technical and organizational measures for protection of the security (including protection against unauthorized or unlawful Processing and against accidental or unlawfu…"

> *"Where SFDC has obtained ISO 27001 certifications and SSAE 18 Service Organization Control (SOC) 2 reports for a particular Service as described in the Documentation, SFDC agrees to maintain these certifications or standards, or appropriate and comparable successors thereof, for the duration of the Agreement"*
> — Data Processing Addendum
> *"At a minimum, Salesforce will align with prevailing industry standards such as ISO 27001, ISO 27002, and ISO 27018."*
> — Security, Privacy and Architecture Report
> *"Security Controls"*
> — Security, Privacy and Architecture Report

Password Encryption

AI Comment: The playbook item requires an affirmative showing that passwords are always stored in encrypted form — a High weight item for any SaaS deployment handling authentication credentials. A comprehensive review of all nine documents in the set reveals no explicit contractual statement that Slack stores user account passwords in encrypted or hashed form.

The four provisions with any relevance to this item are: (1) DPA §6.2, which commits Slack to maintaining ISO 27001 and SOC 2 (SSAE 18) certifications for the duration of the agreement; (2) the Security, Privacy and Architecture Report ("SPARC"), which commits Slack to aligning "at a minimum" with ISO 27001, ISO 27002, and ISO 27018; (3) the Privacy Policy's statement that Slack does not store passwords for third-party service integrations — a distinct and narrower context than Slack account passwords; and (4) MSA §2.2, which provides general "appropriate administrative, physical, and technical safeguards" language. None of these provisions explicitly states that Slack account passwords are stored encrypted or hashed.

Under the silence-handling framework, the default classification for a High weight item is RED. A one-level downgrade to YELLOW is applied on INDUSTRY_NORM grounds for three reasons: (a) SaaS vendor contracts routinely do not enumerate specific cryptographic implementations — instead, such details are delegated to security certification frameworks and audit reports, making contract silence on this specific point standard market practice; (b) Slack's binding commitment to maintain ISO 27001 and SOC 2 Type II certifications (DPA §6.2) implicitly encompasses proper credential management — ISO 27002 Control A.9.4.3 (and its equivalent in current revision) and SOC 2 Trust Services Criteria CC6.1 both require appropriate authentication mechanisms including secure storage of credentials; and (c) the practical risk that an organization sustaining ISO 27001 and SOC 2 Type II audits stores authentication passwords in plaintext is negligible.

The item remains YELLOW rather than GREEN because the acceptable position requires that passwords are stored in encrypted form, and the available evidence is exclusively implicit through certification commitments rather than an explicit contractual warranty or representation. A GREEN classification would require language such as "passwords are stored using industry-standard one-way cryptographic hashing" or an equivalent explicit representation in the contract or a DPA schedule. Reviewers may wish to request such a representation in any negotiated agreement or DPA amendment.

— Applied silence standard —
Basis: INDUSTRY_NORM
Citation: SaaS vendor contracts routinely do not enumerate specific cryptographic implementations for credential storage, instead relying on security certification frameworks. Slack's commitment to maintain ISO 27001 and SOC 2 (SSAE 18) certifications (DPA §6.2) and to align with ISO 27001, ISO 27002, and ISO 27018 (SPARC) implicitly encompasses secure password storage: ISO 27002 addresses authentication and access control mechanisms (including password management), and SOC 2 Trust Services Criteria CC6.1 covers logical access security controls. The practical risk of non-compliance is low given Slack's sustained ISO 27001 and SOC 2 Type II certification posture.

— Superseding reasoning —
DPA §6.2 provides more specific and auditable security obligations than MSA §2.2's general "appropriate safeguards" language. As an addendum to and integral part of the MSA, the DPA supplements the MSA's general security obligation with specific, named certification frameworks (ISO 27001, SOC 2) against which compliance can be independently verified. For purposes of this item, DPA §6.2 is the controlling provision on security standards, with MSA §2.2 acting as the residual general obligation. No conflict exists between these provisions — the DPA is more specific on the same subject.

> *"Where SFDC has obtained ISO 27001 certifications and SSAE 18 Service Organization Control (SOC) 2 reports for a particular Service as described in the Documentation, SFDC agrees to maintain these certifications or standards, or appropriate and comparable successors thereof, for the duration of the Agreement"*
> — Data Processing Addendum
> *"At a minimum, Salesforce will align with prevailing industry standards such as ISO 27001, ISO 27002, and ISO 27018."*

— Security, Privacy and Architecture Report

"We do not, however, receive or store passwords for any of these Third-Party Services when connecting them to the Services."

— Privacy Policy | Legal | Slack

"SFDC will maintain appropriate administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Customer Data, as described in the Documentation. Those safeguards will include, but will not be limited to, measures designed to prevent unauthorized access to or disclosure of Customer Data (other than by Customer or Users)."

— https://www.salesforce.com/en-us/wp-content/uploads/sites/4/documents/legal/salesforce_MSA.pdf

Termination for Cause

AI Comment: The playbook item requires that the Customer be able to terminate the agreement if the Vendor (Slack/SFDC) breaches. The contract fully satisfies this requirement. The governing document — the Salesforce Main Services Agreement (MSA), incorporated by reference into the Slack Terms — contains an explicit bilateral termination-for-cause provision at §11.3. It permits either party, including Customer, to terminate upon 30 days' written notice of an uncured material breach, or immediately upon the other party's insolvency/bankruptcy. This is the market-standard termination-for-cause formulation. The 30-day cure period and "material breach" threshold are standard and do not represent a restriction that undermines the Customer's right. Separately, the DPA adds supplementary termination rights in specific scenarios (sub-processor objection and inability to comply with local data protection laws), which further expand — not restrict — the Customer's exit options. The weight is "Acceptable to Deviate," meaning compliance is not critical, but the terms here are in fact favorable; no exception or deviation is needed. No ideal preference was specified, so aiPreferenceMet is false. Classification is GREEN with HIGH confidence.

— Note —
The AI cited 2 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "A party may terminate this Agreement for cause (i) upon 30 days written notice to the other party of a material breach if such breach remains uncured at the expiration of such period, or (ii) if the o…"
2. "If SFDC is unable to make available such change promptly, Customer may terminate the applicable Order Form(s) and suspend the transfer of Personal Data in respect only to those Services which cannot b…"

"If SFDC is unable to make available such change within a reasonable period of time, which shall not exceed sixty (60) days, Customer may terminate the applicable Order Form(s) with respect only to those Services which cannot be provided by SFDC without the use of the objected-to new Sub-processor by providing written notice to SFDC."

— Data Processing Addendum

Breach Notification Timeline

AI Comment: The DPA (Section 7) and the SPARC (Incident Management section) both commit Slack/SFDC to notify customers "without undue delay" after becoming aware of a Customer Data Incident. The topic is therefore not silent — an affirmative breach notification obligation exists. However, the contract falls short of the playbook's acceptable position on three distinct dimensions:

Gap 1 — Missing 72-hour outer deadline. The acceptable position requires notification "without undue delay, and in any event within 72 hours." Every document in the set uses only "without undue delay," with no explicit hourly cap. The phrase "without undue delay" is a recognized legal standard but it is open-ended and vendor-interpreted. Without a contractual outer bound, there is no enforceable deadline against which the customer could measure lateness. This is the central deficiency.

Gap 2 — Scope limited to actual Customer Data Incidents; suspected breaches not explicitly covered. DPA Section 7 defines the notification trigger as SFDC "becoming aware of the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data" (a "Customer Data Incident"). This definition addresses actual, known incidents. The playbook also requires notification of "suspected" breaches. The DPA's "becoming aware" language may in practice be read narrowly to require confirmed awareness before the obligation arises, leaving suspected-but-unconfirmed incidents outside the contractual trigger.

Gap 3 — No notification obligation for other DPA compliance breaches. The playbook sub-requirement (ii) covers "any other actual or potential breach of the DPA" (i.e., non-data-incident DPA compliance failures). DPA Section 7 is strictly scoped to Customer Data Incidents. General DPA compliance breaches are not covered by any notification provision in the document set.

Superseding determination. The DPA (Agreement-layer document under MSA §12.3 hierarchy) governs over the SPARC (Documentation-layer). The SPARC's incident management provision adds a "to the extent permitted by law" qualifier that further weakens the commitment; this subordinate language is controlled by the DPA. The governing provision is DPA Section 7.

Jurisdiction note. Under California law (most probable governing jurisdiction for a US-domiciled customer), there is no B2B processor-to-controller 72-hour notification statute that would fill the contractual gap. California's breach notification statutes (Cal. Civ. Code §§ 1798.29, 1798.82) regulate consumer-facing disclosures, not processor-to-controller notification timelines. GDPR Article 33's 72-hour standard is not enforceable under California law. No statutory downgrade therefore applies to the gap.

Conclusion. Classification is YELLOW because breach notification is substantively addressed (the obligation exists with a recognized legal standard), but the contract provides materially weaker protection than the acceptable position: no firm 72-

hour deadline, incomplete scope (suspected breaches, DPA compliance breaches), and a qualified SPARC commitment. The ideal 24-hour preference is clearly unmet. For a Critical-weight item, this gap requires documented assessment and should be flagged for renegotiation or risk acceptance by senior legal.

— Superseding reasoning —
The SPARC (Security, Privacy and Architecture Report) is "Documentation" as defined in MSA §1 ("the applicable Service's Trust and Compliance documentation"). The DPA is an addendum to the Main Services Agreement and therefore occupies the "Agreement" layer. Under MSA §12.3, the order of precedence is: (1) applicable Order Form, (2) the Agreement (MSA and addenda), (3) Documentation. Accordingly, the DPA's breach notification provision (Section 7) supersedes the SPARC's Incident Management provision. The SPARC's "to the extent permitted by law" qualifier — which is absent from the DPA — does not carry through to the governing obligation.

— Note —
The AI cited 1 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "SFDC maintains security incident management policies and procedures specified in the Security, Privacy and Architecture Documentation and shall notify Customer without undue delay after becoming aware…"

> *"Salesforce notifies impacted customers without undue delay of any unauthorized disclosure of their respective Customer Data by Salesforce or its agents of which Salesforce becomes aware to the extent permitted by law."*
> — Security, Privacy and Architecture Report

Termination Obligations

AI Comment: The playbook item requires the vendor to return or make available all Customer Data upon termination. Multiple provisions across the Slack document set collectively satisfy this requirement, and no document is silent on the topic.

Primary obligation — MSA § 2.2: The governing Agreement commits to making all Customer Data available for export or download upon customer request within 30 days of termination. This is the enforceable contractual baseline. After that 30-day window, Slack has no further contractual obligation to maintain or provide data and will proceed to delete it. This is the principal practical limitation: if the customer fails to request within 30 days, the right lapses. This condition is standard enterprise SaaS practice but must be tracked as a concrete offboarding action.

Supplementary obligation — DPA § 9: The Data Processing Addendum adds an independent, affirmative "shall return" obligation—stronger framing than the MSA's conditional "will make available upon request." The DPA defers to the SPARC for procedures and timeframes, so the 30-day request window governs the mechanism. Notably, compliance with the DPA continues until data is actually deleted or returned.

Procedural detail — SPARC "Return of Customer Data": As Documentation (subordinate to the MSA per § 12.3), the SPARC operationalizes the 30-day request window and directs customers to the Slack Help Center for export mechanics. The "may request" language describes the customer's option, not Slack's discretion.

Practical extension for standard deployments — SPARC "Deletion of Customer Data": For non-Enterprise Grid paid subscriptions—the segment most applicable to a standard US-domiciled team chat deployment—data is NOT deleted upon paid subscription termination. Instead, the workspace continues under the free tier until the customer actively initiates deletion. This substantially mitigates the 30-day MSA window risk: data remains accessible and exportable for an indefinitely extended period after termination for most customers.

Overall classification (Medium weight): The acceptable position ("return or make available all data upon termination") is met. Data IS made available through a documented, self-service export mechanism backed by contractual obligation. The 30-day request window and free-tier continuation for non-Enterprise Grid customers together provide a workable, if not unconditional, implementation. Minor note: system log artifacts (team names and search query strings embedded in web server access log URLs) are excluded from both deletion and return procedures, but these are server-side artifacts and not substantive Customer Data content.

Practical action item for legal team to flag in onboarding/offboarding checklist: Submit data export request promptly upon subscription termination, particularly for Enterprise Grid plans where deletion is initiated 90 days post-termination regardless of free-tier status.

> *"Upon request by Customer made within 30 days after the effective date of termination or expiration of this Agreement, SFDC will make Customer Data available to Customer for export or download as provided in the Documentation. After such 30-day period, SFDC will have no obligation to maintain or provide any Customer Data, and as provided in the Documentation will thereafter delete or destroy all copies of Customer Data in its systems or otherwise in its possession or control, unless legally prohibited."*
> — https://www.salesforce.com/en-us/wp-content/uploads/sites/4/documents/legal/salesforce_MSA.pdf
> *"SFDC shall return Customer Data to Customer and, to the extent allowed by applicable law, delete Customer Data in accordance with the procedures and timeframes specified in the Security, Privacy and Architecture Documentation. Until Customer Data is deleted or returned, SFDC shall continue to comply with this DPA and its Schedules."*
> — Data Processing Addendum
> *"Return of Customer Data"*
> — Security, Privacy and Architecture Report
> *"Deletion of Customer Data section below). Information about the export capabilities of the Covered Services can be found at theSlack Help Center."*

— Security, Privacy and Architecture Report

Compliance Monitoring

AI Comment: The playbook item requires the vendor to (1) review its compliance with the DPA and applicable data protection and privacy laws at least annually, and (2) adapt that compliance where necessary. The contract documents partially address this requirement through four related provisions, none of which explicitly commits to an annual review-and-adaptation cycle for DPA and data protection law compliance.

DPA §6.1 commits to "regularly" monitoring compliance with technical and organizational measures. "Regularly" is an unspecified frequency — it may satisfy "at least annual" in practice, but the contract does not guarantee this minimum cadence. The clause is also scoped to security-related TOM measures rather than encompassing the full range of DPA obligations and applicable data protection laws.

DPA §6.3 establishes a formal audit program directly covering DPA compliance obligations and applicable Data Protection Laws and Regulations — the substantive scope the playbook item contemplates. However, no review cycle is specified for vendor-initiated self-review, and the customer on-site audit right (§6.3.2–6.3.3) is limited to once per year at customer request — an indirect annual touchpoint, but customer-triggered rather than a vendor self-review obligation.

DPA §6.2 commits to maintaining ISO 27001 and SOC 2 certifications for the Agreement term. By the inherent nature of these standards, renewal requires annual third-party audits, creating an implicit periodic compliance review mechanism. However, this inference relies on external knowledge of certification standards not articulated in the contract, and the certifications are security-focused rather than a direct review of DPA obligations and adaptation to changes in applicable privacy law.

DPA §12.4 (Europe Specific Provisions) commits to notifying Customer promptly when new or changed local laws prevent DPA compliance and to recommending workarounds. This addresses adaptation to legal changes, but it is event-triggered and reactive — applicable only when SFDC "reasonably believes" a law creates a compliance obstacle — rather than a scheduled proactive annual review. Further, this provision is scoped to European third-country transfer restrictions and has limited direct applicability for a US-domiciled customer under California governing law, which is the most probable jurisdiction for this deployment.

Collectively, these provisions demonstrate an ongoing compliance monitoring infrastructure but fall short of the playbook's explicit "at least annual" review-and-adaptation cycle requirement. No provision commits SFDC to a defined annual frequency for reviewing DPA compliance or proactively adapting to changes in applicable data protection laws. Classification: YELLOW.

— Note —
The AI cited 3 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "SFDC shall maintain appropriate technical and organizational measures for protection of the security (including protection against unauthorized or unlawful Processing and against accidental or unlawfu…"
2. "SFDC shall maintain an audit program to help ensure compliance with the obligations set out in this DPA and shall make available to Customer information to demonstrate compliance with the obligations …"
3. "SFDC has obtained the third-party certifications and audits set forth in the Security, Privacy and Architecture Documentation for each applicable Service. Where SFDC has obtained ISO 27001 certificati…"

> *"As of the Effective Date, SFDC has no reason to believe that the laws and practices in any third country of destination applicable to its Processing of the Personal Data as set forth in the Infrastructure and Sub-processors Documentation, including any requirements to disclose Personal Data or measures authorizing access by a Public Authority, prevent SFDC from fulfilling its obligations under this DPA. If SFDC reasonably believes that any existing or future enacted or enforceable laws and practices in the third country of destination applicable to its Processing of the Personal Data ("Local Laws") prevent it from fulfilling its obligations under this DPA, it shall promptly notify Customer."*
> — Data Processing Addendum

Publicity

AI Comment: The Slack Supplemental Terms (Document 7) contain an explicit "Publicity" clause that directly conflicts with the acceptable position and the ideal preference for this playbook item.

The acceptable position requires that Customer must give consent before SFDC may use Customer's logo for marketing purposes. The ideal preference goes further: no use of name or logo without prior written consent, with the sole permitted exception being logo use necessary to provide the services.

The Supplemental Terms §Publicity grants SFDC a blanket, pre-agreed, ongoing license to use "Customer's company name and logo as a reference for marketing or promotional purposes on SFDC's websites and in other public or private communications with existing or potential Slack customers." By executing the Slack Terms, Customer has already granted this right — no per-use consent is required, and no prior written consent is required before any individual marketing use. The only constraint on SFDC's exercise of this right is compliance with "Customer's standard trademark usage guidelines as provided to SFDC from time-to-time," which controls the manner of use (e.g., brand presentation standards) but does not give Customer veto power over whether the name/logo is used for marketing at all.

This is a materially weaker position than both the acceptable threshold (consent before use) and the ideal preference (prior written consent). The clause actively grants the vendor the right Customer's playbook requires the Customer to withhold or condition. Because this is a High-weight item and the contract language explicitly and unambiguously conflicts with the acceptable position — rather than merely being silent — the classification is RED.

No other document in the set contains a competing or superseding publicity or logo-use clause. The MSA §6.2 grants a limited operational license (to host, copy, transmit, and display Customer Data to operate the Services) and §6.3 grants a feedback license; neither covers marketing or promotional use of Customer's name/logo and neither conflicts with or supersedes the Supplemental Terms §Publicity clause. The Supplemental Terms are contractually part of the "Slack Terms" and binding on Customer as a direct supplement to the MSA.

— Note —
The AI cited 2 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "Customer grants SFDC the right to use Customer's company name and logo as a reference for marketing or promotional purposes on SFDC's websites and in other public or private communications with existi…"
2. "Customer grants SFDC, its Affiliates and applicable contractors a worldwide, limited-term license to host, copy, use, transmit, and display any Non-SFDC Applications and program code created by or for…"

Cybersecurity Prevention Systems

AI Comment: The playbook item requires the vendor to have adequate systems and processes to prevent unauthorized access to or disclosure or loss of customer data. This requirement is addressed comprehensively and substantively across multiple authoritative layers of the Slack/Salesforce contract structure.

Contractual Obligations (MSA §2.2 and §8.2): The MSA is directly on point, committing SFDC to "appropriate administrative, physical, and technical safeguards" with language expressly including "measures designed to prevent unauthorized access to or disclosure of Customer Data." This is not a best-efforts commitment but an affirmative obligation. MSA §8.2 adds a warranty dimension: SFDC warrants that the Documentation accurately describes the applicable safeguards and that overall security will not be materially decreased during the subscription term. A warranty claim by the customer is a materially stronger right than a mere contractual promise.

Data Protection Obligations (DPA §6.1 and §6.2): DPA §6.1 maps precisely to the playbook item's three-part risk structure — it expressly covers protection against "unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Customer Data." The phrase "loss" is explicitly addressed, which the MSA §2.2 does not foreground. DPA §6.1 also establishes ongoing compliance monitoring and a no-material-decrease security commitment, further reinforcing the standard. DPA §6.2 commits to maintaining ISO 27001 certifications and SOC 2 reports for the duration of the agreement — providing durable, independently verified third-party assurance of security adequacy, not merely self-reported compliance.

Personnel Access Controls (DPA §4.1): Insider-threat and personnel-side unauthorized access are addressed: access to Personal Data is limited to those performing Services under the Agreement, all such personnel receive confidentiality training and execute written confidentiality agreements with post-termination survival obligations.

Technical Controls (SPARC): The Security, Privacy and Architecture Report — which is the "Documentation" contractually referenced in MSA §2.2 and DPA §6.1 as defining what controls exist — specifies concrete operational measures including: continuous monitoring for unauthorized intrusions by Salesforce or authorized external entities; 2FA for all server access across the production environment; industry-standard firewalls; automated vulnerability scanning with remediation; product security reviews including static analysis, peer code review, and a public bug bounty program; centralized security logging and analysis; and disaster recovery and backup procedures. The SPARC also commits to minimum alignment with ISO 27001, ISO 27002, and ISO 27018.

Notable Caveat (Privacy Policy): The Privacy Policy contains a standard industry disclaimer that Slack "cannot guarantee that Information during transmission through the Internet or while stored on our systems or otherwise in our care will be absolutely safe from intrusion by others." This is a factually accurate general statement about the nature of information security and does not create a contractual weakness. Under the User Terms' explicit document hierarchy (Contract prevails over Privacy Policy in any conflict), the MSA and DPA obligations govern. This caveat is flagged as a YELLOW PIF and superseded by the contractual provisions. It does not alter the overall GREEN classification.

Overall Assessment: The combination of (1) a binding contractual obligation expressly preventing unauthorized access/disclosure, (2) a security warranty with no-material-decrease commitment, (3) DPA-level technical and organizational measures covering the full scope of the playbook item's risks including loss, (4) a contractual commitment to maintain ISO 27001 and SOC 2 certifications for the agreement's duration, and (5) a detailed SPARC document describing concrete, industry-standard technical and operational controls collectively constitutes adequate systems and processes meeting the playbook item's requirement. Classification: GREEN, confidence HIGH.

— Superseding reasoning —
The Privacy Policy (PIF 9) contains a standard industry disclaimer that absolute security cannot be guaranteed. While factually accurate, this general consumer-facing caveat does not diminish the binding contractual security obligations in the MSA and DPA. The User Terms' Entire Agreement clause establishes an explicit order of precedence: "if there is a conflict or inconsistency between the Contract and the User Terms, the terms of the Contract will first prevail, followed by the

provisions in these User Terms, and then followed by the pages referenced in these User Terms (e.g., the Privacy Policy)." MSA §2.2 (PIF 0) and DPA §6.1 (PIF 2) are affirmative, specific security obligations that directly address the playbook item's risk categories (unauthorized access, disclosure, loss), and these govern the contractual relationship. The Privacy Policy caveat is therefore superseded for contractual purposes by the MSA and DPA obligations.

— Note —
The AI cited 4 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "SFDC warrants that during an applicable subscription term (a) this Agreement, the Order Forms and the Documentation will accurately describe the applicable administrative, physical, and technical safe…"
2. "SFDC shall maintain appropriate technical and organizational measures for protection of the security (including protection against unauthorized or unlawful Processing and against accidental or unlawfu…"
3. "SFDC has obtained the third-party certifications and audits set forth in the Security, Privacy and Architecture Documentation for each applicable Service. Where SFDC has obtained ISO 27001 certificati…"
4. "SFDC shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibiliti…"

> *"SFDC will maintain appropriate administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Customer Data, as described in the Documentation. Those safeguards will include, but will not be limited to, measures designed to prevent unauthorized access to or disclosure of Customer Data (other than by Customer or Users)."*
> — https://www.salesforce.com/en-us/wp-content/uploads/sites/4/documents/legal/salesforce_MSA.pdf
> *"Security Controls"*
> — Security, Privacy and Architecture Report
> *"Salesforce, or an authorized external entity, will monitor the Covered Services for unauthorized intrusions."*
> — Security, Privacy and Architecture Report
> *"At a minimum, Salesforce will align with prevailing*
> *industry standards such as ISO 27001, ISO 27002, and ISO 27018."*
> — Security, Privacy and Architecture Report
> *"Firewalls are configured according to industry best practices, using AWS security groups."*
> — Security, Privacy and Architecture Report
> *"Given the nature of communications and information processing technology, Slack cannot guarantee that Information during transmission through the Internet or while stored on our systems or otherwise in our care will be absolutely safe from intrusion by others."*
> — Privacy Policy | Legal | Slack

Regulatory Disclosure Procedure

AI Comment: The playbook's acceptable position requires three cumulative elements: (1) the vendor notifies Customer when contacted by a regulatory or legal authority; (2) this obligation is carved out if notification is legally prohibited; and (3) the vendor awaits Customer's instructions before acting on the request.

DPA §8.1 (Government Requests) robustly satisfies elements (1) and (2) for legally binding government access requests concerning Personal Data: SFDC must promptly notify Customer with a summary of the request, is excused only if legally prohibited, and must use commercially reasonable efforts to obtain a waiver of any notification prohibition. Additionally, SFDC independently commits to challenging unlawful requests, seeking interim measures, and providing the minimum amount of information permissible — protections that go beyond many market standard provisions. MSA §7.3 provides a parallel, if weaker, notification requirement for compelled disclosure of Confidential Information in general (not limited to Personal Data or government access contexts).

Element (3) — awaiting Customer's instructions — is the critical gap. Neither DPA §8.1 nor MSA §7.3 requires SFDC to pause and wait for Customer direction before acting. DPA §8.1 grants SFDC independent authority to assess lawfulness, challenge requests, and ultimately disclose once procedurally required — all without conditioning action on Customer instructions. This is a materially weaker protection than the acceptable position requires.

A secondary scope gap compounds the concern: DPA §8.1's notification obligation is expressly limited to "legally binding request[s] to access Personal Data from a Public Authority." Non-binding regulatory inquiries, administrative correspondence, and requests targeting data categories that Slack processes as a data controller (i.e., "Other Information" under the Privacy Policy — usage logs, IP addresses, device data) fall outside DPA §8.1's scope. The Privacy Policy confirms that Slack may independently disclose "Other Information" to regulators/law enforcement "if we reasonably believe disclosure is in accordance with or required by any applicable law, regulation or legal process" — with no Customer notification obligation for that category.

Classification: YELLOW. The DPA meaningfully addresses notification and the legal prohibition carve-out, but the absence of any "await instructions" mechanism and the narrower-than-needed scope constitute a materially weaker position than the playbook requires. Given the High weight assigned to this item, this gap requires documented assessment and likely negotiation of enhanced language in a negotiated Customer Agreement or order form addendum.

— Superseding reasoning —
DPA §8.1 supersedes MSA §7.3 for the specific scenario of legally binding government access requests for Personal Data, by application of the specific-over-general principle: DPA §8.1 was drafted expressly to govern government and public authority access to Personal Data and contains detailed obligations tailored to that scenario, while MSA §7.3 addresses compelled disclosure of Confidential Information generally (including in civil proceedings). MSA §7.3 continues to govern for compelled disclosures of Confidential Information that fall outside DPA §8.1's scope (e.g., civil subpoenas for non-Personal

Data confidential business information, trade secret matters). DPA Schedule 1 §2.11 reinforces DPA §8.1 for the EU/SCC context and is not a superseding relationship — it is an additive provision operating within the same framework. The Privacy Policy's Law Enforcement provision operates on a parallel, non-overlapping scope (Slack-controlled "Other Information"), so no superseding relationship applies there.

— Note —
The AI cited 1 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "The Receiving Party may disclose Confidential Information of the Disclosing Party to the extent compelled by law to do so, provided the Receiving Party gives the Disclosing Party prior notice of the c…"

> *"If SFDC receives a legally binding request to access Personal Data from a Public Authority, SFDC shall, unless otherwise legally prohibited, promptly notify Customer including a summary of the nature of the request. To the extent SFDC is prohibited by law from providing such notification, SFDC shall use commercially reasonable efforts to obtain a waiver of the prohibition to enable SFDC to communicate as much information as possible, without undue delay. Further, SFDC shall challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful. SFDC shall pursue appeals where available. When challenging a request, SFDC shall seek interim measures to suspend the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the Personal Data requested until required to do so under the applicable procedural rules. SFDC agrees it will provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request. SFDC shall promptly notify Customer if SFDC becomes aware of any direct access by a Public Authority to Personal Data and provide information available to SFDC in this respect, to the extent permitted by law."*
> — Data Processing Addendum
> *"For the purposes of clause 15(1)(a), SFDC shall notify Customer (only)*
> *and not the Data Subject(s) in case of government access requests. Customer shall be solely responsible for promptly notifying the Data Subject as necessary."*
> — Data Processing Addendum
> *"If we receive a request for information, we may disclose Other Information if we reasonably believe disclosure is in accordance with or required by any applicable law, regulation or legal process."*
> — Privacy Policy | Legal | Slack

Security Training

AI Comment: The playbook requires vendor employees who access data to attend security training at least annually. The document set is not wholly silent on this topic — the DPA (Section 4.1, Confidentiality, Reliability and Limitation of Access) is the most directly applicable provision, obligating SFDC to ensure that "personnel engaged in the Processing of Personal Data... have received appropriate training on their responsibilities." However, this provision falls short of the acceptable position in two material respects: (1) it does not characterize the required training as "security training" — it uses the broader phrase "training on their responsibilities"; and (2) it does not specify any minimum frequency, let alone the annual cadence the playbook requires. The MSA's general safeguards obligation (§ 2.2) is complementary but does not address employee training specifically, and is superseded for this item by the more specific DPA § 4.1 clause under the specific-over-general principle. The Security, Privacy and Architecture Report commits to alignment with ISO 27001, ISO 27002, and ISO 27018; ISO 27001 (Annex A.6.3 in the 2022 version) requires periodic security awareness training as a certification control, and this report is incorporated by reference into the contractual framework via the DPA. However, a commitment to "align with" an external standard is not equivalent to an explicit contractual guarantee of annual security training — the inference is indirect and MODERATE-confidence at best. Taken together, the vendor addresses the concept of personnel training for data-processing staff, but the absence of an explicit annual frequency and explicit "security" characterization represents a meaningful gap against the acceptable position. Classification: YELLOW. Weight: Medium.

— Superseding reasoning —
The DPA Section 4.1 is the most specific provision addressing personnel training obligations for employees who process Personal Data. The MSA Section 2.2 establishes only a general administrative/physical/technical safeguards framework and does not specifically address training. Under the specific-over-general principle, DPA § 4.1 controls for this playbook item. The two provisions do not conflict; DPA § 4.1 displaces the general MSA safeguards clause as the operative governing language on this topic.

— Note —
The AI cited 2 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "SFDC shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibiliti…"
2. "At a minimum, Salesforce will align with prevailing industry standards such as ISO 27001, ISO 27002, and ISO 27018."

> *"SFDC will maintain appropriate administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Customer Data, as described in the Documentation."*
> — https://www.salesforce.com/en-us/wp-content/uploads/sites/4/documents/legal/salesforce_MSA.pdf

Disaster Recovery Testing

AI Comment: The Security, Privacy and Architecture Report ("SPARC"), incorporated by reference into the MSA as "Documentation," is the primary source addressing this playbook item. The SPARC confirms: (1) that the operations team "tests disaster recovery measures regularly," and (2) that backup and restoration procedures are tested "at least every 90 days." The MSA §2.2 obligates SFDC to maintain safeguards "as described in the Documentation," and §8.2 warrants that the Documentation will "accurately describe" those safeguards — giving these SPARC statements contractual force rather than treating them as mere marketing representations.

The playbook's acceptable position requires unambiguous evidence of DR/BC plan testing at least once annually. Assessed against that standard, the finding is mixed:

• Backup testing component (SPARC): explicitly states "at least every 90 days" — this clearly exceeds the annual threshold for the backup sub-element.
• Full DR plan testing component (SPARC): described only as "regular" with no defined interval. "Regularly" is legally ambiguous — it does not contractually guarantee "at least annually" and could accommodate a cadence of every 18–24 months or longer without breaching the literal language.

The acceptable position requires a quantified commitment covering the full DR/BC program, not only backups. Because the critical frequency element for the broader DR testing program is vague while only the backup sub-component is explicitly quantified to an exceeding standard, the item is classified YELLOW. The topic is substantively addressed and testing clearly occurs, but the full DR plan testing cadence lacks the contractual specificity needed to satisfy the acceptable position with confidence. As a HIGH weight item, this finding requires documented review and assessment by the reviewing legal professional.

— Note —
The AI cited 1 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "SFDC warrants that during an applicable subscription term (a) this Agreement, the Order Forms and the Documentation will accurately describe the applicable administrative, physical, and technical safe…"

> *"Our operations team tests*
> *disaster recovery measures regularly and has a 24-hour on-call team to quickly resolve unexpected incidents."*
> — Security, Privacy and Architecture Report
> *"We have well-tested backup and restoration procedures which allow recovery from a major disaster. Customer Data and our source code are automatically backed up every night. The operations team is alerted in the event of a failure in this system. Backups are fully tested at least every 90 days to confirm that our processes and tools work as expected."*
> — Security, Privacy and Architecture Report
> *"SFDC will maintain appropriate administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Customer Data, as described in the Documentation."*
> — https://www.salesforce.com/en-us/wp-content/uploads/sites/4/documents/legal/salesforce_MSA.pdf

Data Subject Rights Assistance

AI Comment: The playbook requires two distinct obligations: (1) the vendor must first notify Customer when it receives a Data Subject Request (DSR), and (2) the vendor must promptly assist Customer in fulfilling that DSR. The Salesforce/Slack Data Processing Addendum (Revision April 2026, Doc ID: rztql8356vi4ymqu0aokqwuv), which is incorporated by reference into the governing MSA (Doc ID: mjamzpskvqbntyittdey1ue3, §2.2), addresses both requirements across three dedicated provisions.

NOTIFICATION REQUIREMENT: §3.1 (Data Subject Request) explicitly requires SFDC to "promptly notify Customer" of any DSR it receives — the very language the playbook calls for. It further confirms SFDC will not independently respond to or resolve DSRs, instead redirecting them to Customer. This directly satisfies the "first notify us" element of the acceptable position. The qualifier "to the extent legally permitted" is standard and necessary for situations involving legally-mandated gag orders (e.g., certain law enforcement requests) and does not practically impair routine DSRs from individuals exercising GDPR/CCPA rights.

ASSISTANCE REQUIREMENT: §3.2 (Required Assistance) imposes a base-level assistance obligation using "appropriate technical and organizational measures, insofar as this is possible" — the standard GDPR Article 28(3)(e) processor obligation language. This meets the spirit of "assist us in fulfilling" DSRs. §3.3 (Additional Assistance) provides a supplementary tier: upon Customer's explicit request, SFDC will use "commercially reasonable efforts" to assist in cases where Customer lacks direct ability to respond. §3.3 is individually YELLOW in isolation (requires Customer's request, commercially reasonable efforts standard rather than unqualified obligation, and shifts costs to Customer), but it supplements rather than replaces the base §3.2 obligation.

QUALIFIERS ASSESSED: The qualifiers present throughout ("to the extent legally permitted," "insofar as this is possible," "commercially reasonable efforts," cost-shifting in §3.3) are industry-standard for cloud processor DPAs under GDPR/CCPA and do not materially undermine the core notification and base-assistance obligations. Under the most probable governing law (California + controlling US federal law for a US-domiciled Customer), these obligations are enforceable and are consistent with — and in several respects exceed — CCPA service provider requirements (Cal. Civ. Code §1798.100 et seq.).

EXECUTION NOTE: The DPA document itself states (§14 / "Legal Effect") that it becomes independently binding only upon

separate Customer execution. However, the MSA (§2.2) incorporates the DPA by reference, providing a contractual foundation regardless. Practitioners should confirm the DPA has been separately executed to ensure standalone enforceability as a DPA instrument. This is a process/compliance matter rather than a language deficiency in the vendor's terms.

OVERALL: Both elements of the acceptable position — notify first, then assist — are explicitly and substantively addressed. Classification: GREEN.

— Note —
The AI cited 4 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "SFDC shall, to the extent legally permitted, promptly notify Customer of any complaint, dispute or request it has received from a Data Subject such as a Data Subject's right of access, right to rectif…"
2. "Taking into account the nature of the Processing, SFDC shall assist Customer by appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of Customer's obliga…"
3. "To the extent Customer, in its use of the Services, does not have the ability to address a Data Subject Request, SFDC shall upon Customer's request provide commercially reasonable efforts to assist Cu…"
4. "The terms of the data processing addendum at https://www.salesforce.com/company/legal/agreements/ ("DPA") posted as of the Effective Date are hereby incorporated by reference."

Our liability

AI Comment: The acceptable position requires the vendor's (and/or the Customer organization's) aggregate liability to be capped at the amount paid. The governing commercial terms for the Customer entity — the Salesforce MSA incorporated by reference into the Slack Terms — satisfy this standard directly. MSA §10.1 caps each party's aggregate liability at "the total amount paid by Customer and its Affiliates hereunder for the Services giving rise to the liability in the twelve months preceding the first incident." This is a mutual, amount-paid cap that covers both Slack's liability to the Customer and the Customer's liability to Slack. The standard 12-month lookback is widely accepted market practice and does not materially diminish the protection relative to a total-fees-paid formulation. MSA §10.2 reinforces the cap with a broad consequential/indirect/punitive damages exclusion, subject to a statutory override carve-out. The DPA (§11) expressly defers all DPA-related liability to the MSA's Limitation of Liability section, so even data breach claims are governed by the same amount-paid cap. A separate $100 flat aggregate cap appears in the User Terms of Service, applying to Slack's liability to individual Authorized Users — a different contractual relationship. Because it falls below the "amount paid" standard and governs users rather than the Customer entity, it is marked YELLOW and superseded for purposes of this item. Additionally, MSA §2.7 disclaims virtually all liability for Free Services tiers (capped at $1,000 if exclusion is unenforceable), which would not satisfy "limited to amount paid" for a free-tier Customer — noted as a conditional YELLOW caveat. For the standard paid SAAS deployment described in the intake brief, the MSA §10.1 amount-paid cap governs and fully satisfies the playbook's acceptable position. Weight is Acceptable to Deviate; alignment with no residual risk for a paid subscription.

— Superseding reasoning —
MSA §10.1 (PIF index 0) is the operative provision for the Customer entity's aggregate liability analysis and supersedes the User Terms §Limitation of Liability (PIF index 3) for that purpose. The User Terms govern Slack's liability to individual Authorized Users, not the Customer entity's commercial relationship. The User Terms' own hierarchy clause (§Entire Agreement) explicitly confirms: "if there is a conflict or inconsistency between the Contract and the User Terms, the terms of the Contract will first prevail." The MSA is the Contract; it prevails. The MSA's 12-month amount-paid cap — not the User Terms' flat $100 cap — is therefore what governs for purposes of this playbook item.

— Note —
The AI cited 4 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "IN NO EVENT SHALL THE AGGREGATE LIABILITY OF EACH PARTY TOGETHER WITH ALL OF ITS AFFILIATES ARISING OUT OF OR RELATED TO THIS AGREEMENT EXCEED THE TOTAL AMOUNT PAID BY CUSTOMER AND ITS AFFILIATES HERE…"
2. "IN NO EVENT WILL EITHER PARTY OR ITS AFFILIATES HAVE ANY LIABILITY ARISING OUT OF OR RELATED TO THIS AGREEMENT FOR ANY LOST PROFITS, REVENUES, GOODWILL, OR INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL…"
3. "Each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, and all DPAs between Authorized Affiliates and SFDC, whether in contract, tor…"
4. "NOTWITHSTANDING THE "REPRESENTATIONS, WARRANTIES, EXCLUSIVE REMEDIES AND DISCLAIMERS" SECTION AND "INDEMNIFICATION BY SFDC" SECTION BELOW, THE FREE SERVICES ARE PROVIDED "AS-IS" WITHOUT ANY WARRANTY A…"

> *"OUR MAXIMUM AGGREGATE LIABILITY TO YOU FOR ANY BREACH OF THE USER TERMS IS ONE HUNDRED DOLLARS ($100) IN THE AGGREGATE."*
> — User Terms of Service | Legal | Slack

Data Retention & Deletion

AI Comment: The vendor's terms across four documents — the Security, Privacy and Architecture Report (SPARC), the DPA, the MSA, and the Privacy Policy — extensively and specifically address data retention and deletion practices. The governing deletion timelines are established in the SPARC, which the DPA (§ 9) explicitly designates as the authoritative source for deletion "procedures and timeframes." The DPA, in turn, is incorporated into the Agreement per MSA § 2.2.

AGAINST THE ACCEPTABLE POSITION (production deletion within 30 days of request; backup purge within 364 days):

(1) Production deletion timeline: The SPARC specifies hard deletion from production systems within 24 hours of workspace Primary Owner-initiated deletion — more than 30× faster than the 30-day acceptable threshold. For granular message and file deletion, customer-configurable retention policies result in nightly deletion from production servers, also comfortably within threshold.

(2) Backup purge timeline: The SPARC specifies backup destruction within 14 days — approximately 26× faster than the 364-day acceptable threshold. A minor operational caveat allows temporary extension during an ongoing incident investigation; this is a standard and reasonable carve-out that does not materially undermine compliance.

AGAINST THE IDEAL PREFERENCE (production deletion within 10 days): The 24-hour Primary Owner-initiated deletion and the nightly retention-policy-based deletion both exceed the 10-day ideal preference. aiPreferenceMet is set to true accordingly.

NOTABLE QUALIFICATIONS (not sufficient to downgrade from GREEN):
(a) The 24-hour rule applies specifically to workspace-level Primary Owner-initiated deletion. Granular data deletion is handled through customer-configurable retention policies on a nightly cycle — both mechanisms honour the playbook thresholds.
(b) For non-Enterprise Grid paid subscriptions, when a customer cancels without actively requesting deletion, data persists under the free tier rather than being auto-deleted. However, the customer retains the right to request deletion at any time — processed within 24 hours for workspace self-deletion or within 14 days for elected account deletion — fully satisfying the on-request deletion standard.
(c) Both production and backup deletion exclude "team names and search terms embedded in URLs in web server access logs" — a narrow, operationally standard exclusion.
(d) The "to the extent allowed by applicable law" qualifier in DPA § 9 is standard and does not undermine the deletion framework for typical commercial deployments.

SUPERSEDING: The DPA § 9 (Agreement-level) supersedes the MSA § 2.2's general post-termination deletion language by being the specific data processing addendum and by explicitly establishing the SPARC as the governing source for deletion procedures and timeframes. The SPARC's operational timelines (24-hour production, 14-day backup) are the controlling deletion standards.

CLASSIFICATION: GREEN. The vendor clearly meets and substantially exceeds the acceptable position on both the production deletion and backup purge dimensions. The ideal preference is also met.

— Superseding reasoning —
The DPA (§ 9 Return and Deletion of Customer Data), incorporated into the Agreement per MSA § 2.2, is the specific data processing addendum governing deletion procedures for Customer Data. It supersedes the MSA § 2.2's general post-termination deletion clause by addressing data deletion in a data-processing-specific context, and critically, by explicitly establishing the Security, Privacy and Architecture Documentation (SPARC) as the governing source for deletion "procedures and timeframes." The SPARC's operational timelines — 24 hours for production systems, 14 days for backups — are therefore the controlling deletion standards, with Agreement-level contractual force through their incorporation via the DPA.

— Note —
The AI cited 1 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "Owners of paid Slack teams can configure custom message retention policies on a team-wide and per-channel basis. Setting a custom duration for retention means that messages or files older than the dur…"

> *"Within 24 hours of workspace Primary Owner-initiated deletion, Salesforce hard deletes all information from currently running production systems (excluding team names and search terms embedded in URLs in web server access logs). Covered Services backups are destroyed within 14 days (backups are destroyed within 14 days, except that during an on-going investigation of an incident such period may be temporarily extended)."*
> — Security, Privacy and Architecture Report
> *"Deletion of Customer Data section below). Information about the export capabilities of the Covered Services can be found at theSlack Help Center."*
> — Security, Privacy and Architecture Report
> *"Deletion of Customer Data section below). Information about the export capabilities of the Covered Services can be found at theSlack Help Center."*
> — Security, Privacy and Architecture Report
> *"Data Retention](https://slack.com/trust/privacy/privacy-policy#retention)"*
> — Privacy Policy | Legal | Slack
> *"SFDC shall return Customer Data to Customer and, to the extent allowed by applicable law, delete Customer Data in accordance with the procedures and timeframes specified in the Security, Privacy and Architecture Documentation. Until*

> *Customer Data is deleted or returned, SFDC shall continue to comply with this DPA and its Schedules."*
> — Data Processing Addendum
> *"Upon request by Customer made within 30 days after the effective date of termination or expiration of this Agreement, SFDC will make Customer Data available to Customer for export or download as provided in the Documentation. After such 30-day period, SFDC will have no obligation to maintain or provide any Customer Data, and as provided in the Documentation will thereafter delete or destroy all copies of Customer Data in its systems or otherwise in its possession or control, unless legally prohibited."*
> — https://www.salesforce.com/en-us/wp-content/uploads/sites/4/documents/legal/salesforce_MSA.pdf

Vendor Audit Rights

AI Comment: The playbook item requires that Customer hold the right to audit Vendor's systems and compliance with the DPA. The Salesforce/Slack DPA (Document 6, §§6.3.1–6.3.4) does provide audit mechanisms, but they are materially conditional and constrained in ways that fall short of an unconditional, broad audit right.

What is provided:
1. **Certification-first channel (§6.3.1):** Upon written request at reasonable intervals, SFDC will make available copies of its most recent third-party audit reports/certifications (e.g., ISO 27001, SOC 2) and sub-processor audit reports. This is an unconditional right to audit *evidence*, but not a right to conduct Customer-directed audits.
2. **Conditional on-site audit right (§6.3.2):** A Customer-directed on-site audit is only available if one of three enumerated triggers is satisfied: (i) certification information is insufficient to demonstrate compliance; (ii) a Customer Data Incident notice has been issued; or (iii) required by Data Protection Laws or a supervisory authority.
3. **Frequency and notice restrictions (§6.3.3):** On-site audits are limited to once per year, require at least three weeks' advance written notice, and must be conducted during normal business hours without unreasonably interfering with SFDC operations.
4. **Scope controlled jointly (§6.3.3):** Scope, timing, and duration must be mutually agreed. Critically, SFDC retains the right to adapt scope unilaterally "to avoid or mitigate risks with respect to...service levels, availability, and confidentiality of other SFDC customers' information" — giving SFDC significant de facto scope veto.
5. **Third-party auditor restrictions (§6.3.4):** Any third-party auditor engaged by Customer must (a) not be a competitor of SFDC, (b) execute a protective NDA, and (c) have its costs borne by Customer.

Gap Analysis vs. Acceptable Position:
The playbook requires a right to audit Vendor's systems and compliance with the DPA. The DPA provides a certification-first model where Customer's access to direct (on-site) audit is conditional on specific triggering events — most significantly, that SFDC's own certification reports are "not sufficient to demonstrate compliance." Given that SFDC maintains ISO 27001 and SOC 2 certifications (confirmed in §6.2 and the Security Report, Document 9), SFDC would typically argue trigger (i) is not met, making direct on-site audits practically difficult to invoke on a routine basis. The mutual scope agreement and SFDC's right to adapt scope further limit Customer's ability to direct the audit. The once-per-year limitation, three-week notice requirement, and Customer-borne costs add further friction.

These restrictions collectively mean the audit right is real but substantially weakened relative to an unconditional DPA audit right. Classification is YELLOW: the topic is addressed, but the protections are weaker and more conditional than the playbook's acceptable position implies. This is a High-weight item, requiring documented review and assessment.

Note on DPA execution: The Slack DPA landing page (Document 5) instructs that an authorized individual must separately execute the DPA. Document 6 bears SFDC pre-signatures (April 2026) and includes Slack Technologies, LLC and Slack Technologies Limited as named SFDC entities. Customer must confirm its own execution is on file; absent Customer signature, these audit rights are not yet legally binding.

— Note —
The AI cited 5 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "Upon Customer's written request at reasonable intervals, and subject to the confidentiality obligations set forth in the Agreement, SFDC shall:

(i) the make available to Customer (or Customer's Third…"
2. "Customer can request an on-site audit of SFDC's Processing activities covered by this DPA ("On-Site Audit"). An On-Site Audit may be conducted by Customer either itself or through a Third-Party Audito…"
3. "An On-Site Audit shall be conducted by Customer or its Third-Party Auditor:
(i) acting reasonably, in good faith, and in a proportional manner, taking into account the nature and complexity of the Ser…"
4. "A Third-Party Auditor means a third-party independent contractor that is not a competitor of SFDC. An On-Site Audit can be conducted through a Third Party Auditor if:
(i) prior to the On-Site Audit, t…"
5. "SFDC has obtained the third-party certifications and audits set forth in the Security, Privacy and Architecture Documentation for each applicable Service. Where SFDC has obtained ISO 27001 certificati…"

User Authentication Policies

AI Comment: The playbook item requires that the vendor have policies for both (1) user authentication and (2) password protection. The documents address the first element substantively and the second element only implicitly.

Authentication policies — GREEN quality. The Security, Privacy and Architecture Report (SPARC) is the operative source. It documents four concrete authentication controls: (a) administrator-enforceable two-factor authentication for all end users (Team-wide 2FA); (b) mandatory 2FA for all internal production server access; (c) detailed per-sign-in access logging capturing device type and IP address, accessible to both users and paid-tier administrators; and (d) administrator-triggered remote session termination across all authenticated devices. The MSA (§ 2.2) and DPA (§ 6.1) create binding contractual obligations to maintain these safeguards, with the MSA explicitly cross-referencing the Documentation (the SPARC) as the operative description of those safeguards. This authentication posture — 2FA capability, access logging, and active session management — is substantive and well-documented.

Password protection — inferential only. No document explicitly articulates password-specific controls: complexity requirements, minimum length, rotation periods, lockout thresholds, or storage/hashing standards are absent from all provided materials. The SPARC states that Salesforce will "at a minimum" align with ISO 27001, ISO 27002, and ISO 27018 — standards that formally require password management controls (ISO 27002 § 8.5 Secure authentication; § 5.17 Authentication information). This alignment claim provides a reasonable inference that password policies exist internally, and the Privacy Policy's reference to "internationally recognized security certifications" reinforces that Slack holds active certifications (not merely aspirational alignment). However, under the Functional Equivalence Standard, the inferential ISO-alignment path does not achieve the "same legal protection and enforceability" as an explicit contractual commitment to defined password standards. It is a weaker form of protection — YELLOW, not GREEN.

Overall classification: YELLOW. The playbook item is conjunctive — both authentication AND password protection must be addressed. The authentication element is clearly met; the password protection element is addressed only by reference to standards compliance, without explicit enumeration of policy controls. For a High-weight item, this gap warrants documented assessment. Recommended remediation: request Slack's ISO 27001 Statement of Applicability and/or a vendor questionnaire response confirming specific password controls in scope.

— Superseding reasoning —
The SPARC (Security, Privacy and Architecture Report) is the Documentation referenced in MSA § 2.2 and DPA § 6.1 as the operative description of Salesforce/Slack's security safeguards. The SPARC's specific authentication controls (2FA, access logging, session management) therefore supersede the Privacy Policy's general security overview statement on the topic of authentication policies: the specific and technically detailed Documentation governs over the high-level consumer-facing privacy policy summary. This is a SPECIFIC_OVER_GENERAL determination — the SPARC sets out the actual controls; the Privacy Policy security section is merely a general overview that points toward the same controls without specifying them.

— Note —
The AI cited 1 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "SFDC shall maintain appropriate technical and organizational measures for protection of the security (including protection against unauthorized or unlawful Processing and against accidental or unlawfu…"

> *"Team-wide Two-factor Authentication: Team Administratorscan require all users to set up two-factor authentication on their accounts."*
> — Security, Privacy and Architecture Report
> *"%Ï Network Protection:In addition to sophisticated systemmonitoring and logging, we have implemented two-factor authentication for all server access across our production environment."*
> — Security, Privacy and Architecture Report
> *"%Ï Access Logging: Detailed access logs are availableboth to users and administrators of paid teams. We log every time an account signs in, noting the type of device used and the IP address of the connection. Team Administrators and owners of paid teams can review consolidated access logs for their whole team."*
> — Security, Privacy and Architecture Report
> *"%Ï Access Management: Administrators can remotely terminateall connections and sign out all devices authenticated to the Covered Services at any time, on demand."*
> — Security, Privacy and Architecture Report
> *"At a minimum, Salesforce will align with prevailing industry standards such as ISO 27001, ISO 27002, and ISO 27018."*
> — Security, Privacy and Architecture Report
> *"Slack takes security of data very seriously. Slack works hard to protect Information you provide from loss, misuse, and unauthorized access or disclosure. These steps take into account the sensitivity of the Information we collect, process and store, and the current state of technology. Slack has received internationally recognized security certifications."*
> — Privacy Policy | Legal | Slack
> *"SFDC will maintain appropriate administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Customer Data, as described in the Documentation. Those safeguards will include, but will not be limited to, measures designed to prevent unauthorized access to or disclosure of Customer Data (other than by Customer or Users)."*
> — https://www.salesforce.com/en-us/wp-content/uploads/sites/4/documents/legal/salesforce_MSA.pdf

Employee Confidentiality Agreements

AI Comment: The playbook requires that vendor employees who access data have executed written confidentiality agreements. This requirement is directly and explicitly satisfied by DPA Section 4.1, which mandates that SFDC "shall ensure that its personnel engaged in the Processing of Personal Data... have executed written confidentiality agreements" — language that precisely tracks the acceptable position. Critically, the DPA additionally requires that these obligations survive the termination of employment and that access to Personal Data is limited to personnel performing Services in accordance with the Agreement, providing durable and layered protection beyond the bare minimum.

The MSA Section 7.2 provides complementary contractual reinforcement at the broader Confidential Information level, requiring employees and contractors who access Confidential Information (which expressly includes Customer Data under MSA § 7.1) to have "signed confidentiality agreements... containing protections not materially less protective of the Confidential Information than those herein." This operates as a parallel, reinforcing obligation.

The AUP and Security, Privacy and Architecture Report both reference strict employee access controls and access logging, which supports the operational picture but neither on its own satisfies the written confidentiality agreement requirement — they are contextual supporting evidence, not the operative contractual commitments.

The DPA Section 4.1 is the governing provision for this item (SPECIFIC_OVER_GENERAL relative to MSA § 7.2): the DPA is the operative instrument for all data processing personnel obligations, specifically scoped to "personnel engaged in the Processing of Personal Data." Both the DPA and MSA support a GREEN classification. Overall confidence is HIGH — the operative contractual language is unambiguous, exact, and directly on point.

— Superseding reasoning —
DPA Section 4.1 governs over MSA Section 7.2 for this specific playbook item on the basis of SPECIFIC_OVER_GENERAL: the DPA is the operative instrument for all data processing personnel obligations, addressing specifically "personnel engaged in the Processing of Personal Data." MSA Section 7.2 addresses the same topic more broadly across all Confidential Information and all employees/contractors. Both provisions support a GREEN classification — the superseding determination clarifies which provision controls, without altering the outcome.

— Note —
The AI cited 2 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "SFDC shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibiliti…"
2. "limit access to Confidential Information of the Disclosing Party to those of its and its Affiliates' employees and contractors who need that access for purposes consistent with this Agreement and who …"

> *"We place strict controls over employee access to Customer Data. There are technical controls and audit policies in place to ensure that access to Customer Data is logged."*
> — Acceptable Use Policy | Legal | Slack
> *"We place strict controls over employee access to Customer Data. There are technical controls and audit policies in place to ensure that access to Customer Data is logged."*
> — Security, Privacy and Architecture Report

Employee Access Control

AI Comment: The playbook requires the vendor to grant system access only to authorized personnel, on a need-to-know basis, strictly limited to what is required to fulfill their function.

The document set satisfies this requirement, with the DPA Section 4.1 providing the most specific and directly binding control.

Primary governing provision — DPA § 4.1: SFDC's access to Personal Data is explicitly limited to "those personnel performing Services in accordance with the Agreement." This is functionally equivalent to a need-to-know / least-privilege access model: access is scoped to those who require it to perform their defined function, not granted more broadly. The same provision mandates (i) that all personnel handling Personal Data receive confidentiality training and execute written confidentiality agreements, (ii) that those confidentiality obligations survive termination of employment, and (iii) that commercially reasonable steps are taken to ensure personnel reliability. This exceeds the basic acceptable position by also requiring affirmative confidentiality commitments and post-engagement obligations.

Supporting framework — MSA § 2.2: The master agreement establishes the overarching obligation to maintain "appropriate administrative, physical, and technical safeguards" including measures specifically designed to prevent unauthorized access to or disclosure of Customer Data. The MSA incorporates the DPA by reference (MSA § 2.2), so the two operate in tandem.

Operational confirmation — SPARC and AUP page: Both the Security, Privacy and Architecture Report (formally referenced in the MSA and DPA as the Security, Privacy and Architecture Documentation) and the Acceptable Use Policy page explicitly confirm "strict controls over employee access to Customer Data" backed by "technical controls and audit policies in place to ensure that access to Customer Data is logged." This confirms that the contractual obligation is operationally implemented with technical enforcement and an audit trail.

Supplementary context — Privacy Principles: Slack's Privacy Principles confirm that technical measures affirmatively prevent employee access to Customer Data content during AI/ML model development, providing additional evidence of

enforced access segregation beyond policy statements.

Scope note: The DPA § 4.1 is scoped to Personal Data within Customer Data. For a standard US-domiciled team chat deployment (Slack used for employee communications), virtually all Customer Data processed will constitute Personal Data. The SPARC and MSA § 2.2 language covers all Customer Data broadly, ensuring comprehensive coverage.

Overall assessment: The contract documents collectively meet the acceptable position. Access is restricted to personnel performing defined Services (need-to-know equivalent), confidentiality obligations are technically enforced and contractually binding, and access is logged and audited. Classification: GREEN. Preference field set to false — no ideal preference was specified against which to evaluate a higher threshold.

No preference specified: `aiPreferenceMet` is false because no ideal preference was stated in the playbook item; this is a GREEN-acceptable, not GREEN-ideal, determination.

— Superseding reasoning —
DPA § 4.1 (PIF index 0) supersedes the general MSA § 2.2 safeguards language (PIF index 1) on the specific question of how personnel access to Personal Data is controlled. The MSA § 2.2 is the general administrative/technical safeguards obligation; the DPA § 4.1 is the specific, granular personnel-access-control provision that directly addresses authorized access, training, confidentiality agreements, and access limitation scope. Per the specific-over-general principle, the DPA provision governs on this precise topic. Notably, the MSA § 2.2 itself incorporates the DPA by reference ("The terms of the data processing addendum… are hereby incorporated by reference"), establishing the DPA as the operative instrument for data processing and protection obligations. No conflict exists between these provisions — they are complementary, with the DPA providing the operative detail.

— Note —
The AI cited 1 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "SFDC shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibiliti…"

> *"SFDC will maintain appropriate administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Customer Data, as described in the Documentation. Those safeguards will include, but will not be limited to, measures designed to prevent unauthorized access to or disclosure of Customer Data (other than by Customer or Users)."*
> — https://www.salesforce.com/en-us/wp-content/uploads/sites/4/documents/legal/salesforce_MSA.pdf
> *"We place strict controls over employee access to Customer Data. There are technical controls and audit policies in place to ensure that access to Customer Data is logged."*
> — Acceptable Use Policy | Legal | Slack
> *"We place strict controls over employee access to Customer Data. There are technical controls and audit policies in place to ensure that access to Customer Data is logged."*
> — Security, Privacy and Architecture Report
> *"We have technical controls in place to prevent access.** When developing AI/ML models or otherwise analyzing Customer Data, Slack employees can’t access the underlying content. We have various technical measures preventing this from occurring. Please visit [Security at Slack](https://slack.com/resources/why-use-slack/security-at-slack) for more information on these controls that protect the confidentiality and security of Customer Data."*
> — Slack Privacy Principles

Employee Offboarding Access

AI Comment: The playbook item requires the vendor to have both policies and systems in place to promptly offboard employee access or change access rights on job function change — with a hard outer limit of 24 hours after termination or job change. Analysis across all documents reveals partial but insufficient coverage.

What the documents establish: (1) The DPA (§ 4.1) contractually commits SFDC to limiting Personal Data access to personnel actively performing Services and requires confidentiality obligations to survive termination of employment. (2) The MSA (§ 2.2) imposes a general obligation to maintain administrative, physical, and technical safeguards preventing unauthorized access to Customer Data. (3) The Security Report and AUP each assert that "strict controls over employee access to Customer Data" exist, backed by technical controls and access logging.

What is absent: None of these provisions specify any timeframe — 24 hours or otherwise — for revoking or adjusting employee access rights upon termination or job function change. The DPA's language that access is "limited to those personnel performing Services" establishes a correctness principle but does not create a binding obligation to act within any particular window. The Security Report and AUP describe controls as a general state without defining SLA or SLO commitments for access removal.

The gap relative to the acceptable position is therefore narrowly specific: the existence of access control policies and systems is confirmed (meeting the "policies and systems" half of the requirement), but the binding commitment to prompt ("d24 hour) offboarding is entirely absent. This is a YELLOW finding — the topic is addressed at a weaker level of protection than the playbook requires. For a High-weight item, this requires review and documented assessment before acceptance.

— Note —
The AI cited 1 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "SFDC shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature

of the Personal Data, have received appropriate training on their responsibiliti…"

> *"SFDC will maintain appropriate administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Customer Data, as described in the Documentation. Those safeguards will include, but will not be limited to, measures designed to prevent unauthorized access to or disclosure of Customer Data (other than by Customer or Users)."*
> — https://www.salesforce.com/en-us/wp-content/uploads/sites/4/documents/legal/salesforce_MSA.pdf
> *"We place strict controls over employee access to Customer Data. There are technical controls and audit policies in place to ensure that access to Customer Data is logged."*
> — Security, Privacy and Architecture Report
> *"We place strict controls over employee access to Customer Data. There are technical controls and audit policies in place to ensure that access to Customer Data is logged."*
> — Acceptable Use Policy | Legal | Slack

Confidentiality

AI Comment: The Salesforce MSA (which governs Slack under the Slack Terms, comprised of the MSA plus Slack Supplemental Terms) contains a comprehensive mutual confidentiality clause in § 7 that fully satisfies the acceptable position of this playbook item.

The acceptable position has three prongs — all are met:

(1) CUSTOMER CAN SHARE CI WITH SUBCONTRACTORS ON NEED-TO-KNOW BASIS: MSA § 7.2 expressly permits each Receiving Party (including Customer) to share CI with "its and its Affiliates' employees and contractors who need that access for purposes consistent with this Agreement," provided those parties have signed confidentiality agreements with protections no less protective than the MSA. Customer can therefore share CI (including its own sensitive information) with its subcontractors and subprocessors on a need-to-know basis.

(2) VENDOR MUST NOT DISCLOSE CI TO THIRD PARTIES UNLESS NEED-TO-KNOW FOR SERVICES: SFDC's third-party disclosure rights are expressly limited in § 7.2 to: (a) Affiliates, legal counsel, and accountants — with SFDC maintaining responsibility for their compliance — and (b) contractors and Non-SFDC Application Providers only "to the extent necessary to perform SFDC's obligations under this Agreement," subject to equivalent confidentiality protections. Both categories are tethered to a need-to-know-for-services rationale, satisfying the acceptable position.

(3) STANDARD CARVE-OUTS PRESENT: All four required exclusions from the definition of CI are explicit in § 7.1: (i) publicly known without breach; (ii) previously known to the Receiving Party without breach; (iii) received from a third party without knowledge of breach; (iv) independently developed. A compelled-disclosure provision with prior notice obligation (§ 7.3) is also included. The DPA supplements these protections for the subset of CI that constitutes Personal Data: SFDC must treat Personal Data as CI (§ 2.2), personnel must execute written confidentiality agreements (§ 4.1), and sub-processors must operate under data protection obligations no less protective than the Agreement (§ 5.1).

IDEAL PREFERENCE NOT MET: The ideal preference — mutual confidentiality with Vendor unable to share any CI at all — is not met. While the obligations are symmetric and mutual, the MSA explicitly preserves SFDC's right to share CI with its Affiliates, legal counsel, accountants, and contractors/Non-SFDC Application Providers. These exceptions are subject to adequate confidentiality protections and are consistent with the acceptable position's need-to-know standard, but they foreclose the absolute "will not share any of it" restriction the ideal preference contemplates.

Care standard note: SFDC's obligation is "the same degree of care that it uses to protect the confidentiality of its own confidential information of like kind (but not less than reasonable care)" — market-standard for enterprise SaaS. Classification: GREEN; aiPreferenceMet = false.

— Note —
The AI cited 7 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. ""Confidential Information" means all information disclosed by a party ("Disclosing Party") to the other party ("Receiving Party"), whether orally or in writing, that is designated as confidential or t…"
2. "Disclosing Party for any purpose outside the scope of this Agreement and (ii) except as otherwise authorized by the Disclosing Party in writing, limit access to Confidential Information of the Disclos…"
3. "Neither party will disclose the terms of this Agreement or any Order Form to any third party other than its Affiliates, legal counsel and accountants without the other party's prior written consent, p…"
4. "The Receiving Party may disclose Confidential Information of the Disclosing Party to the extent compelled by law to do so, provided the Receiving Party gives the Disclosing Party prior notice of the c…"
5. "SFDC shall treat Personal Data as Confidential Information and shall Process Personal Data on behalf of and only in accordance with Customer's documented instructions for the following purposes: (i) P…"
6. "SFDC shall ensure that its personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibiliti…"
7. "Customer acknowledges and agrees that (a) SFDC's Affiliates may be retained as Sub-processors; and (b) SFDC and SFDC's Affiliates respectively may engage third-party Sub-processors to provide the Serv…"

Physical Security Controls

AI Comment: The playbook item requires that the vendor has system controls and policies to prevent unauthorized physical access. The document set satisfies this requirement at the contractual level with explicit language, reinforced by third-party certification commitments and operational documentation — though with a notable gap in granular enumeration of specific physical access controls in the Security, Privacy and Architecture Report (SPARC).

Contractual foundation (strong): Both the Salesforce Main Services Agreement (MSA §2.2) and the DPA (Schedule 2 §11) contain identical explicit language committing SFDC to maintaining "administrative, physical, and technical safeguards" for protection of Customer Data. The MSA further specifies that these safeguards "will include, but will not be limited to, measures designed to prevent unauthorized access to or disclosure of Customer Data." The word "physical" appears expressly, directly addressing the acceptable position.

Certification commitment (strong): DPA §6.2 commits SFDC to maintaining ISO 27001 certifications and SSAE 18 SOC 2 reports "for the duration of the Agreement." ISO 27001 (and its predecessor/successor domains A.11 and A.7) explicitly mandates physical and environmental security controls — including secure area access controls, physical entry restrictions, equipment protection, and visitor management. SOC 2 evaluates physical security under its Common Criteria. A contractual commitment to maintain these certifications functions as a commitment to the physical control requirements embedded within them.

Operational documentation (moderate): The SPARC commits to alignment with ISO 27001, ISO 27002, and ISO 27018 and describes security controls, but the enumerated controls in that document are predominantly logical/technical in nature (access logging, 2FA, network protection, vulnerability scanning). Specific physical access controls — badge access systems, biometric controls, visitor management procedures, locked cage/rack policies — are not explicitly described. Physical security at the infrastructure layer is effectively delegated to AWS (the infrastructure provider), whose physical security practices are referenced but not reproduced in the SPARC.

Delegation to AWS (standard industry practice): For a cloud SaaS provider, delegating data center physical security to an IaaS provider (AWS) is standard market practice and does not represent a deficiency. AWS holds extensive independent physical security certifications (ISO 27001, SOC 1/2/3) that Slack references and builds upon. The SPARC references AWS certification documentation as the pathway to verification.

Overall: The contractual commitment to physical safeguards is explicit and unambiguous, and the mandatory maintenance of ISO 27001/SOC 2 certifications provides third-party validation that physical controls exist in practice. The absence of a dedicated "Physical Security Controls" section in the SPARC with enumerated controls is a documentation presentation gap rather than a control gap, but it prevents HIGH confidence. Classification: GREEN at MODERATE confidence.

— Note —
The AI cited 2 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "SFDC shall maintain appropriate technical and organizational measures for protection of the security (including protection against unauthorized or unlawful Processing and against accidental or unlawfu…"
2. "SFDC has obtained the third-party certifications and audits set forth in the Security, Privacy and Architecture Documentation for each applicable Service. Where SFDC has obtained ISO 27001 certificati…"

> *"SFDC will maintain appropriate administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Customer Data, as described in the Documentation. Those safeguards will include, but will not be limited to, measures designed to prevent unauthorized access to or disclosure of Customer Data (other than by Customer or Users)."*
> — https://www.salesforce.com/en-us/wp-content/uploads/sites/4/documents/legal/salesforce_MSA.pdf
> *"SFDC will maintain administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Personal Data uploaded to the Services, as described in the Security, Privacy and Architecture Documentation applicable to the specific Services purchased by Customer. SFDC will not materially decrease the overall security of the Services during a subscription term."*
> — Data Processing Addendum
> *"At a minimum, Salesforce will align with prevailing*
> *industry standards such as ISO 27001, ISO 27002, and ISO 27018."*
> — Security, Privacy and Architecture Report
> *"Infrastructure"*
> — Security, Privacy and Architecture Report

Compliance with Referenced Laws

AI Comment: This playbook item requires identification of every compliance obligation in the vendor terms that references a specific statute, regulation, or other legal requirement. Per the playbook instruction, all findings are classified YELLOW because whether the reviewing organization can abide by any given obligation is not determinable from the documents alone — reviewer confirmation is required for each. The ideal preference (no compliance obligations beyond laws applicable to the Customer's own use of the services) is NOT met.

Eleven distinct compliance obligations were identified across five documents (MSA, DPA, Supplemental Terms, and Security Report). They fall into five substantive categories:

1. Broad "Applicable Laws" Catch-All and Vendor-Policy Compliance (MSA §3.3)

Customer must use the Services in accordance with "applicable laws and government regulations" and must also comply with two externally-hosted vendor policy documents incorporated by reference: the Acceptable Use and External Facing Services Policy and the Artificial Intelligence Acceptable Use Policy. The content of these policies is not fully available in the provided document set (the Acceptable Use Policy document, Doc 3, is a placeholder page redirecting to an external Salesforce PDF). Any compliance obligations embedded in these vendor-authored policies cannot be assessed here and require separate review. This directly conflicts with the ideal preference because it imposes obligations tied to vendor-specific policy instruments that go beyond laws the Customer would otherwise face.

2. Specific Named Statutory/Regulatory Obligations (MSA §12.1, §12.2; DPA §2.1)
Three named regulatory frameworks are explicitly invoked:
— U.S. Export Laws (EAR/OFAC): Customer must not permit users to access Services from named embargoed regions and must not violate any U.S. export law or regulation. Customer also represents it is not on a U.S. denied-party list. These obligations are specific and concrete.
— Anti-Corruption Laws: A mutual representation that no illegal bribe or kickback has been offered or received implicitly obligates Customer to comply with applicable anti-corruption law (e.g., FCPA) in connection with the Agreement.
— Data Protection Laws and Regulations (DPA §2.1): The DPA expressly obligates Customer (as Controller or Processor) to process Personal Data in accordance with "Data Protection Laws and Regulations," which the DPA defines to include all applicable laws of the EU, EEA, Switzerland, UK, and United States and its states — sweeping in, for a US deployment, CCPA/CPRA and any applicable state privacy laws. Customer also bears sole responsibility for the legality of Personal Data and its means of acquisition.

3. Third-Party Privacy Rights (MSA §3.4)
Customer is prohibited from using the Services to store or transmit material in violation of third-party privacy rights. This is a legal-standard reference (privacy law obligations) that becomes binding via the contract's usage restrictions.

4. Jurisdiction-Specific Statutory Obligations — Conditional (MSA §12.12.1, §12.14)
Two jurisdiction-specific compliance obligations are embedded in the contract:
— France: If Customer is subject to French public health code Article L.1111-8, Customer must comply with the PGSSI-S (Global Information Security Policy for the Healthcare Sector).
— Italy: Customer commits to comply with the principles of Italian Legislative Decree 231/2001 (corporate liability for criminal acts) and SFDC's Code of Conduct. Violation may entitle SFDC to terminate for cause.
For a standard US-domiciled team chat deployment (governing law: California), these provisions are not currently triggered. However, they are present in the operative agreement and will activate if Customer's scope of operations extends to those jurisdictions.

5. Sensitive Data Regulatory Restrictions (Security Report)
The Security, Privacy and Architecture Documentation imposes data-submission restrictions tied to specific regulatory frameworks. For health data: if Customer submits PHI or other sensitive/regulated data, Customer bears responsibility for ensuring its processing complies with "all applicable laws and regulations" (a direct compliance obligation). For payment card data (PCI DSS framework), CJI, and FTI: outright prohibitions apply unless SFDC has obtained specific certifications/attestations, and for CJI/FTI, express SFDC permission is also required. These provisions reference specific regulatory classifications (HIPAA-adjacent, PCI DSS, FBI CJIS, IRS FTI rules) and impose compliance-management obligations on Customer.

Third-Party AI Acceptable Use Policies (Supplemental Terms)
Customer is required to comply with the "applicable third-party acceptable use policies" of AI providers powering Slack's generative AI features. These policies are external documents that vary by provider and are not available in the provided document set. This is an open-ended compliance obligation that exceeds laws applicable to the Customer's own use of the services.

Preference Analysis: The ideal preference is not met. In addition to laws that Customer would independently face (e.g., export control, data protection), the terms impose obligations on vendor-authored external policy documents (AUP, AI AUP, third-party AI AUPs), jurisdiction-conditional statutory compliance requirements (France PGSSI-S, Italy LD 231/2001), and a broad "Data Protection Laws and Regulations" obligation that may sweep in regulatory regimes beyond the Customer's current compliance program.

Document Quality Note: The Acceptable Use Policy document (Doc 3: y016g9ds96m5oykz4lg5ercu) is a landing page that redirects to an external Salesforce PDF. The full AUP content is not available in the document set; additional compliance obligations may exist in that document and should be assessed separately before closing this review item.

— Note —
The AI cited 4 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "Customer will (a) be responsible for Users' compliance with this Agreement, Documentation and Order Forms, (b) be responsible for the accuracy, quality and legality of Customer Data, the means by whic…"
2. "SFDC and Customer each represents that it is not on any U.S. government denied-party list. Customer will not permit any User to access or use any Service in a U.S.-embargoed country or region (current…"
3. "Customer acknowledges that SFDC has adopted an Organization, Management and Control Model pursuant to Legislative Decree 231/2001 to prevent crimes provided for therein and commits to comply with the …"
4. "Criminal justice information ("CJI") and federal tax information ("FTI") are prohibited except where (i) Salesforce has obtained any required certifications or attestations for the Covered Services an…"

"use a Service or Non-SFDC Application to store or transmit infringing, libelous, or otherwise unlawful or tortious material, or to store or transmit material in violation of third-party privacy rights"
— https://www.salesforce.com/en-us/wp-content/uploads/sites/4/documents/legal/salesforce_MSA.pdf
"Neither party has received or been offered any illegal or improper bribe, kickback, payment, gift, or thing of value from an employee or agent of the other party in connection with this Agreement. Reasonable gifts and entertainment provided in the ordinary course of business do not violate the above restriction."
— https://www.salesforce.com/en-us/wp-content/uploads/sites/4/documents/legal/salesforce_MSA.pdf
"12.12.1 PGSSI-S. To the extent Customer is subject to Article L.1111-8 (or any successor thereto) of the French public health code (Code de la Santé Publique), Customer shall abide by the Global Information Security Policy for the Healthcare Sector (PGSSI-S) pursuant to Article L.1110-4-1 (or any successor thereto) of the aforementioned code."
— https://www.salesforce.com/en-us/wp-content/uploads/sites/4/documents/legal/salesforce_MSA.pdf
"Customer as Controller or Processor shall, in its use of the Services, Process Personal Data in accordance with the requirements of Data Protection Laws and Regulations, including any applicable requirement to provide notice to Data Subjects of the use of SFDC as Processor (including where the Customer is a Processor, by ensuring that the ultimate Controller does so)."
— Data Processing Addendum
"Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data."
— Data Processing Addendum
"This Documentation provides information and product requirements specific to these generative AI features and providers, including applicable third-party acceptable use policies with which Customer must comply when using the generative AI technology."
— Slack Supplemental Terms | Legal | Slack
"If Customer does submit personal health information or other sensitive or regulated data to the Covered Services, then Customer is responsible for ensuring that its use of the Covered Services to process that information complies with all applicable laws and regulations."
— Security, Privacy and Architecture Report

Vendor's liability

AI Comment: The MSA (the primary contract governing Slack for US/California-domiciled Customer organizations) sets an aggregate liability cap equal to fees paid in the 12-month period preceding the first incident (MSA §10.1). This meets the acceptable position's cap-level threshold. However, the acceptable position also requires carve-outs from the cap for four specified categories — data breaches, breaches of confidentiality, IP infringement, and indemnification obligations — and none of these carve-outs are present in any document in the set.

DATA BREACH CARVE-OUT: The DPA §11 expressly subjects all DPA-based liability — including Customer Data incident claims — to the same MSA aggregate cap, and further specifies that the cap applies in the aggregate across both the MSA and all DPAs. This is a positive contractual statement that vendor liability for a data breach is capped at the same level as any routine breach, with no super-cap or exclusion. This directly contradicts the playbook's requirement for a data-breach carve-out.

CONFIDENTIALITY BREACH CARVE-OUT: No exception from the aggregate cap is provided for confidentiality breaches. The consequential damages exclusion in MSA §10.2 further restricts recovery (lost profits, business interruption, and goodwill are unrecoverable) with no carve-outs for breach-of-confidentiality scenarios. Under California law — the governing law for a US-domiciled team — such waivers are generally enforceable between commercial parties.

IP INFRINGEMENT CARVE-OUT: MSA §9.3 designates the Mutual Indemnification framework as the "sole liability" and "exclusive remedy" for third-party IP claims. While this directs IP claims into the indemnification regime rather than ordinary damages, neither §9 nor §10 explicitly carves the indemnification obligation out from the §10.1 aggregate cap. The prevailing interpretation under California contract law is that "sole liability / exclusive remedy" language confines the remedy type (to indemnification), not the remedy amount (which remains subject to the aggregate cap absent an explicit exclusion). Classified with MODERATE confidence due to this interpretive ambiguity — an alternative reading might find that the "sole liability" framing implicitly operates outside the aggregate cap.

INDEMNIFICATION OBLIGATIONS CARVE-OUT: No general carve-out from the aggregate cap for indemnification obligations is provided.

IDEAL PREFERENCE: The preference for uncapped vendor liability or a data-breach super-cap is not met.

USER TERMS $100 CAP: The User Terms cap Slack's liability to Authorized Users (individual employees) at $100. This cap applies only to claims brought by Authorized Users under the User Terms; it is superseded for Customer-level liability by the MSA per the User Terms' own precedence clause (§Entire Agreement). For completeness, this provision is included as a PIF and flagged as superseded.

GERMANY CARVE-OUTS (non-applicable): MSA §10.1 (Germany) provides unlimited liability for willful misconduct, gross negligence, guaranteed obligations, concealed defects, and bodily injury under German Product Liability Law. These carve-outs apply only to Germany-domiciled customers and are not operative under California law for this deployment.

CLASSIFICATION RATIONALE: YELLOW — the contract meets the fee-threshold component of the acceptable position but

is entirely missing all four required carve-outs. This falls short of the acceptable position, which requires both elements. The item is not RED because the cap amount itself is adequate; it is not GREEN because the carve-outs are absent. The practical risk is elevated for a team chat application that continuously processes employee communications: a data security incident could cause damages far exceeding 12 months' subscription fees, and the consequential damages exclusion in §10.2 would bar recovery for associated lost profits or business interruption without a breach-specific carve-out.

— Superseding reasoning —
The User Terms §Limitation of Liability contains a $100 aggregate cap applicable to Authorized Users. This provision is superseded by MSA §10.1's 12-month-fees aggregate cap for Customer-level liability claims. Two bases apply: (1) Document hierarchy — the User Terms §Entire Agreement explicitly states that "if there is a conflict or inconsistency between the Contract and the User Terms, the terms of the Contract will first prevail," subordinating the User Terms to the MSA (the Contract) for any conflict. (2) Party scope — the User Terms' liability cap addresses claims by and against Authorized Users (individual employees); Customer organizations bring claims against Slack under the MSA, not the User Terms. The MSA's aggregate cap therefore exclusively governs all Customer-level liability claims.

— Note —
The AI cited 4 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "IN NO EVENT SHALL THE AGGREGATE LIABILITY OF EACH PARTY TOGETHER WITH ALL OF ITS AFFILIATES ARISING OUT OF OR RELATED TO THIS AGREEMENT EXCEED THE TOTAL AMOUNT PAID BY CUSTOMER AND ITS AFFILIATES HERE…"
2. "IN NO EVENT WILL EITHER PARTY OR ITS AFFILIATES HAVE ANY LIABILITY ARISING OUT OF OR RELATED TO THIS AGREEMENT FOR ANY LOST PROFITS, REVENUES, GOODWILL, OR INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL…"
3. "Each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, and all DPAs between Authorized Affiliates and SFDC, whether in contract, tor…"
4. "This "Mutual Indemnification" section states the indemnifying party's sole liability to, and the indemnified party's exclusive remedy against, the other party for any third-party claim described in th…"

> *"Limitation of Liability"*
> — User Terms of Service | Legal | Slack

License Grant to Data – Our Company to Vendor

AI Comment: The contract addresses data licensing explicitly across multiple documents; the item is not silent. Analysis proceeds against the acceptable position (license must be non-exclusive) and the ideal preference (revocable, only to provide the service, data not used for vendor's own purposes).

Acceptable Position — Non-Exclusive: The primary data license in MSA §6.2 grants SFDC a "worldwide, limited-term" license to Customer Data "as appropriate for SFDC to provide and ensure proper operation of the Services." The license is never labeled "non-exclusive," but it also contains no exclusivity grant. Under California law (the governing law for US/Canada-domiciled customers per Supplemental Terms §18), a license grant that is silent on exclusivity is presumptively non-exclusive. The MSA reinforces this: §6.2 expressly states SFDC "acquires no right, title or interest" in Customer Data beyond the limited licenses. Applying the functional equivalence standard — same legal protection through different language — the acceptable position is met. However, for a Critical weight item, the absence of explicit "non-exclusive" language is a material drafting gap. If Slack's interpretation of the agreement changed or a dispute arose, the non-exclusivity would need to be litigated from a presumption rather than plain text.

Ideal Preference — Not Met. Two structural provisions prevent the ideal preference from being satisfied:

(1) **Supplemental Terms AI/ML Expansion (most significant):** The Slack Supplemental Terms §7.7 create a default authorization — framed as Customer "instructing" SFDC — for Slack to use Customer Data for: (a) training models for services/features the Customer has access to; (b) improving those services/features; and (c) R&D of products the Customer will access at no additional cost. These are vendor-beneficial purposes that exceed "only to provide the service to us." Critically, this is an opt-in by default — affirmative action by Org/Workspace Owners is required to opt out (via contact to feedback@slack.com per the Privacy Principles). Partial mitigations exist: the scope is limited to products/services Customer already has access to (not open-ended commercial exploitation); an opt-out mechanism is contractually referenced in §7.9 pointing to the Privacy Principles; and generative AI model training separately requires affirmative opt-in consent per Privacy Principles §10.43. These mitigations reduce the severity below RED but do not satisfy the ideal preference.

(2) **Feedback License (§6.3):** The MSA grants SFDC a "worldwide, perpetual, irrevocable, royalty-free" license to feedback from Customer and Users. "Perpetual" and "irrevocable" directly contradict the ideal preference of revocability. The practical scope is limited — feedback/suggestions about service operation, not core Customer Data (messages, files) — and the structure is standard SaaS industry practice. This limits the concern, but the terms remain materially inconsistent with the ideal preference.

DPA Caveat: The DPA §2.2 limits SFDC's processing of Personal Data to Customer's documented instructions, nominally supporting the ideal preference. However, this protection is circular: the Supplemental Terms' AI/ML provision constitutes such "documented instructions," so the DPA permits rather than restricts the ML/R&D data uses. The DPA also applies only to the Personal Data subset of Customer Data.

Overall Classification — YELLOW: The acceptable position (non-exclusive) is functionally met under California law's

presumption, supported by the "no right, title or interest" language in §6.2. The contract does not grant an exclusive license. However, the absence of explicit non-exclusive language for a Critical item, combined with the Supplemental Terms' default opt-in for AI/ML model training and R&D, the SFDC ownership of ML results derived from Customer Data, and the perpetual/ irrevocable feedback license, collectively prevent a GREEN classification. The ideal preference is clearly not met.

Remediation options for consideration: (1) Negotiate explicit "non-exclusive" language into MSA §6.2; (2) Amend the Supplemental Terms to default to opt-out rather than opt-in for AI/ML model training and R&D; (3) Scope the feedback license to be co-terminous with the subscription term or limit it to exclude Customer Data content.

— Note —
The AI cited 3 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "Customer grants SFDC, its Affiliates and applicable contractors a worldwide, limited-term license to host, copy, use, transmit, and display any Non-SFDC Applications and program code created by or for…"
2. "Customer grants to SFDC and its Affiliates a worldwide, perpetual, irrevocable, royalty-free license to use, distribute, disclose, and make and incorporate into its services any suggestion, enhancemen…"
3. "SFDC shall treat Personal Data as Confidential Information and shall Process Personal Data on behalf of and only in accordance with Customer's documented instructions for the following purposes: (i) P…"

> *"SFDC may access Customer Data in Slack for the following reasons, and Customer instructs SFDC to process its Customer Data for such purposes:*
>
> *1. to train models for use by the services and features that Customer has access to;*
> *2. to improve services and features that Customer has access to;*
> *3. to conduct research and development of products that Customer will have access to without additional cost;*
> *4. as otherwise provided in the MSA between SFDC and Customer."*
> — Slack Supplemental Terms | Legal | Slack
> *"Customer retains all ownership of its Customer Data and SFDC retains all ownership in and to aggregated machine learning results."*
> — Slack Supplemental Terms | Legal | Slack
> *"Slack will not use Customer Data to train generative AI models unless Customer provides affirmative opt-in consent."*
> — Slack Privacy Principles

Retention of our Rights to our Property

AI Comment: The playbook item requires that no ownership of the reviewing organization's products, services, materials, content, or data be transferred to the vendor. This is a Critical-weight item — a RED finding would require Board approval and a documented exception.

Overall Assessment: GREEN. The Slack/Salesforce document suite explicitly and consistently confirms that Customer retains ownership of its Customer Data. No ownership transfer occurs under any provision in the provided document set.

Governing provisions confirming ownership retention:
1. User Terms (§"What This Means for You"): "Customer Data is owned by Customer"
2. MSA §6.2 (general): "SFDC acquires no right, title or interest from Customer or its licensors under this Agreement in or to any Customer Data"
3. Slack Supplemental Terms (governing, Slack-specific): "Customer retains all ownership of its Customer Data and SFDC retains all ownership in and to aggregated machine learning results" — the most specific statement of ownership allocation for Slack services
4. DPA §2.2: SFDC treats Personal Data as Confidential Information and processes it only per Customer's documented instructions

Three nuances that do not constitute prohibited ownership transfers but warrant awareness (each surfaced as YELLOW PIFs):

(a) ML Model Derivative Ownership (Supplemental Terms §7-7/7-8): By accepting the Supplemental Terms, Customer pre-authorizes SFDC to use Customer Data for ML model training and R&D by default. SFDC acquires ownership of the resulting "aggregated machine learning results." Customer Data ownership is retained, but SFDC builds and owns commercially valuable proprietary ML assets derived from that data. Customers may opt out of predictive ML training; generative AI training requires affirmative opt-in consent (Privacy Principles).

(b) Perpetual, Irrevocable Feedback License (MSA §6.3): SFDC obtains a worldwide, perpetual, irrevocable, royalty-free license over any feedback provided by Customer or Users about the service. Though expressly limited to feedback about service operation rather than Customer Data broadly, the durability and scope of this license (perpetual, irrevocable) is functionally ownership-equivalent for that category of content.

(c) Aggregated/De-identified Data (Privacy Policy): Slack may "disclose or use aggregated or de-identified Information for any purpose." De-identification removes the data from Customer Data status under applicable law, so this does not transfer ownership of Customer Data itself; however, it creates a broad commercial right over data derived from Customer Data with no stated restriction.

None of these nuances constitutes a prohibited transfer of ownership under the playbook's acceptable position. Customer Data ownership is expressly and repeatedly reserved to Customer across the document set. Classification: GREEN, Confidence: HIGH.

Jurisdiction note (California, most probable governing law for US-domiciled team): Under California law, contractual ownership-retention provisions of this clarity are enforceable. The opt-out mechanism for ML training (and opt-in requirement for generative AI) is accessible to US Customers.

— Superseding reasoning —
The Slack Supplemental Terms §"Slack Search, Learning and Artificial Intelligence" (PIF index 4, sentence 7-8) is more specific to Slack's operational context than the general Salesforce MSA §6.2 provision (PIF index 1, sentence 4-131) and governs the ownership-allocation question for Slack services. Both provisions confirm that SFDC acquires no ownership of Customer Data; however, the Supplemental Terms adds the Slack-specific nuance that SFDC retains ownership of aggregated machine learning results derived from Customer Data. Under the specific-over-general principle, the Supplemental Terms controls for Slack AI/ML ownership matters, and its language is the final governing statement on ownership allocation for Slack services.

— Note —
The AI cited 3 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "When an Authorized User (including, you) submits content or information to the Services, such as messages or files ("Customer Data"), you acknowledge and agree that the Customer Data is owned by Custo…"
2. "Customer grants to SFDC and its Affiliates a worldwide, perpetual, irrevocable, royalty-free license to use, distribute, disclose, and make and incorporate into its services any suggestion, enhancemen…"
3. "SFDC shall treat Personal Data as Confidential Information and shall Process Personal Data on behalf of and only in accordance with Customer's documented instructions for the following purposes: (i) P…"

> *"Subject to the limited licenses granted herein, SFDC acquires no right, title or interest from Customer or its licensors under this Agreement in or to any Customer Data, Non-SFDC Application or such program code."*
> — https://www.salesforce.com/en-us/wp-content/uploads/sites/4/documents/legal/salesforce_MSA.pdf
> *"SFDC may access Customer Data in Slack for the following reasons, and Customer instructs SFDC to process its Customer Data for such purposes:*
>
> *1. to train models for use by the services and features that Customer has access to;*
> *2. to improve services and features that Customer has access to;*
> *3. to conduct research and development of products that Customer will have access to without additional cost;*
> *4. as otherwise provided in the MSA between SFDC and Customer."*
> — Slack Supplemental Terms | Legal | Slack
> *"Customer retains all ownership of its Customer Data and SFDC retains all ownership in and to aggregated machine learning results."*
> — Slack Supplemental Terms | Legal | Slack
> *"We may disclose or use aggregated or de-identified Information for any purpose."*
> — Privacy Policy | Legal | Slack
> *"Slack will not use Customer Data to train generative AI models unless Customer provides affirmative opt-in consent."*
> — Slack Privacy Principles
> *"If you want to exclude your Customer Data from helping train Slack global models, you can opt out."*
> — Slack Privacy Principles

No AI/ML Training on Our Data

AI Comment: The Slack Supplemental Terms directly and unambiguously address AI/ML training on Customer Data in the "Slack Search, Learning and Artificial Intelligence" section, which is the dispositive contractual provision for this item. As a precondition of the service, the Supplemental Terms require Customer to pre-authorize SFDC's use of Customer Data to: (1) train models for services and features the Customer has access to; (2) improve those services and features; and (3) conduct R&D for products the Customer will access without additional cost. SFDC also explicitly retains ownership of "aggregated machine learning results" derived from Customer Data.

The playbook's acceptable position permits training only on "models used solely for us." The Supplemental Terms' authorization is materially broader on all three purposes. Purposes (2) and (3) involve general service-wide improvement and R&D benefiting all Slack customers — not models exclusive to any one customer. Purpose (1) — "models for use by the services and features that Customer has access to" — describes shared, globally-deployed infrastructure (every Slack customer accesses the same features), not customer-exclusive models. This reading is confirmed by the Privacy Principles, which acknowledge that Slack trains "global models" "used broadly across all of our customers," with Customer Data contributing to those models unless the customer affirmatively opts out.

Two partial mitigations exist but are insufficient to satisfy the acceptable position:

1. An opt-out mechanism for global model training is referenced in the Supplemental Terms and detailed in the Privacy Principles (Documentation level). However: the contractual default is opt-IN — Customer Data IS used for global model training absent affirmative opt-out; even after opt-out, Customer Data continues to be used to "improve the experience on your own workspace," meaning workspace-level model training persists; and the operative terms of the opt-out are contained only in subordinate Documentation, not the governing Slack Terms.

2. For generative AI specifically, the Privacy Principles require affirmative opt-in consent. This is a stronger protection, but it: (a) resides in Documentation-level Privacy Principles, subordinate to the Slack Terms per MSA §12.3 order of precedence; (b) covers only generative AI — predictive/ML models remain opt-out by default per the broader Privacy Principles; and (c) is not carved out in the Supplemental Terms' express AI training authorization.

The DPA (§2.2) and MSA (§2.5) both condition AI/data processing on "Customer's documented instructions," which appears protective. However, those provisions do not restrict AI/ML training here because the Supplemental Terms define those instructions to include AI/ML training as a service precondition — the Supplemental Terms satisfy the "documented instructions" standard by embedding broad AI training authorization in the contractual terms themselves.

Classification: RED. The governing contractual terms (Supplemental Terms) authorize AI/ML training on Customer Data for global models as a default condition of service, directly and materially conflicting with the acceptable position requiring training to be limited to models used solely for the Customer. For this Critical-weight item, this is a blocking finding requiring Board approval and a documented exception if accepted.

— Superseding reasoning —
The Slack Supplemental Terms ("Slack Search, Learning and Artificial Intelligence" section) govern on this item via two superseding principles: (1) SPECIFIC_OVER_GENERAL — the Supplemental Terms provide Slack-specific AI/ML processing authorizations that define and operationalize the scope of "Customer's documented instructions" referenced generically in MSA §2.5 and DPA §2.2; on the AI training question, the specific Slack provisions displace the general processing-instruction standard. (2) DOCUMENT_HIERARCHY — the Privacy Principles' operational commitments (opt-out mechanism, generative AI opt-in requirement, statement of no generative AI development) are Documentation-level, expressly subordinate to the Agreement per MSA §12.3 order of precedence (Order Form !' Agreement [including Supplemental Terms] !' Documentation). The Privacy Principles represent operational commitments that cannot contractually override the Supplemental Terms' express AI training authorization, though they remain relevant as practical risk-mitigation context for the reviewing attorney.

— Note —
The AI cited 1 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "SFDC shall treat Personal Data as Confidential Information and shall Process Personal Data on behalf of and only in accordance with Customer's documented instructions for the following purposes: (i) P…"

> *"SFDC may access Customer Data in Slack for the following reasons, and Customer instructs SFDC to process its Customer Data for such purposes:*
>
> *1. to train models for use by the services and features that Customer has access to;*
> *2. to improve services and features that Customer has access to;*
> *3. to conduct research and development of products that Customer will have access to without additional cost;*
> *4. as otherwise provided in the MSA between SFDC and Customer."*
> — Slack Supplemental Terms | Legal | Slack
> *"Customer retains all ownership of its Customer Data and SFDC retains all ownership in and to aggregated machine learning results."*
> — Slack Supplemental Terms | Legal | Slack
> *"Slack Search, Learning and Artificial Intelligence"*
> — Slack Supplemental Terms | Legal | Slack
> *"2.5 AI Features. The Services may comprise or include artificial intelligence ("AI") features or functionality. SFDC is committed** to the responsible development of AI in the Services as further described in the Documentation at https://www.salesforce.com/en-us/wp-content/uploads/sites/4/documents/legal/misc/salesforce-trusted-ai-resources.pdf. Processing of Customer Data by Services that include AI features or functionality will only be in accordance with Customer's documented instructions."*
> — https://www.salesforce.com/en-us/wp-content/uploads/sites/4/documents/legal/salesforce_MSA.pdf
> *"Slack will not use Customer Data to train generative AI models unless Customer provides affirmative opt-in consent."*
> — Slack Privacy Principles
> *"If you want to exclude your Customer Data from helping train Slack global models, you can opt out. If you opt out, Customer Data on your workspace will only be used to improve the experience on your own workspace and you will still enjoy all of the benefits of our globally trained ML models without contributing to the underlying models."*
> — Slack Privacy Principles
> *"We do not develop generative AI models using Customer Data."*
> — Slack Privacy Principles

Processing Limitation

AI Comment: The playbook requires processing to be limited to fulfilling contractual obligations and written instructions. The document set presents a significant internal tension: strong, explicit instruction-following provisions in the DPA (§ 2.2) and MSA (§ 2.5) that, read in isolation, directly satisfy this Critical-weight requirement — alongside a competing pre-authorization in the Slack Supplemental Terms that permits SFDC to use Customer Data for model training, service improvement, and R&D, framed as deemed "Customer instructions" embedded in vendor-drafted standard terms.

The DPA § 2.2 is the strongest provision in the set. It restricts SFDC to processing "on behalf of and only in accordance with Customer's documented instructions" for three enumerated purposes. The MSA § 2.5 extends this explicitly to AI features. These provisions, if governing, fully satisfy the playbook requirement.

The Supplemental Terms' "Slack Search, Learning and Artificial Intelligence" section cuts directly against this. It pre-authorizes SFDC to access Customer Data for (1) model training, (2) service improvement, and (3) R&D for future products, and characterizes this as the Customer "instructing" SFDC to process. This is a vendor-embedded deemed-instruction construct — the Customer has not affirmatively directed these uses; Slack has incorporated them into its standard terms

and deemed the Customer to have agreed. Processing for model training and R&D goes beyond "fulfilling contractual service delivery obligations" in the traditional, GDPR Article 28 / CCPA service-provider sense of the term. The Privacy Principles confirm this plays out in practice: Customer Data is analyzed for predictive ML model development by default, with only an opt-out mechanism available to restrict it — not an opt-in requirement. For generative AI training specifically, the Privacy Principles do require affirmative opt-in, which is the stronger and more compliant posture.

The conflict between the DPA § 2.2 (instruction-only processing) and the Supplemental Terms (pre-authorized AI/ML uses) cannot be silently resolved: both documents are part of the same contractual framework without an explicit hierarchy for this specific conflict type. This conflict is flagged for human review.

YELLOW is assigned (not GREEN) because: (1) the Supplemental Terms meaningfully expand permitted processing beyond what a genuine instruction-following model allows; (2) the default opt-out posture for predictive model training departs from the acceptable position for a Critical item; and (3) for a Critical-weight item, this ambiguity and gap prevent GREEN. YELLOW is assigned rather than RED because strong instruction-following language does exist in the DPA and MSA, the Supplemental Terms' pre-authorized uses are not entirely unbounded (scoped to products/services Customer accesses), and the conflict creates genuine ambiguity rather than an unambiguous violation.

— Superseding reasoning —
The Supplemental Terms' "Slack Search, Learning and Artificial Intelligence" section (PIF index 4) directly conflicts with both the DPA § 2.2 instruction-only processing limitation (PIF index 2) and the MSA § 2.5 AI processing requirement (PIF index 1). Two superseding principles apply in tension: (1) SPECIFIC_OVER_GENERAL — the Supplemental Terms are Slack-product-specific and would, under this principle, govern Slack's AI/ML processing over the general DPA instruction requirement and the general Salesforce MSA AI provision. (2) However, the MSA § 2.5 is also AI-specific, making the Supplemental Terms vs. MSA § 2.5 a peer-level conflict rather than a clear specific-over-general case. Additionally, the DPA embodies GDPR Article 28 and CCPA service-provider compliance obligations that arguably function as a minimum protection floor that commercial terms cannot erode — meaning the DPA's "documented instructions only" standard may prevail regardless of Supplemental Terms language. The documents do not contain an explicit hierarchy between the DPA and the Supplemental Terms for this conflict type. This is a FLAGGED competing hierarchy situation requiring human review; the governing language cannot be stated with confidence without legal determination.

— Note —
The AI cited 3 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "Processing of Customer Data by Services that include AI features or functionality will only be in accordance with Customer's documented instructions."
2. "SFDC shall treat Personal Data as Confidential Information and shall Process Personal Data on behalf of and only in accordance with Customer's documented instructions for the following purposes: (i) P…"
3. "SFDC shall inform Customer immediately (i) if, in its opinion, an instruction from Customer constitutes a breach of the GDPR and/or (ii) if SFDC is unable to follow Customer's instructions for the Pro…"

> *"How We Process Your Information and our Legal Bases for Doing So"*
> — Privacy Policy | Legal | Slack
> *"SFDC may access Customer Data in Slack for the following reasons, and Customer instructs SFDC to process its Customer Data for such purposes:*
>
> *1. to train models for use by the services and features that Customer has access to;*
> *2. to improve services and features that Customer has access to;*
> *3. to conduct research and development of products that Customer will have access to without additional cost;*
> *4. as otherwise provided in the MSA between SFDC and Customer."*
> — Slack Supplemental Terms | Legal | Slack
> *"Privacy Principles: Search, Learning and Artificial Intelligence"*
> — Slack Privacy Principles
> *"Slack will not use Customer Data to train generative AI models unless Customer provides affirmative opt-in consent."*
> — Slack Privacy Principles

Insurance

AI Comment: The playbook item requires that the vendor maintains adequate insurance. A complete review of all nine provided documents — User Terms of Service (Doc 1), Privacy Policy (Doc 2), Acceptable Use Policy (Doc 3), Salesforce Main Services Agreement / MSA (Doc 4), Data Processing Addendum landing page (Doc 5), Data Processing Addendum full text (Doc 6), Slack Supplemental Terms (Doc 7), Slack Main Services Agreement page (Doc 8), Security/Privacy/Architecture Report (Doc 9), and Privacy Principles (Doc 10) — reveals no insurance representation, covenant, maintenance obligation, or certification anywhere across the entire Slack/Salesforce contractual framework for online orders.

Silence Classification: The item weight is "Acceptable to Deviate," which triggers a default YELLOW classification per the silence-handling framework.

Statutory Mitigation Evaluated: No California statute, nor any other potentially governing law identified in the three-tier jurisdiction clause (California / England / Japan), requires SaaS vendors to maintain specific insurance coverage and certify such in a public-facing agreement. No statutory downgrade is applicable.

Industry Norm Evaluated: Silence on insurance in publicly posted SaaS online terms is standard market practice. Enterprise customers who require insurance certifications — for example, minimum coverage levels for commercial general liability, errors & omissions, or cyber liability — routinely negotiate those requirements into custom MSAs or Order Form riders, not

through standard online clickwrap agreements. Slack/Salesforce is a major public company operating internationally and almost certainly carries commercial insurance in practice. However, a formal industry norm downgrade to GREEN has not been applied here: GREEN would imply the acceptable position is affirmatively met, which cannot be established from silence alone. The downgrade framework reduces the assessed risk of silence; it does not certify compliance.

Risk Context: Practical risk is low given: (1) the item is weighted Acceptable to Deviate — the lowest playbook weight, explicitly noting this is not a dealbreaker; (2) the deployment is a standard team chat tool (Slack) for an internal team, not a high-risk data processor or regulated-data environment; (3) Slack/Salesforce's scale and public company status makes total absence of commercial insurance coverage an implausible business scenario. If insurance requirements are important to the reviewing organization, they must be addressed through negotiated enterprise agreement terms or an Order Form addendum — they will not be found in, or satisfied by, Slack's standard online terms.

Ownership of Custom Deliverables

AI Comment: The playbook requires that the vendor affirmatively assign ownership of custom deliverables to Customer, while the vendor may retain rights to its own pre-existing and background IP. This is a High-weight item. Across all reviewed documents, no such assignment provision exists — the contract is entirely silent on this obligation.

The existing IP framework in the Salesforce MSA and Slack Supplemental Terms works in the opposite direction from the playbook requirement:

1. **Broad SFDC IP Reservation (MSA §6.1):** SFDC reserves "all of their right, title and interest in and to the Services, including all of their related intellectual property rights," granting no rights to Customer except as expressly stated. No exception exists for custom-developed work product created specifically for a Customer. Under the default contractual framework, any custom deliverable developed by SFDC under the MSA would be claimed by SFDC, not assigned to Customer.

2. **Adverse Feedback License (MSA §6.3):** Customer grants SFDC a worldwide, perpetual, irrevocable, royalty-free license to use and incorporate Customer feedback and suggestions. This provision runs contrary to a custom deliverables assignment framework — improvements arising from Customer input belong to SFDC, not Customer.

3. **SFDC Retains ML Results (Supplemental Terms §Slack Search, Learning and AI):** SFDC explicitly retains ownership of "aggregated machine learning results" derived from processing Customer Data, further demonstrating that SFDC retains deliverables arising from its processing activities rather than assigning them to Customer.

4. **Narrow Favorable Carve-Out — AI Output (Supplemental Terms §Generative AI):** The Supplemental Terms designate AI-generated output as Customer Data ("as between SFDC and Customer, such output is Customer Data"). This is a narrow positive provision for one specific category of output, but it does not constitute a general assignment framework for custom deliverables, nor does it address custom software, custom integrations, or professional services work product.

5. **Customer's Own IP Protected (MSA §6.2):** SFDC affirms it "acquires no right, title or interest from Customer" in Customer Data, Non-SFDC Applications, or program code Customer brings to or builds using the platform. This partially satisfies the "vendor retains background IP" aspect of the playbook item by confirming Customer's own pre-existing IP is protected. However, this provision addresses what Customer brings in — it says nothing about IP that SFDC itself creates for Customer.

Contextual note: Slack is a standard SaaS team communication platform, not a professional services or custom software development vendor. Its standard service model does not involve creating bespoke custom deliverables for individual customers in the conventional sense. However, this SaaS context does not cure the contractual gap: if any custom work were developed (custom Slack apps, bespoke integrations, custom feature development under a professional services engagement), the MSA §6.1 IP reservation would default to SFDC ownership with no assignment mechanism for Customer. No separate professional services agreement or statement of work containing an IP assignment was included in the document set.

Silence Classification: High-weight item !' default RED. No statutory downgrade applies (no statute provides equivalent custom deliverables assignment protection). No industry norm downgrade applies (the absence of an assignment clause in a SaaS vendor agreement where the vendor does provide custom professional services work is not standard practice that reduces practical risk — it is a meaningful gap). Classification: **RED**.

— Superseding reasoning —
The Slack Supplemental Terms' Generative AI provision (PIF index 3) is more specific than the MSA's general IP reservation (PIF index 0) for the narrow category of AI-generated output. Where the MSA broadly reserves SFDC's rights "in and to the Services," the Supplemental Terms specifically address the output of Generative AI features, designating that output as Customer Data and therefore Customer-owned. Because the Supplemental Terms were designed to supplement and modify the MSA specifically for Slack's AI/ML product features, the more specific Supplemental Terms provision governs Customer ownership of AI-generated output. This superseding determination is strictly limited to AI-generated output from the Generative AI features; the MSA §6.1 IP reservation continues to govern for all other Services IP and for any custom deliverables that fall outside the definition of AI-generated output.

— Note —
The AI cited 2 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.

1. "Subject to the limited rights expressly granted hereunder, SFDC, its Affiliates, and its licensors reserve all of their right, title and interest in and to the Services, including all of their related…"
2. "Customer grants to SFDC and its Affiliates a worldwide, perpetual, irrevocable, royalty-free license to use, distribute, disclose, and make and incorporate into its services any suggestion, enhancemen…"

> *"Subject to the limited licenses granted herein, SFDC acquires no right, title or interest from Customer or its licensors under this Agreement in or to any Customer Data, Non-SFDC Application or such program code."*
> — https://www.salesforce.com/en-us/wp-content/uploads/sites/4/documents/legal/salesforce_MSA.pdf
> *"Customer assumes all responsibility for output generated by the Services and, as between SFDC and Customer, such output is Customer Data."*
> — Slack Supplemental Terms | Legal | Slack
> *"Customer retains all ownership of its Customer Data and SFDC retains all ownership in and to aggregated machine learning results."*
> — Slack Supplemental Terms | Legal | Slack

Governing Law

AI Comment: The governing law is explicitly addressed across multiple documents. For the most probable deployment scenario — a US-domiciled customer — the applicable governing law is California and controlling United States federal law, as established in the Slack Supplemental Terms (superseding the MSA for online Slack orders) and confirmed in the MSA itself.

The acceptable position requires the governing law to be Michigan, Delaware, New York, "or another jurisdiction with a reasonable connection (nexus) to either party — e.g., where a party is incorporated or headquartered." California clearly satisfies the nexus carve-out: Slack Technologies, LLC and its parent Salesforce, Inc. maintain their principal place of business at Salesforce Tower, 415 Mission Street, San Francisco, California. Additionally, the DPA confirms that Slack Technologies, LLC is a Delaware LLC — Delaware is one of the playbook's enumerated acceptable jurisdictions — though California law governs the contract rather than Delaware law. California's nexus is independently sufficient.

The Slack Supplemental Terms (doc 7) are the controlling instrument for online Slack orders: they explicitly state the governing law section applies "in place of" the MSA's corresponding provision. In practice, for US/Canada domiciled customers both documents converge on California, so the superseding does not change the substantive outcome here.

The User Terms of Service (doc 1) simply defer to "the same applicable governing law of the Contract," presenting no independent governing law choice and no conflict.

Item weight is Acceptable to Deviate. California meets the acceptable position's nexus standard; classification is GREEN. aiPreferenceMet is false because no ideal preference was specified in the playbook item.

— Superseding reasoning —
The Slack Supplemental Terms (doc 7, PIF index 0) explicitly state that, for online orders of Slack Services, their governing law/venue section applies "in place of the SFDC Contracting Entity, Notices, Governing Law, and Venue sections in the MSA." This language is an express, specific override of the MSA's (doc 4, PIF index 1) general governing law clause. The Supplemental Terms are Slack-specific (narrow scope) versus the MSA's applicability to all Salesforce products (broad scope). For a US/Canada domiciled customer, both documents independently reach the same outcome — California governing law — so the superseding determination does not alter the substantive classification, but the Supplemental Terms are the operative instrument.

— Note —
The AI cited 1 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "12.9 SFDC Contracting Entity, Notices, Governing Law, and Venue. The SFDC entity entering into this Agreement, the address to which Customer should direct notices under this Agreement, the law that wi…"

> *"For an online order of Slack Services (a Slack plan purchased via the Slack website), the following applies in place of the SFDC Contracting Entity, Notices, Governing Law, and Venue sections in the MSA:*
>
> *The SFDC entity entering into the Slack Terms, the address to which Customer should direct notices under the Slack Terms, the law that will apply in any dispute or lawsuit arising out of or in connection with the Slack Terms, and the courts that have jurisdiction over any such dispute or lawsuit, depend on where Customer is domiciled."*
> — Slack Supplemental Terms | Legal | Slack
> *"Governing Law; Venue; Fees"*
> — User Terms of Service | Legal | Slack

Encryption at Rest

AI Comment: The playbook requires explicit data encryption at rest at AES-256 bit or the then-current industry standard. After reviewing all documents in the set — User Terms, Privacy Policy, Acceptable Use Policy, MSA, Slack Supplemental Terms, DPA, and the Security, Privacy and Architecture Report (SPARC) — no document explicitly confirms AES-256 encryption at rest or names any specific encryption algorithm applied to stored Customer Data.

Three documents address security measures at varying levels of specificity. The SPARC (Doc 9) is the operative governing document for specific security technical controls: both the DPA §6.1 (which states controls apply "as set forth in the Security, Privacy and Architecture Documentation") and the MSA §2.2 (which states safeguards are "as described in the Documentation," defined as Salesforce's Trust and Compliance documentation) defer to the SPARC for specifics. The SPARC commits to "appropriate technical and organizational measures" and to alignment "with prevailing industry

standards such as ISO 27001, ISO 27002, and ISO 27018."

ISO 27002 is a widely recognized cryptographic controls standard — its 2022 revision includes Control 8.24 (Use of cryptography), which requires organizations to apply appropriate cryptographic controls based on risk assessment, and AES-256 is the prevailing practice for data at rest under that framework. ISO 27018 addresses protection of PII in public cloud environments. These references are meaningful and provide indirect support for encryption compliance, and the DPA §6.3 further commits to maintaining ISO 27001 certifications for the duration of the Agreement (6-118). However, an ISO alignment commitment is not equivalent to an explicit contractual AES-256 confirmation: ISO 27001/27002 compliance requires cryptographic controls but does not mandate a specific algorithm in contractual language.

Critically, the SPARC's enumerated list of security controls (Access Logging, Access Management, Data Retention, Host Management, Network Protection, Product Security Practices, Team-wide 2FA) does not include an "encryption at rest" control. The SPARC's "Data at Rest" section (9-67) addresses only data residency geography, not encryption. No encryption algorithm is named anywhere in the document set.

Classification: YELLOW. The vendor's terms address the security topic broadly through general TOMs language and ISO standards alignment — this addresses the same subject matter as the playbook item but with weaker and less specific protection than required. The contract is not silent, but the explicit AES-256 (or equivalent named standard) confirmation that the playbook requires is absent.

The playbook's "then-current industry standard" alternative provides some flexibility, and ISO 27001/27002 alignment is a meaningful commitment — but the contractual language stops short of confirming the specific encryption standard for data at rest. Additional information may be contained in the full Trust and Compliance documentation linked from the SPARC but not reproduced in this document set. For a HIGH weight item, documented justification is required; the reviewer should seek explicit vendor confirmation of encryption at rest standard via the Trust and Compliance portal or direct inquiry before acceptance.

— Superseding reasoning —
The SPARC (Security, Privacy and Architecture Report, Doc 9) is the operative document for specific security technical controls, as both the DPA and MSA explicitly defer to it. The DPA §6.1 states that technical and organizational measures apply "as set forth in the Security, Privacy and Architecture Documentation" — a direct cross-reference making the SPARC the source of truth for specific security control content. The MSA §2.2 refers to "the Documentation," which is defined in MSA §1 as "the applicable Service's Trust and Compliance documentation," again pointing to the SPARC. The SPARC therefore supersedes the DPA §6.1 and MSA §2.2 for specific security technical controls under a specific-over-general rule. As between DPA and MSA, the DPA governs over the MSA on data processing and protection matters by document hierarchy — the DPA is a purpose-built addendum for data protection obligations that supplements and narrows the general MSA commitments.

— Note —
The AI cited 1 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "SFDC shall maintain appropriate technical and organizational measures for protection of the security (including protection against unauthorized or unlawful Processing and against accidental or unlawfu…"

> *"Security Controls"*
> — Security, Privacy and Architecture Report
> *"At a minimum, Salesforce will align with prevailing*
> *industry standards such as ISO 27001, ISO 27002, and ISO 27018."*
> — Security, Privacy and Architecture Report
> *"SFDC will maintain appropriate administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Customer Data, as described in the Documentation."*
> — https://www.salesforce.com/en-us/wp-content/uploads/sites/4/documents/legal/salesforce_MSA.pdf

Subprocessor Change Notification

AI Comment: The DPA (Document 6) contains a structured, three-part subprocessor notification and objection framework that substantially meets the acceptable position.

Notification (§5.2): SFDC maintains a current subprocessor list in publicly accessible Infrastructure and Sub-processor Documentation and, upon Customer subscription to the notification mechanism, is contractually obligated to notify Customer *before* authorizing any new subprocessor to process Customer Data. The subscription condition is a procedural step within Customer's control and does not fundamentally undermine the protection—once subscribed, notification is guaranteed prior to authorization. However, "before" authorizing is not the same as "at least 30 days before" authorizing, which is the gap from the ideal preference.

30-Day Objection Window (§5.3): Explicitly and unambiguously provided. Customer has 30 days from receipt of notice to object in writing. Upon valid objection, SFDC must use reasonable efforts to accommodate (e.g., by restructuring the service to avoid the subprocessor) for up to 60 days. This directly satisfies the acceptable position's requirement that Customer have at least 30 days from notice to object.

Termination with Refund (§5.3): If SFDC cannot accommodate the objection within 60 days, Customer may terminate the applicable Order Form(s) for the affected Services, and SFDC will refund all prepaid fees covering the remainder of the term, with no penalties. This directly satisfies the acceptable position's requirement that Customer may terminate with a pro-rata refund if the vendor proceeds with an objected-to subprocessor.

Why GREEN and not YELLOW: All three required elements of the acceptable position are present with explicit contractual language — notification mechanism, 30-day objection window, and termination-with-refund remedy. The subscription requirement for active notifications is a mild procedural step, not a substantive protection gap.

Why aiPreferenceMet = false: The preference requires "at least 30 days' advance notice before the subprocessor begins processing." The DPA guarantees only that notice will be given "before authorizing" the subprocessor — which could, in theory, be one day before. There is no contractual minimum lead time of 30 days ahead of the subprocessor's first processing activity. This is a meaningful gap from the ideal because a very short advance notice window would render the 30-day objection period functionally insufficient to prevent processing from occurring.

Superseding note: For European data transfer contexts, the Standard Contractual Clauses in Schedule 1, Section 2.8 of the DPA establish an unconditional "shall inform" obligation that supersedes §5.2's subscription-conditional language, per the DPA's own hierarchy clause (§6.321: "In the event of any conflict or inconsistency between the body of this DPA and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail"). For this US-domiciled deployment (California governing law), the SCC provisions do not directly govern the Customer's own data flows, so §5.2's subscription-conditional mechanism remains the primary operative notification provision.

DPA execution note: The DPA is a separately executable instrument (Docusign-executed, April 2026 revision). However, the Salesforce MSA (§2.2) incorporates the DPA by reference, so these subprocessor protections bind SFDC under the Slack Terms regardless of whether Customer separately executes the standalone DPA form.

— Superseding reasoning —
DPA §5.2 (subscription-conditional notification in the main DPA body) is superseded by Schedule 1 §2.8 (unconditional "shall inform" obligation under the SCC framework) for European data transfer contexts. The DPA's own Section 6.321 establishes the hierarchy: "In the event of any conflict or inconsistency between the body of this DPA and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail." Because §2.8 imposes an unconditional notification duty while §5.2 conditions it on Customer subscription, these provisions are in direct conflict, and §2.8 controls for SCC-governed transfers. For the US-domiciled, California-law scenario that is the most probable governing context for this deployment, the SCCs do not govern Customer's own data flows (they apply to EU/EEA/UK !’ US transfers), so §5.2's subscription-conditional mechanism remains the operative notification provision for this Customer's primary use case.

— Note —
The AI cited 3 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "The Infrastructure and Sub-processor Documentation contains a mechanism to subscribe to notifications of new Sub-processors for each applicable Service, and if Customer subscribes, SFDC shall provide …"
2. "Customer may object to SFDC's use of a new Sub-processor by notifying SFDC promptly in writing within thirty (30) days of receipt of SFDC's notice in accordance with the mechanism set out in section 5…"
3. "Pursuant to clause 9(a), Customer acknowledges and expressly agrees that SFDC may engage new Sub-processors as described in sections 5.2 and 5.3 of this DPA. SFDC shall inform Customer of any changes …"

Assignment

AI Comment: The playbook item requires two things: (1) both parties may freely assign to successors in interest via merger or acquisition without consent; and (2) any other assignment by the Vendor requires the Customer's prior consent.

The governing Customer-Vendor agreement is the Salesforce Main Services Agreement ("MSA") as supplemented by the Slack Supplemental Terms (together, the "Slack Terms"). MSA § 12.8 directly addresses both requirements:

Requirement 1 — M&A / Successor assignment without consent: MSA § 12.8 permits either party to assign the Agreement "without the other party's consent to its Affiliate or in connection with a merger, acquisition, corporate reorganization, or sale of all or substantially all of its assets." This covers successors in interest via merger or acquisition for both parties, satisfying the first limb of the playbook item. The scope is slightly broader than the playbook baseline in that it also includes affiliate assignments without consent — this is standard market practice and customer-neutral.

Requirement 2 — Vendor's other assignments require Customer prior consent: MSA § 12.8 states that "neither party may assign any of its rights or obligations hereunder… without the other party's prior written consent (not to be unreasonably withheld)." This means any Vendor assignment outside the M&A/affiliate carve-out requires Customer's prior written consent. The "(not to be unreasonably withheld)" qualifier is an extremely common commercial formulation that prevents a party from using consent as an arbitrary veto, but does not eliminate the consent requirement itself. The playbook item requires "prior consent" without specifying that it must be unfettered; the MSA satisfies the requirement while adding a standard reasonableness qualifier.

Additional customer-protective provision: The MSA includes a termination right in Customer's favor: if Vendor is acquired by, or undergoes a change of control in favor of, a direct competitor of Customer, Customer may terminate the Agreement on written notice. This goes beyond the playbook's baseline and affords meaningful protection.

A secondary assignment provision appears in the User Terms of Service (Doc 1), which governs individual authorized users rather than the Customer organization. That provision follows the same bilateral structure. Since it applies to a different contractual relationship (Slack !" end users), it does not compete with or supersede MSA § 12.8 for purposes of this playbook item.

Overall: MSA § 12.8 meets the acceptable position on both limbs of the playbook item. Classification is GREEN. No ideal preference was specified, so aiPreferenceMet is false. Item weight is Acceptable to Deviate; a GREEN finding at this weight is informational and requires no documented justification.

— Note —
The AI cited 2 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "Neither party may assign any of its rights or obligations hereunder, whether by operation of law or otherwise, without the other party's prior written consent (not to be unreasonably withheld); provid…"
2. "You may not assign any of your rights or delegate your obligations under these User Terms, including the Acceptable Use Policy, whether by operation of law or otherwise, without the prior written cons…"

Cyber Risk Insurance

AI Comment: The playbook item requires the vendor to maintain cyber risk insurance covering first-party and third-party losses, with a stated ideal preference for coverage of not less than $5M, customer named as additional insured, and a waiver of subrogation. After a comprehensive review of all nine provided documents — the User Terms of Service, Privacy Policy, Acceptable Use Policy, Salesforce Main Services Agreement (MSA), Slack Supplemental Terms, Data Processing Addendum (landing page and full executed document), Security Privacy and Architecture Report, and Slack Privacy Principles — no language addressing cyber risk insurance, general liability insurance, or any insurance obligation whatsoever was identified. The contract is entirely silent.

Under the silence-handling framework: this is a Medium weight item, so the default classification upon silence is YELLOW.

Statutory/regulatory mitigation was evaluated: no statute under California law (the most probable governing jurisdiction for a US-domiciled customer) or federal law mandates that a SaaS vendor contractually commit to maintaining minimum cyber insurance coverage in favor of its customers. CCPA/CPRA imposes data-handling obligations but does not require insurance. No statutory downgrade applies.

Industry-norm mitigation was also evaluated: it is well-established market practice that standard, publicly available SaaS vendor terms — including enterprise-grade platforms like Slack/Salesforce — do not include insurance obligations in their public-facing contract documents. Such provisions, if obtained, are typically the product of bespoke enterprise negotiation and appear in custom schedules or side letters. However, while the absence of insurance language in standard terms is a recognized norm, the practical risk is not trivially low: without a contractual commitment, the customer (a) cannot verify that coverage exists or is maintained throughout the term, (b) cannot enforce any minimum coverage amount, (c) cannot obtain additional insured status, and (d) cannot obtain a waiver of subrogation. These are legally material gaps that limit the customer's remediation options following a vendor-side security incident. Accordingly, the industry-norm downgrade from YELLOW to GREEN is not applied.

Classification remains YELLOW. The acceptable position (vendor maintains cyber risk insurance for first- and third-party losses) is not satisfied because there is no contractual evidence whatsoever. The ideal preference ($5M minimum, additional insured, waiver of subrogation) is correspondingly unmet. If contractual assurance is required, the customer should negotiate a custom enterprise agreement incorporating express insurance obligations, or submit a vendor questionnaire seeking written confirmation of coverage levels.

Warranty & Remedy

AI Comment: The Salesforce MSA (applicable to Slack per the Slack Main Services Agreement and Supplemental Terms) expressly satisfies both limbs of the playbook's acceptable position. First, §8.2(c) warrants that "the Services will perform materially in accordance with the applicable Documentation," directly matching the requirement. Second, the MSA provides a structured remedy pathway that is functionally equivalent to "if Vendor cannot repair or replace at no cost, we receive a pro-rata refund": §8.2 designates termination and refund as the exclusive remedies for warranty breach; §11.3 affords a 30-day cure period before Customer may terminate (functioning as the repair/replace opportunity, at no cost to Customer); and §11.4 provides that upon Customer-initiated termination for cause, SFDC refunds all prepaid fees covering the remainder of the subscription term — the pro-rata refund the playbook requires. The "exclusive remedy" label in §8.2 is a noted limitation — it forecloses breach-period damages and broader common-law claims — but does not remove the specific protections the playbook requires. The general implied-warranty disclaimer in §8.3 is explicitly subject to its own opening carve-out ("EXCEPT AS EXPRESSLY PROVIDED HEREIN"), which preserves the §8.2 express warranty. Note: Free Trial and Free Services are expressly excluded from the warranty (§§2.6, 2.7); for a standard paid subscription this carve-out does not apply. At Acceptable to Deviate weight, and with all playbook-required protections present, the overall classification is GREEN.

— Superseding reasoning —
MSA §8.2 contains an express performance warranty. MSA §8.3 contains a general disclaimer of all warranties, but §8.3 opens with "EXCEPT AS EXPRESSLY PROVIDED HEREIN," explicitly carving out express contractual provisions such as §8.2. Because §8.2 is an express provision, it survives §8.3 by operation of the carve-out language. The specific express warranty in §8.2(c) governs and is not negated by the general disclaimer in §8.3.

— Note —
The AI cited 4 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "SFDC warrants that during an applicable subscription term (a) this Agreement, the Order Forms and the Documentation

will accurately describe the applicable administrative, physical, and technical safe…"
2. "For any breach of a warranty above, Customer's exclusive remedies are those described in the "Termination" and "Refund or Payment upon Termination" sections below."
3. "A party may terminate this Agreement for cause (i) upon 30 days written notice to the other party of a material breach if such breach remains uncured at the expiration of such period, or (ii) if the o…"
4. "If this Agreement is terminated by Customer in accordance with the "Termination" section above, SFDC will refund Customer any prepaid fees covering the remainder of the term of all Order Forms after t…"

> *"EXCEPT AS EXPRESSLY PROVIDED HEREIN, NEITHER PARTY MAKES ANY WARRANTY OF ANY*
>
> *KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, AND EACH PARTY SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW."*
> — https://www.salesforce.com/en-us/wp-content/uploads/sites/4/documents/legal/salesforce_MSA.pdf

Automatic Renewal

AI Comment: The acceptable position requires: (1) automatic renewal disclosed, (2) at least 30 days' prior notice before the renewal date, and (3) a right to cancel before renewal. The Salesforce Main Services Agreement (MSA), Section 11.2, directly and explicitly satisfies all three requirements. Subscriptions auto-renew for one-year terms; either party may prevent renewal by providing written notice (email acceptable) at least 30 days before the end of the subscription term. The 30-day notice period exactly meets the "at least 30 days" threshold in the acceptable position, and the mutual right to cancel is unambiguously preserved for both parties.

One structural caveat worth noting: the renewal provision opens with "Except as otherwise specified in an Order Form," meaning a custom Order Form could theoretically override the 30-day notice period. For a standard online Slack purchase governed by the Slack Supplemental Terms + MSA, no deviating Order Form is expected; the default terms analyzed here govern. A bespoke enterprise Order Form should be checked separately if executed.

Additionally, Section 11.2 contains a renewal pricing note — promotional or one-time priced subscriptions renew at list price, and any reduction in subscription volume or length at renewal triggers re-pricing — which is out of scope for this playbook item but may be relevant to a separate pricing/commercial review.

No ideal preference was specified for this item; GREEN reflects that the acceptable threshold is met. aiPreferenceMet is set to false accordingly.

— Note —
The AI cited 1 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "Except as otherwise specified in an Order Form, subscriptions will automatically renew for additional one year terms, unless either party gives the other written notice (email acceptable) at least 30 …"

Restrictions on Use

AI Comment: The playbook item requires that use restrictions must not prohibit the intended use (team chat for a standard US-domiciled organization) and that standard acceptable-use restrictions are acceptable; the ideal preference is no restrictions beyond a single standard AUP.

Primary Restriction Framework — MSA §3.4: The most operative restriction clause across the document set appears in MSA §3.4. Its ten enumerated prohibitions cover: no unauthorized access sharing beyond Customer/Users, no resale or sublicensing, no storage/transmission of infringing or malicious content, no service disruption, no unauthorized system access, no circumvention of usage limits, no derivative works, no benchmarking for competitive intelligence, and no reverse engineering. Every one of these is a standard, industry-normal SaaS acceptable-use restriction. None of them would restrict a team using Slack for workplace messaging and collaboration — the platform's core designed purpose. The MSA preamble adds a specific anti-benchmarking clause and a direct-competitor prohibition. Both are standard SaaS vendor protections, inapplicable to a standard team chat Customer that is not an SFDC competitor.

AUP Reference Gap — Material Verification Risk: MSA §3.3 requires Customer compliance with two externally hosted policy documents: the Salesforce "Acceptable Use and External Facing Services Policy" and a separate "Artificial Intelligence Acceptable Use Policy," both linked by URL but not included in this document set. The Slack AUP page (Document 3) confirms the operative AUP is the same Salesforce-hosted PDF, and provides no independent AUP terms. This creates a verification gap: the full operative AUP content cannot be confirmed from the materials provided. Based on industry norms for workplace collaboration SaaS, these policies would be expected to prohibit content misuse, spam, illegal activity, and similar standard categories — none of which would affect team chat use. However, this gap prevents a full verification and warrants independent review of the external PDF before closing the assessment. The dual-policy requirement (one standard AUP plus a separate AI AUP) also technically exceeds the ideal preference for "no restrictions beyond a standard acceptable-use policy."

AI/ML Data Processing Provision: The Supplemental Terms grant SFDC default rights to use Customer Data for model training and service improvement (with opt-out available per the Privacy Principles). This is a data processing/licensing provision, not a restriction on the Customer's use of the service for team chat. It is more appropriately evaluated under a "Data Use / AI Training" playbook item. Noted here for completeness; it does not affect the classification of this item.

Sensitive Data Restrictions: The Security/Privacy/Architecture documentation prohibits submission of PHI, payment

cardholder data, CJI, and similar regulated data types to the covered services. These are standard compliance-posture restrictions reflecting Slack's certification boundaries and would not apply to a standard team chat deployment that does not process these categories.

Document Hierarchy: Per MSA §12.3 (Order Form > MSA > Documentation) and Supplemental Terms §7-6 ("the MSA takes precedence over the Documentation"), the MSA §3.4 restriction list is the highest-authority restriction provision in the document set. The sensitive data restrictions in the Security document are Documentation-level and subordinate to the MSA.

Classification Rationale: The acceptable position is met — all documented restrictions are standard and none prohibit or materially limit team chat use. The ideal preference is not met because: (1) the Customer must comply with two separate external AUP-type documents (standard AUP + AI AUP) rather than a single standard AUP; (2) the Supplemental Terms add an AI/ML data processing obligation; and (3) the full AUP text is unverified. Confidence is MODERATE rather than HIGH solely due to the external AUP verification gap — reviewers should independently obtain and review the Salesforce External Facing Services Policy PDF to close this gap.

— Note —
The AI cited 3 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "Customer will not (a) make any Service available to anyone other than Customer or Users, or use any Service for the benefit of anyone other than Customer or its Affiliates, unless expressly stated oth…"
2. "The Services may not be accessed for purposes of monitoring their availability, performance or functionality, or for any other benchmarking or competitive purposes.

SFDC's direct competitors are proh…"
3. "Customer will (a) be responsible for Users' compliance with this Agreement, Documentation and Order Forms, (b) be responsible for the accuracy, quality and legality of Customer Data, the means by whic…"

> *"The Acceptable Use Policy (AUP) sets out a list of acceptable and unacceptable conduct for our Services."*
> — Acceptable Use Policy | Legal | Slack
> *"SFDC may access Customer Data in Slack for the following reasons, and Customer instructs SFDC to process its Customer Data for such purposes:*
>
> *1. to train models for use by the services and features that Customer has access to;*
> *2. to improve services and features that Customer has access to;*
> *3. to conduct research and development of products that Customer will have access to without additional cost;*
> *4. as otherwise provided in the MSA between SFDC and Customer."*
> — Slack Supplemental Terms | Legal | Slack
> *"If a Customer is a health care provider, health care clearinghouse, health plan, or an entity performing functions on behalf of such entities, submitting personal health data is prohibited, except in limited circumstances where, subject to restrictions, Salesforce has expressly permitted such submission."*
> — Security, Privacy and Architecture Report
> *"While You Are Here, You Must Follow the Rules"*
> — User Terms of Service | Legal | Slack

Indemnification – Vendor to Our Company

AI Comment: The playbook item requires vendor indemnification covering two distinct obligations: (1) intellectual property infringement claims and (2) data breaches. Analysis across all documents reveals a split picture.

IP INFRINGEMENT INDEMNIFICATION — PRESENT WITH CONDITIONS (YELLOW): The Salesforce MSA Section 9.1 expressly provides IP indemnification for Purchased Services. SFDC will defend and indemnify Customer against third-party claims alleging that any Purchased Service infringes or misappropriates intellectual property rights. Four exclusions limit this obligation: (I) allegations must specifically identify the Services as the basis; (II) combination claims (where infringement results from integrating Slack with non-SFDC tools — practically significant given Slack's extensive third-party integration ecosystem); (III) free/no-charge services are excluded entirely; (IV) claims from Non-SFDC Applications or Customer's own breach are excluded. Additionally, MSA Section 9.3 designates the indemnification section as Customer's exclusive remedy for covered third-party IP claims, limiting recourse to what Section 9 provides. These are largely market-standard carve-outs, but exclusion (II) is particularly notable for a team chat deployment where integrations are common, and exclusion (III) is relevant if the organization uses the free Slack tier.

DATA BREACH INDEMNIFICATION — ABSENT (GAP): No provision across any document — MSA, DPA, Slack Supplemental Terms, Security Report, or Privacy Policy — provides indemnification for third-party claims arising from a data breach. The DPA Section 7 addresses data breach response through notification ("without undue delay") and SFDC's obligation to make "reasonable efforts to remediate," but these are operational obligations, not indemnification. There is no commitment by SFDC to defend Customer or indemnify Customer's losses arising from third-party claims attributable to a breach of Customer Data. DPA Section 11 further confirms this gap by expressly subjecting all DPA-related liability to the MSA's aggregate liability cap (12 months' fees paid), with no carve-out for data breach indemnification claims. Even the MSA Section 8.2 security warranty — under which SFDC commits not to materially decrease overall security — provides only termination and refund as remedies for breach, not indemnification against third-party claims.

OVERALL: Because the playbook requires both IP and data breach indemnification, and only the IP component is addressed (albeit with meaningful exclusions), the overall classification is YELLOW. The data breach indemnification gap is a material deficiency relative to the stated acceptable position. Under California governing law (applicable for a US-domiciled team), no statute fills the data breach indemnification gap — this is a purely contractual obligation that must be

negotiated. Weight is Medium.

— Note —
The AI cited 5 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "SFDC will defend Customer against any claim, demand, suit or proceeding made or brought against Customer by a third party alleging that any Purchased Service infringes or misappropriates such third pa…"
2. "The above defense and indemnification obligations do not apply if (I) the allegation does not state with specificity that the Services are the basis of the Claim Against Customer; (II) a Claim Against…"
3. "This "Mutual Indemnification" section states the indemnifying party's sole liability to, and the indemnified party's exclusive remedy against, the other party for any third-party claim described in th…"
4. "SFDC maintains security incident management policies and procedures specified in the Security, Privacy and Architecture Documentation and shall notify Customer without undue delay after becoming aware…"
5. "Each party's and all of its Affiliates' liability, taken together in the aggregate, arising out of or related to this DPA, and all DPAs between Authorized Affiliates and SFDC, whether in contract, tor…"

License Grant – Vendor to Our Company

AI Comment: The Slack/SFDC agreement documents do not contain a standalone, explicit license grant clause from SFDC to Customer. Access rights are instead conferred through three overlapping mechanisms: (1) SFDC's contractual obligation to "make the Services available to Customer" (MSA §2.1), (2) the subscription model defining who constitutes an authorized "User" (MSA §3.1 and §1 definitions), and (3) the usage restriction in §3.4(a), which negatively defines the bounds of permitted access. While this service-provision framing is consistent with standard enterprise SaaS practice and functionally confers access rights, it falls short of the clarity and enforceability provided by a dedicated license grant article that affirmatively states scope, permitted use, and sublicense rights. The reservation clause in §6.1 confirms the gap: "No rights are granted to Customer hereunder other than as expressly set forth herein," but no provision expressly grants a license with defined scope.

For the intended use (team chat / workplace productivity), the functional access is adequate. Slack is explicitly described as an "online workplace productivity tools and platform," squarely covering the stated deployment purpose. The User definition is broad, covering employees, contractors, consultants, and third-party business partners — sufficient for all ordinary team chat participants.

Affiliate coverage is the primary substantive gap. The MSA defines "Customer" to include Affiliates, but only those that have separately executed Order Forms. The usage restriction in §3.4(a) further distinguishes between direct access (limited to "Customer or Users") and benefit use (extended to "Customer or its Affiliates"). Affiliate employees wishing to access the service as Users must therefore be covered by a separate Affiliate-level Order Form. Automatic affiliate inclusion without additional contracting steps is not provided — a meaningful limitation against the playbook's acceptable position.

The usage restrictions in §3.4(b)–(j) are standard SaaS prohibitions (no sublicensing, no resale, no benchmarking, no reverse engineering, no competitive use). None of these defeat the purpose of a team chat deployment for a standard US-domiciled team.

A material asymmetry in the license framework is created by the Slack Supplemental Terms' AI/ML provision, which grants SFDC broad rights to access Customer Data for model training, service improvement, and R&D — a significant reverse obligation that is default-active (subject to an opt-out for global models and an opt-in for generative AI training). While this is primarily a data-use rights issue and not a direct license from SFDC to Customer, it is a material condition embedded in the licensing relationship.

Overall classification: YELLOW. Access rights for the intended use and user base are functionally present but lack an explicit license grant article; affiliate access is conditional on separate Order Form execution rather than automatic; and the AI/ML data-use obligation imposes a significant default condition on the licensing arrangement.

— Note —
The AI cited 5 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "SFDC will (a) make the Services available to Customer pursuant to this Agreement, and the applicable Order Forms and Documentation, (b) provide applicable SFDC standard support for the Purchased Servi…"
2. "Subject to the limited rights expressly granted hereunder, SFDC, its Affiliates, and its licensors reserve all of their right, title and interest in and to the Services, including all of their related…"
3. ""User" means, in the case of an individual accepting these terms on his or her own behalf, such individual, or, in the case of an individual accepting this Agreement on behalf of a company or other le…"
4. ""Customer" means in the case of an individual accepting this Agreement on his or her own behalf, such individual, or in the case of an individual accepting this Agreement on behalf of a company or oth…"
5. "Customer will not (a) make any Service available to anyone other than Customer or Users, or use any Service for the benefit of anyone other than Customer or its Affiliates, unless expressly stated oth…"

> *"SFDC may access Customer Data in Slack for the following reasons, and Customer instructs SFDC to process its Customer Data for such purposes:*
>
> *1. to train models for use by the services and features that Customer has access to;*
> *2. to improve services and features that Customer has access to;*
> *3. to conduct research and development of products that Customer will have access to without additional cost;*

4. as otherwise provided in the MSA between SFDC and Customer."
— Slack Supplemental Terms | Legal | Slack

Exclusivity

AI Comment: Comprehensive review of all provided documents — User Terms of Service, Privacy Policy, Acceptable Use Policy, Main Services Agreement (MSA), Slack Supplemental Terms, Data Processing Addendum, Security/Privacy/Architecture Report, and Privacy Principles — reveals no exclusivity clause of any kind that would bind the Customer to use Slack or any Salesforce/SFDC service as its sole or exclusive provider of team collaboration services. The contract documents are silent on the topic of exclusivity.

The acceptable position for this High-weight item is that the Customer must not be required to accept any exclusivity restriction. That position is met. Under controlling California law (the most probable governing jurisdiction for a US-domiciled customer, per the Slack Supplemental Terms governing law table) and foundational contract principles, no exclusivity obligation may be implied from a contract's silence alone — a party is bound only by express agreement. The absence of any exclusivity clause is therefore dispositive: the Customer is contractually free to use competing or parallel collaboration tools simultaneously with Slack.

Two tangentially related restrictions were identified in the MSA preamble and examined for exclusivity implications. First, the MSA prohibits using the Services for competitive benchmarking or performance monitoring purposes. This is a narrow use-restriction on the Services themselves — it prevents the Customer from leveraging Slack as an instrument for competitor analysis — but it says nothing about the Customer's freedom to engage or contract with competing vendors. Second, the MSA bars SFDC's own direct competitors from accessing the Services as customers. This is an eligibility restriction on who may become an SFDC customer, not an obligation imposed on this Customer regarding its purchasing decisions. Neither provision constitutes an exclusive dealing or exclusivity requirement.

On the silence-default framework: the standard High-weight silence default (RED) is calibrated for playbook items where the absence of protective language exposes the Customer to risk. This item inverts that logic — it asks whether an unwanted obligation is present. When the contract is silent on exclusivity, there is no exclusivity obligation, which is exactly what the acceptable position requires. Applying the RED default here would produce a materially misleading result. Industry norm further reinforces this: SaaS vendors characteristically do not impose exclusive dealing obligations on customers, making the absence of such a clause entirely standard market practice and carrying negligible practical risk. The classification is GREEN on that basis.

— Applied silence standard —
Basis: INDUSTRY_NORM
Citation: It is standard SaaS market practice for vendors not to impose exclusive dealing or exclusive purchasing obligations on customers. The absence of an exclusivity clause in a SaaS agreement carries negligible practical risk because, under California contract law (the governing jurisdiction for US-domiciled customers), no exclusivity obligation can be implied from silence — the Customer is free to engage competing services without contractual consequence.

— Note —
The AI cited 1 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "SFDC's direct competitors are prohibited from accessing the Services, except with SFDC's prior written consent."
"The Services may not be accessed for purposes of monitoring their availability, performance or functionality, or for any other benchmarking or competitive purposes."
— https://www.salesforce.com/en-us/wp-content/uploads/sites/4/documents/legal/salesforce_MSA.pdf

Non-Solicitation of Employees

AI Comment: All documents in the Slack/Salesforce contract set — the Salesforce MSA, Slack Supplemental Terms, User Terms of Service, Privacy Policy, Acceptable Use Policy, Data Processing Addendum (both the landing page and executed document), and Security/Privacy Architecture Report — are entirely silent on non-solicitation of employees. No provision in any document restricts either party from soliciting or hiring the other's employees.

The acceptable position for this playbook item requires that any non-solicitation restriction at minimum disclaim instances where applicants respond to general public postings. The ideal preference is stronger: no limitations on solicitation whatsoever, plus an explicit disclaimer for recruiter referrals.

This is a case where contractual silence is unambiguously and affirmatively favorable to the Customer. Because no non-solicitation covenant exists anywhere in the document set, the Customer faces zero solicitation restrictions — an outcome that fully satisfies both the acceptable position and the ideal preference. There is nothing to carve out, because there is no restriction from which a carve-out would be needed.

Regarding the second element of the preference — "disclaim recruiter referrals" — this language contemplates an explicit carve-out within an otherwise existing non-solicitation clause. Because no such clause exists, the recruiter referral element is not applicable but is satisfied a fortiori: recruiter-sourced hires are entirely unrestricted. The practical protection achieved by silence is broader than any explicit disclaimer would provide.

The closest section in which non-solicitation language would conventionally appear in a SaaS MSA is the Relationship of the Parties provision (MSA §12.4). A review of that section confirms it addresses only independent contractor status and allocation of employment taxes, without any non-solicitation covenant. No other section of any document in the set contains responsive language.

Classification: GREEN with preference met. Confidence: HIGH — the absence of any non-solicitation provision across the full document set is clear and unambiguous.

— Note —
The AI cited 1 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "The parties are independent contractors. This Agreement does not create a partnership, franchise, joint venture, agency, fiduciary or employment relationship between the parties. Each party will be so…"

Subprocessor Audit Rights

AI Comment: The DPA (Document 6) directly addresses sub-processor compliance oversight, but does not grant the Customer a direct right to audit third-party sub-processors' own systems. The playbook item requires "the right to audit Subprocessor's systems and compliance with DPA." The DPA addresses this through a layered but indirect and qualified mechanism: (1) Under §6.3.1, SFDC makes available to Customer reports of SFDC's own audits of third-party sub-processors and any third-party auditor reports those sub-processors have provided, but this access is conditional — "to the extent such reports or evidence may be shared with Customer." §6.3.1 further notes that such reports are confidential information of the sub-processor, and certain sub-processors may require the Customer to sign an NDA before viewing them. (2) Under §6.3.2 and §6.3.3, the on-site audit right is available to the Customer but is explicitly "limited to Customer Data Processing and storage facilities operated by SFDC or any of SFDC's Affiliates" — third-party sub-processors are therefore expressly excluded from the on-site audit scope. Significant mitigating protections are present: §5.1 requires SFDC to bind each sub-processor by a written agreement with data protection obligations no less protective than those in the Agreement, and §5.4 makes SFDC fully liable for sub-processor acts and omissions as if SFDC had performed those services directly. These provisions reduce the practical risk of the audit gap but do not satisfy the playbook requirement for a direct audit right over sub-processors. The indirect report-sharing mechanism is a common large-scale SaaS/cloud industry pattern, but it represents materially weaker protection than a contractual right to audit sub-processors' own systems. Classification YELLOW for Medium weight: the topic is substantively addressed with real but incomplete protections — the acceptable position (direct sub-processor audit right) is not met.

— Note —
The AI cited 3 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "SFDC shall be liable for the acts and omissions of its Sub-processors to the same extent SFDC would be liable if performing the services of each Sub-processor directly under the terms of this DPA, unl…"
2. "(ii) provide Customer with a report and/or confirmation of SFDC\'s audits of third-party Sub-processors\' compliance with the data protection controls set forth in this DPA and/or a report of third-pa…"
3. "Any On-Site Audits will be limited to Customer Data Processing and storage facilities operated by SFDC or any of SFDC\'s Affiliates."

> *"SFDC or an SFDC Affiliate has entered into a written agreement with each Sub-processor containing, in substance, data protection obligations no less protective than those in the Agreement with respect to the protection of Personal Data to the extent applicable to the nature of the Services provided by such Sub-processor."*
> — Data Processing Addendum

Encryption in Transit

AI Comment: The document set broadly addresses data security during transmission but does not, in any document, explicitly commit to TLS 1.2 or higher — nor to any specific transport encryption protocol or version. This is the central gap relative to the playbook item's acceptable position.

The Security, Privacy and Architecture Report (SPARC — Document 9) is the governing document for specific security implementation details: both the MSA (§ 2.2: "as described in the Documentation") and the DPA (§ 6.1: "as set forth in the Security, Privacy and Architecture Documentation") expressly delegate to it. The SPARC commits Salesforce to "appropriate technical and organizational measures to protect… Customer Data… processed or transmitted through the Covered Services" and states that "at a minimum, Salesforce will align with prevailing industry standards such as ISO 27001, ISO 27002, and ISO 27018." ISO 27002 (control 8.24 in the 2022 edition) does encompass cryptographic controls for data in transit, and the Privacy Policy's reference to "current state of technology" is directionally consistent with the playbook's "then-current industry-standard" language. These provisions together indicate that industry-standard transport encryption is very likely deployed in practice — but they do not constitute a specific, enforceable contractual commitment to TLS 1.2+.

This falls short of the playbook's acceptable position for two reasons: (1) "appropriate measures" and ISO standards alignment are principles-based, leaving the specific version to Salesforce's discretion without a floor; and (2) there is no verification mechanism or contractual floor for the minimum TLS version. This is a YELLOW, not a RED: the topic is substantively addressed across multiple documents, and the ISO 27002 / "current state of technology" language provides meaningful (if indirect) coverage. The gap is specificity and enforceability, not complete absence.

For a High-weight item, this warrants documented review. The recommended remediation path is to obtain written confirmation from Slack/Salesforce of their current transport encryption standard (Slack's public-facing documentation commonly references TLS 1.2+, but that representation is not captured in the contractual documents provided here) and confirm whether that commitment can be incorporated into an Order Form addendum or supplemental security exhibit.

— Superseding reasoning —
Both the MSA (§ 2.2) and the DPA (§ 6.1) contain general security safeguard language but expressly defer to the Security, Privacy and Architecture Documentation (SPARC) for the specific details of those safeguards. The SPARC is therefore the

governing document for transport security specifics and supersedes the general provisions in the MSA and DPA. Within the SPARC, the "Security Controls" section — providing the "appropriate technical and organizational measures" commitment for transmitted data alongside the ISO 27001/27002/27018 alignment standard — constitutes the controlling security language after applying this hierarchy. The Privacy Policy (PIF 4) is not superseded: it operates in a parallel, distinct scope (applying to "Other Information," i.e., non-Customer Data) and is not in conflict with the SPARC framework.

— Note —
The AI cited 1 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "SFDC shall maintain appropriate technical and organizational measures for protection of the security (including protection against unauthorized or unlawful Processing and against accidental or unlawfu…"

> *"Security Controls"*
> — Security, Privacy and Architecture Report
> *"At a minimum, Salesforce will align with prevailing industry standards such as ISO 27001, ISO 27002, and ISO 27018."*
> — Security, Privacy and Architecture Report
> *"SFDC will maintain appropriate administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of Customer Data, as described in the Documentation. Those safeguards will include, but will not be limited to, measures designed to prevent unauthorized access to or disclosure of Customer Data (other than by Customer or Users)."*
> — https://www.salesforce.com/en-us/wp-content/uploads/sites/4/documents/legal/salesforce_MSA.pdf
> *"Slack works hard to protect Information you provide from loss, misuse, and unauthorized access or disclosure. These steps take into account the sensitivity of the Information we collect, process and store, and the current state of technology."*
> — Privacy Policy | Legal | Slack

Indemnification – Our Company to Vendor

AI Comment: The governing indemnification-by-Customer provision is MSA § 9.2. It imposes three distinct triggers for Customer's obligation to defend and indemnify SFDC, and they do not map entirely to the acceptable position.

Trigger mapping against the acceptable position ("third-party claims arising from our content or our misuse of the services"):

• § 9.2(b)(ii) — "any Customer Data or Customer's use of Customer Data with the Services" — maps squarely to "our content." '
• § 9.2(b)(i) — "Customer's use of the Services in an unlawful manner or in violation of the Agreement, the Documentation, or Order Form" — maps squarely to "our misuse of the services." '
• § 9.2(a) — third-party IP infringement claims arising from "the combination of a Non-SFDC Application or configuration provided by Customer and used with the Services" — does NOT map to "our content or our misuse." This trigger activates when Customer-introduced integrations or configurations, combined with Slack, give rise to an IP claim, even if Customer's use of Slack itself was fully compliant. & þ
• § 9.2(b)(iii) — "a Non-SFDC Application provided by Customer" — similarly does NOT map to "our content or our misuse." This covers Customer-introduced third-party apps as a standalone category, distinct from Customer Data. & þ

The Non-SFDC Application triggers (§ 9.2(a) and § 9.2(b)(iii)) expand the indemnification obligation beyond the acceptable position. For a team chat deployment, this exposure is practically significant if the Customer enables third-party Slack integrations (bots, workflow apps, etc.) — a common configuration.

Mitigating factors: (1) The obligation is limited to third-party claims only (no direct/first-party claim obligation). (2) § 9.3's exclusive remedy clause confirms the indemnification is bounded and non-open-ended. (3) § 9.2's final sentence carves out claims arising from SFDC's own breach. (4) The EU Data Act switching/deletion indemnification (MSA § 12.18) is expressly scoped to EU/EEA-domiciled customers and is inapplicable to this US (California) deployment.

Conclusion — YELLOW: The indemnification obligation is addressed and limited to third-party claims, but its scope exceeds the acceptable position by including Non-SFDC Application and configuration-combination triggers. The preference (no indemnification at all) is not met. Weight is Medium, yielding a low-priority review per the risk matrix.

— Note —
The AI cited 4 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "Customer will defend SFDC and its Affiliates against any claim, demand, suit or proceeding made or brought against SFDC by a third party (a) alleging that the combination of a Non-SFDC Application or …"
2. "The above defense and indemnification obligations do not apply if a Claim Against SFDC arises from SFDC's breach of this Agreement, the Documentation or applicable Order Forms."
3. "This "Mutual Indemnification" section states the indemnifying party's sole liability to, and the indemnified party's exclusive remedy against, the other party for any third-party claim described in th…"
4. "Customer will defend SFDC and its Affiliates against any claim, demand, suit or proceeding made or brought against SFDC by Impacted Parties (a) alleging that the Switching or Deletion Request infringe…"

Payment Terms

AI Comment: The Salesforce MSA—which governs Slack under the Slack Terms (MSA + Slack Supplemental Terms)—expressly addresses both payment modalities contemplated by the playbook item.

Invoiced (non-credit-card) payments: MSA § 5.2 provides "invoiced fees are due net 30 days from the invoice date," meeting the playbook's acceptable position of at least 30 days to pay from receipt of invoice. A minor textual distinction exists between "invoice date" (contract language) and "receipt of invoice" (playbook language); however, for a SaaS platform like Slack where invoices are delivered electronically, issuance and receipt are functionally contemporaneous. This distinction is not material and does not degrade the classification.

Credit card autopay: MSA § 5.2 provides that credit card charges "shall be made in advance, either annually or in accordance with any different billing frequency stated in the applicable Order Form." This constitutes an autopay arrangement where charges are processed at or before the start of a billing period — effectively less than 30 days. The playbook explicitly carves out credit card autopay as acceptable even when the payment window is shorter than 30 days. This provision therefore also satisfies the acceptable position.

Additional favorable provisions: § 5.4 contextually confirms the 30-day invoiced-payment window by setting the overdue trigger at "30 days or more overdue" for standard accounts, consistent with the net-30 term. § 5.5 further protects customers by suspending Slack's enforcement rights (overdue charges, suspension of service, acceleration) while a customer is disputing applicable charges in good faith — preserving the practical payment window during genuine billing disputes.

Qualifier note: The "Unless otherwise stated in the Order Form" qualifier in § 5.2 is standard commercial drafting. Any Order Form deviation would be mutually negotiated between the parties and does not constitute a unilateral gap against the playbook's acceptable position.

Jurisdictional note: For a US/Canada-domiciled customer (most probable per the intake brief), governing law is California per the Slack Supplemental Terms. Country-specific payment term replacements (Italy: § 12.14; India: § 12.16.2) are not applicable. Standard § 5.2 controls and is fully enforceable under California law.

Ideal preference: No ideal preference was specified in the Review Specific Playbook, so aiPreferenceMet is set to false — this reflects the absence of a stated ideal, not a shortfall in vendor terms.

— Note —
The AI cited 3 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "If Customer provides credit card information to SFDC, Customer authorizes SFDC to charge such credit card for all Purchased Services listed in the Order Form for the initial subscription term and any …"
2. "If any charge owing by Customer under this or any other agreement for services is 30 days or more overdue, (or 10 or more days overdue in the case of amounts Customer has authorized SFDC to charge to …"
3. "SFDC will not exercise its rights under the "Overdue Charges" or "Suspension of Service and Acceleration" section above if Customer is disputing the applicable charges reasonably and in good faith and…"

> *"Unless otherwise stated in the Order Form, invoiced fees are due net 30 days from the invoice date."*
> — https://www.salesforce.com/en-us/wp-content/uploads/sites/4/documents/legal/salesforce_MSA.pdf

Data Protection Officer (DPO)

AI Comment: The playbook item requires either (a) a designated Data Protection Officer or (b) a named privacy point of contact with sufficient qualifications (acceptable threshold), with the ideal preference being a qualified DPO designation. Three distinct references across two documents collectively satisfy both thresholds.

First, the Privacy Policy contains a dedicated "Data Protection Officer" section that explicitly acknowledges the DPO role and provides a dedicated contact channel at dpo@slack.com — confirming the existence of the role, though without naming the incumbent.

Second, DPA Section 4.2 elevates this: it confirms that "Members of the SFDC Group" — a defined term expressly including Slack Technologies, LLC and Slack Technologies Limited (per the SFDC entity list in the DPA definitions) — have appointed a DPO, reachable at privacy@salesforce.com.

Third, and most specifically, DPA Schedule 2 names Lindsey Finch as DPO with direct contact details (privacy@salesforce.com). While this designation is formally listed in the Schedule in the data-importer capacity of Salesforce, Inc., it represents the named group-level DPO whose appointment covers the SFDC Group under Section 4.2.

Taken together: (1) a DPO is explicitly designated across the SFDC Group including the Slack entities; (2) a named individual with DPO title is identified in the executed DPA; and (3) a dedicated Slack DPO contact email (dpo@slack.com) is provided in the public-facing Privacy Policy. This exceeds the acceptable threshold (DPO or named privacy POC) and satisfies the ideal preference (qualified DPO). Classification: GREEN, aiPreferenceMet = true.

One minor observation for the reviewer's awareness: the Privacy Policy (dpo@slack.com) and the DPA Schedule 2 (privacy@salesforce.com) use different contact addresses. This reflects the group structure rather than a conflict — the Slack-branded DPO email routes to the same DPO function. No reclassification is warranted, but the team may wish to confirm routing.

— Note —
The AI cited 2 finding(s) whose source text could not be located in the document. The findings were discarded; review the quoted text below against the source manually.
1. "Members of the SFDC Group have appointed a data protection officer. The appointed person may be reached at privacy@salesforce.com."
2. "Contact person's name, position and contact details: Lindsey Finch, DPO, privacy@salesforce.com"

> *"Data Protection Officer](https://slack.com/trust/privacy/privacy-policy#dpo)"*
> — Privacy Policy | Legal | Slack

Documents

Title	URL	Type	Scraped At	Replaced
User Terms of Service | Legal | Slack	https://slack.com/terms-of-service/user	text/markdown	2026-07-14T09:18:31.147Z	No
Privacy Policy | Legal | Slack	https://slack.com/privacy-policy	text/markdown	2026-07-14T09:18:38.015Z	No
Acceptable Use Policy | Legal | Slack	https://slack.com/acceptable-use-policy	text/markdown	2026-07-14T09:18:54.170Z	No
https://www.salesforce.com/en-us/wp-content/uploads/sites/4/documents/legal/salesforce_MSA.pdf	https://salesforce.com/en-us/wp-content/uploads/sites/4/documents/legal/salesforce_MSA.pdf	text/markdown	2026-08-05T15:04:13.039Z	No
Data Processing Addendum | Legal | Slack	https://slack.com/terms-of-service/data-processing	text/markdown	2026-07-14T09:19:50.037Z	No
Data Processing Addendum	https://salesforce.com/content/dam/web/en_us/www/documents/legal/Agreements/data-processing-addendum.pdf	text/markdown	2026-08-05T14:58:42.079Z	No
Slack Supplemental Terms | Legal | Slack	https://slack.com/slack-supplemental-terms	text/markdown	2026-07-14T09:20:09.225Z	No
Main Services Agreement | Legal | Slack	https://slack.com/main-services-agreement	text/markdown	2026-07-14T09:20:42.469Z	No
Security, Privacy and Architecture Report	https://salesforce.com/content/dam/web/en_us/www/documents/legal/misc/slack-security-privacy-and-architecture.pdf	text/markdown	2026-08-05T15:05:26.317Z	No
Slack Privacy Principles	https://slack.com/trust/data-management/privacy-principles	text/markdown	2026-08-05T15:06:50.176Z	No

Beyond-Playbook Findings

None.

Reviewers

Name	Current Step
Acme Tenant Admin	ANALYSIS