# Software Review Report

## Hubspot

*Generated: 2026-07-22T13:07:24.109Z*
*Schema Version: 1.2.0*

## Table of Contents



## Review Summary

**Review ID:** s4raf8ll2b3hmq2d63ni23lq
**Status:** ANALYSIS
**Decision:** Pending
**Created At:** 2026-06-28T18:06:41.506Z
**Submitted At:** Not submitted
**Submitted By:** N/A
**Analysis Completed At:** 2026-06-29T18:37:12.708Z
**General Notes:** None
**Usage Conditions:** None
**AI Jurisdiction:** Location-dependent per Jurisdiction Specific Terms Appendix. Default (North America / South America / unspecified region / Free Services only): Commonwealth of Massachusetts, U.S.A. — exclusive forum: courts of Boston, Massachusetts, U.S.A. & þ  Customer's registered Company Address is the operative trigger; no customer location was provided in the intake brief.
**Human Jurisdiction:** N/A

## Intake Form

**Purpose:** n/a
**Risk Concerns:** n/a
**Review Priorities:** n/a

## Playbook Items

| Name | Category | Weight | AI Color | Human Color |
|---|---|---|---|---|
| Data Segregation | Data: Segregation | HIGH | Needs Review | Unaddressed |
| Compliance Monitoring | Monitoring | HIGH | Needs Review | Unaddressed |
| Retention of our rights to our property | Intellectual Property | HIGH | Aligned | Unaddressed |
| Business Continuity Plan | Misc | ACCEPTABLE_TO_DEVIATE | Needs Review | Unaddressed |
| Termination Obligations | Termination | ACCEPTABLE_TO_DEVIATE | Needs Review | Unaddressed |
| Cyber Risk Insurance | Insurance | HIGH | Needs Review | Unaddressed |
| Statutes (Laws, Regulations, etc.) | Misc | HIGH | Aligned | Unaddressed |
| Insurance | Misc | ACCEPTABLE_TO_DEVIATE | Aligned | Unaddressed |
| Disaster Recovery Testing | Disaster Recovery and BCP | HIGH | Needs Review | Unaddressed |

| Name | Category | Weight | AI Color | Human Color |
|---|---|---|---|---|
| Unauthorized Equipment Prevention | Access:  Equipment | HIGH | Needs Review | Unaddressed |
| Physical Security Controls | Physical Security | HIGH | Aligned | Unaddressed |
| Publicity | Misc | HIGH | At Risk | Unaddressed |
| Password Encryption | Passwords | HIGH | Aligned | Unaddressed |
| Automatic Renewal | Misc | ACCEPTABLE_TO_DEVIATE | Needs Review | Unaddressed |
| Employee Access Control | Access: Employees | HIGH | Aligned | Unaddressed |
| Cybersecurity Prevention Systems | Cybersecurity systems | HIGH | Aligned | Unaddressed |
| Termination for Convenience | Termination | ACCEPTABLE_TO_DEVIATE | At Risk | Unaddressed |
| Authorized Equipment Usage | Access:  Equipment | HIGH | Needs Review | Unaddressed |
| User Authentication Policies | Passwords | HIGH | Aligned | Unaddressed |
| Warranty | Misc | ACCEPTABLE_TO_DEVIATE | Aligned | Unaddressed |
| Data Subject Rights Assistance | Subject Rights | HIGH | Aligned | Unaddressed |
| Assignment | Misc | ACCEPTABLE_TO_DEVIATE | Needs Review | Unaddressed |
| License Grant – Vendor to Our Company | License Grant | HIGH | Needs Review | Unaddressed |
| Our Rights to deliverables | Intellectual Property | HIGH | At Risk | Unaddressed |
| Warranty Breach Remedy | Misc | ACCEPTABLE_TO_DEVIATE | Aligned | Unaddressed |
| Data Protection Officer (DPO) | DPO | HIGH | Needs Review | Unaddressed |
| Our liability | Limitation of Liability | ACCEPTABLE_TO_DEVIATE | Aligned | Unaddressed |
| Payment Terms | Misc | HIGH | Aligned | Unaddressed |
| Anti-Virus Solution | Antivirus | HIGH | Aligned | Unaddressed |
| Data Backup & Restoration | Backup | HIGH | Needs Review | Unaddressed |
| Data Retention & Deletion | Data: Retention | HIGH | At Risk | Unaddressed |
| Employee Offboarding Access | Employee-Offboarding | HIGH | Needs Review | Unaddressed |
| Termination for Cause | Termination | ACCEPTABLE_TO_DEVIATE | Aligned | Unaddressed |
| Exclusivity | Misc | HIGH | Aligned | Unaddressed |
| External Links | Misc | HIGH | At Risk | Unaddressed |
| Employee Confidentiality Agreements | Employee:  Access | HIGH | Needs Review | Unaddressed |
| Need-to-Know Access | Employee: Access | HIGH | Aligned | Unaddressed |
| Non Solicitation of Employees | Misc | HIGH | Aligned | Unaddressed |
| Vendor Audit Rights | Audit of Vendor | HIGH | Needs Review | Unaddressed |
| Data Ownership | Data: Ownership | HIGH | Needs Review | Unaddressed |
| Arbitration or other dispute resolution process | Misc | ACCEPTABLE_TO_DEVIATE | Aligned | Unaddressed |
| Indemnification – Vendor to Our Company | Indemnification | ACCEPTABLE_TO_DEVIATE | Needs Review | Unaddressed |

| Name | Category | Weight | AI Color | Human Color |
|---|---|---|---|---|
| Indemnification – Our Company to Vendor | Indemnification | ACCEPTABLE_TO_DEVIATE | Aligned | Unaddressed |
| Modification of Terms | Misc | HIGH | Aligned | Unaddressed |
| Vendor's liability | Limitation of Liability | HIGH | Needs Review | Unaddressed |
| Background Check Requirements | Misc | ACCEPTABLE_TO_DEVIATE | Aligned | Unaddressed |
| Security Training | Employee: Access | HIGH | Needs Review | Unaddressed |
| Subprocessor Audit Rights | Audit of Subprocessors | HIGH | Needs Review | Unaddressed |
| Vendor Rights | Intellectual Property | HIGH | At Risk | Unaddressed |
| Audit Logging | Audit Log | HIGH | Needs Review | Unaddressed |
| Regulatory Disclosure Procedure | Disclosure-Required | HIGH | Needs Review | Unaddressed |
| Encryption at Rest | Encryption at rest | HIGH | Needs Review | Unaddressed |
| Subprocessor Change Notification | Subprocessor-Change Notice | HIGH | Needs Review | Unaddressed |
| Expenses (travel or otherwise) | Misc | ACCEPTABLE_TO_DEVIATE | Needs Review | Unaddressed |
| Breach Notification Timeline | Breach Notice | HIGH | At Risk | Unaddressed |
| License Grant to Data – Our Company to Vendor | License Grant | HIGH | Aligned | Unaddressed |
| Breach Indemnification | Indemnification | HIGH | At Risk | Unaddressed |
| Processing Limitation | Data Processed | HIGH | Needs Review | Unaddressed |
| Restrictions on Use | Misc | HIGH | Needs Review | Unaddressed |
| Governing Law | Misc | ACCEPTABLE_TO_DEVIATE | Needs Review | Unaddressed |
| Encryption in Transit | Encryption during transmission | HIGH | Aligned | Unaddressed |
| Data Processing Security Policies | Cybersecurity systems | HIGH | Aligned | Unaddressed |
| Subprocessor Agreements | Subprocessor-Agreement | HIGH | Needs Review | Unaddressed |
| Processing Location Restrictions | Location | HIGH | Needs Review | Unaddressed |
| Confidentiality | Misc | HIGH | Needs Review | Unaddressed |

## Data Segregation

**AI Comment:** The playbook item requires physical and/or logical separation of data received from different controllers. A review of all five provided documents — Customer Terms of Service, Product Specific Terms, DPA, AUP, and Privacy Policy — finds no explicit contractual commitment to "data segregation" as a defined security obligation. The most relevant language is concentrated in DPA Annex 2 (Security Measures).

**Physical Separation — Absent.** DPA Annex 2 explicitly states that HubSpot hosts its product infrastructure on "multi-tenant, outsourced infrastructure providers." This affirmatively confirms that data from different controllers shares the same underlying physical infrastructure. No hardware-level isolation between customers exists. The passage noting that "Production servers and client-facing applications are logically and physically secured from our internal corporate information systems" addresses the boundary between HubSpot's production environment and its own internal corporate IT — not the boundary between different customers'/controllers' datasets.

**Logical Separation — Partially Addressed.** Annex 2 describes a permission-based authorization model in which Customer Data is stored in "multi-tenant storage systems" accessible only through application interfaces and APIs. Access is gated by validating user permissions against attributes of each data set, and customers have no direct access to underlying infrastructure. This represents application-layer logical access control that functionally prevents one controller's users from accessing another's data. However, this is framed as an access-control/authorization mechanism, not as a data segregation or logical isolation commitment. The distinction is material: access controls prevent unauthorized viewing, but do not guarantee that data from different controllers is stored in isolated containers, partitions, or namespaces at the storage layer.

**General Security Commitment (DPA § 3.3)** creates a broad obligation to implement "appropriate technical and

organizational measures" and cross-references Annex 2, but neither the DPA body nor Annex 2 uses the words "segregation," "isolation," or any functionally equivalent term that would constitute an explicit contractual data-separation commitment.

**Acceptable Position Assessment:** For a High weight item requiring physical and/or logical data separation, the absence of an explicit segregation commitment — and the affirmative disclosure of a multi-tenant architecture without physical separation — leaves a material gap. The authorization model achieves a functional degree of logical access control and is the industry-standard approach for multi-tenant SaaS, but the contractual framing is weaker than a direct segregation commitment. Classified YELLOW: the topic is partially addressed through the access-control architecture, but the available language does not clearly satisfy the requirement for an affirmative, contractual data-segregation obligation.

— 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 Data is stored in multi-tenant storage systems accessible to Customers via only application user interfaces and application programming interfaces. Customers are not allowed direct access to …"
2. "We host our product infrastructure with multi-tenant, outsourced infrastructure providers. We do not own or maintain hardware located at the outsourced infrastructure providers' data centers. Producti…"

> *"We will implement and maintain appropriate technical and organizational measures to protect Customer Personal Data from Customer Personal Data Breaches, as described under Annex 2 to this DPA ("Security Measures"). Notwithstanding any provision to the contrary, we may modify or update the Security Measures at our discretion provided that such modification or update does not result in a material degradation in the protection offered by the Security Measures."*
> — Data Processing Agreement

## Compliance Monitoring

**AI Comment:** The playbook item requires HubSpot to continually monitor — and adapt where necessary — its compliance with the DPA, applicable data protection laws, and privacy laws, at a minimum annually. The documents contain a constellation of compliance-adjacent provisions, but none expressly establishes a proactive, structured, at-least-annual compliance monitoring and adaptation program covering the full scope of the DPA and applicable privacy laws.

The strongest relevant provision is DPA §7 (Demonstration of Compliance), which discloses that HubSpot undergoes annual SOC 2 compliance audits and regular third-party penetration testing. While SOC 2 Type II represents a rigorous, externally validated annual review, its scope is security-centric (the SOC 2 trust service criteria address security, availability, processing integrity, confidentiality, and privacy of systems) rather than a holistic legal compliance review of the DPA's obligations and applicable data protection regulations. This addresses the security dimension of DPA compliance well, but does not extend to monitoring legal developments across GDPR, CCPA, or other applicable privacy law frameworks, nor to reviewing and adapting the full set of DPA obligations.

DPA §11.1 (Data Privacy Framework) implies periodic compliance re-certification with the EU-U.S. DPF, which involves annual recertification — providing targeted compliance monitoring for cross-border data transfer mechanisms. This is meaningful but narrow in scope.

The General Terms §12.5 commits HubSpot to comply with all applicable U.S. state and federal laws, and DPA §3.1 limits processing to purposes within lawful instructions. These are performance obligations — commitments to maintain compliant conduct — but they are not monitoring obligations. A commitment to comply and a commitment to actively monitor compliance and adapt are distinct; only the latter satisfies the playbook item.

DPA §3.2 (Conflict of Laws) and §9.4 (CCPA, notify if unable to meet obligations) suggest some reactive compliance awareness — HubSpot will notify the customer if it identifies a legal conflict. However, these are triggered by discovered conflicts rather than by proactive, structured periodic reviews designed to identify gaps before they manifest as conflicts.

The classification is YELLOW because: (1) HubSpot has meaningful compliance infrastructure — annual SOC 2 audits, DPF re-certification, general legal compliance commitments, and reactive notification mechanisms — that collectively represent partial compliance monitoring; (2) but the explicit affirmative obligation to actively and periodically audit its compliance with the full DPA and applicable data protection/privacy laws, identify any gaps or changes in the regulatory landscape, and adapt practices accordingly (at least annually) is absent. For a High-weight item, this gap warrants documented assessment by the reviewing legal team. Confidence: MODERATE — the contract language is clear; the question is whether the combination of security-oriented annual audits and reactive legal obligations constitutes functional equivalence with comprehensive compliance monitoring; the AI assesses it does not reach that threshold.

> *"We will make all information reasonably necessary to demonstrate compliance with this DPA available to you and allow for and contribute to audits, including inspections conducted by you or your auditor in order to assess compliance with this DPA, where required by applicable law."*
> — Data Processing Agreement
> *"You acknowledge that the Subscription Service is hosted by our hosting Sub-Processors who maintain independently validated security programs (including SOC 2 and ISO 27001) and that our systems are audited annually as part of SOC 2 compliance and regularly tested by independent third party penetration testing firms. Upon request, we will supply (on a confidential basis) our SOC 2 report and summary copies of our penetration testing report(s) to you so that you can verify our compliance with this DPA."*
> — Data Processing Agreement
> *"If we become aware that we cannot Process Customer Personal Data in accordance with your Instructions due to a legal requirement under any applicable law, we will (i) promptly notify you of that legal requirement to the extent*

*permitted by the applicable law; and (ii) where necessary, cease all Processing (other than merely storing and maintaining the security of the affected Customer Personal Data) until such time as you issue new Instructions with which we are able to comply."*
— Data Processing Agreement
*"We will (i) comply with the obligations applicable to us as a Service Provider under the CCPA; (ii) provide the same level of protection for California Personal Information as is required by the CCPA; and (iii) notify you if we make a determination that we can no longer meet our obligations as a Service Provider under the CCPA."*
— Data Processing Agreement
*"We will comply with all U.S. state and federal laws (where applicable) in our provision of the Subscription Service, the Consulting Services and our processing of Customer Data."*
— Customer Terms of Service
*"HubSpot, Inc. participates in and certifies compliance with the Data Privacy Framework."*
— Data Processing Agreement

## Retention of our rights to our property

**AI Comment:** The playbook item requires that HubSpot's terms prohibit any transfer of ownership of the customer's products, services, materials, content, or data. HubSpot's General Terms satisfy this requirement for the core subscription service: §5.1 explicitly states "You own and retain all rights to the Customer Materials and Customer Data," with only a limited, purpose-bound license granted to HubSpot to use this data to provide the service. HubSpot separately retains its own IP in its services and content (§6.1), and the Product Specific Terms explicitly preserve the customer's rights to AI-generated outputs (PST §7.4). No ownership transfer of the customer's core property occurs.

Two notable carve-outs exist but do not constitute formal ownership transfers: (1) HubSpot claims full ownership of customer suggestions and feedback about the service (§6.2) — a narrow, industry-standard clause scoped solely to improvement suggestions, not to business data or content used in the service; and (2) HubSpot may use Customer Data to train its AI models (§5.3.1), building its own proprietary asset using customer data — however, an opt-out mechanism is available and the customer retains legal title to the underlying data.

For customers using enrichment products, PST §6.5(ii) — which contains explicit superseding language overriding prior conflicting terms — permits HubSpot to copy transmitted Enrichment Data into its commercial dataset and process it as "HubSpot Content." This is a meaningful additional license grant that goes well beyond service provision for enrichment product users. While legal title to the customer's original data is not expressly transferred, treating Enrichment Data as HubSpot Content for commercial dataset purposes is a significant right concession that warrants attention for any customer using those features.

Overall classification is GREEN because: (a) no ownership transfer of Customer Data or Customer Materials occurs under the main subscription service terms; (b) customer ownership is affirmatively and explicitly preserved; (c) the AI training license is opt-outable; and (d) the enrichment data carve-out is scoped to a specific product tier and disclosed. The suggestions/feedback clause is the only outright assignment of customer-originated IP to HubSpot, but it is narrowly scoped and represents standard market practice with low practical risk for the vast majority of customer data. Legal teams should nevertheless flag the enrichment products clause if the customer uses or plans to use those features, as the rights grant is broad.

— Superseding reasoning —
PST §6.5(ii) contains explicit superseding language ("this authorization is necessary for the functionality of enrichment products and supersedes any prior or conflicting terms") that overrides the general Customer Data ownership provisions of ToS §5.1 specifically with respect to Enrichment Data transmitted through enrichment products. The specific enrichment-product terms govern over the general customer ownership clause for that defined category of data. The customer ownership principle in §5.1 remains fully operative for all Customer Data outside the enrichment products context.

*"You own and retain all rights to the Customer Materials and Customer Data. You grant permission to us and our licensors to use the Customer Materials and Customer Data as necessary to provide the Subscription Service and Consulting Services to you, as permitted by this Agreement, and as permitted by applicable law."*
— Customer Terms of Service
*"Between you and HubSpot, you retain all rights you may have to use and exploit your AI Output. This means you can use your AI Output for any lawful purpose, including commercial purposes such as sale or publication, in accordance with the Customer Terms of Service (including these Product Specific Terms)."*
— Product Specific Terms
*"We may use Customer Data to develop, support, and improve HubSpot AI features and functionality. We may also use Customer Data to train our AI models in compliance with our obligations under the Agreement. You may opt out of having your Customer Data used for this purpose by updating your settings in your HubSpot account. If you opt out, we will no longer collect Customer Data to train our AI models, unless you later update your settings and opt in."*
— Customer Terms of Service
*"We retain all intellectual property rights to the HubSpot Content, the Subscription Service, the Consulting Services, and any other products or services provided under this Agreement. You agree not to copy, rent, lease, sell, distribute, or create derivative works based on the HubSpot Content, the Subscription Service, or the Consulting Services in whole or in part, by any means, except as expressly authorized in writing by us."*
— Customer Terms of Service
*"You agree that all such comments and suggestions will be non-confidential and that we own all rights to use and incorporate them into the Subscription Service or Consulting Services, without payment or attribution to you."*
— Customer Terms of Service
*"You acknowledge we may use Enrichment Data to provide, maintain, append, improve, enhance, and develop our commercial dataset and the Subscription Services; this authorization is necessary for the functionality of enrichment*

> *products and supersedes any prior or conflicting terms. For the avoidance of doubt, by using the enrichment products, you agree that only the Enrichment Data you transmit to HubSpot via the Subscription Services may be copied to our commercial dataset and processed further as HubSpot Content."*
> — Product Specific Terms

## Business Continuity Plan

**AI Comment:** The playbook item requires confirmation that the vendor has a Business Continuity Plan (BCP). The document set is not silent — HubSpot's DPA Annex 2 (§5, Availability Control) explicitly states that the vendor maintains and regularly tests disaster recovery plans covering critical business processes, and documents fault-tolerant infrastructure including multi-availability-zone backup and replication. Annual SOC 2 Type II audits (referenced in DPA §7) provide additional, independent assurance that availability and continuity controls are in place and tested.

However, the term "Business Continuity Plan" (or "BCP") does not appear anywhere in the document set. "Disaster Recovery Plans" (DRP) are disclosed, but DRP and BCP are not fully equivalent: a DRP is typically narrower, focused on IT/data recovery, while a comprehensive BCP also covers non-IT continuity (personnel, facilities, communications, supply chain, and operational processes). HubSpot does not confirm the existence or scope of a broader BCP program that would address business-wide disruption beyond the technical/infrastructure layer.

The General Terms §12.2 (Force Majeure) further requires each party to use "reasonable efforts to mitigate" force majeure events, which implies some level of disruption planning, but does not confirm a formal BCP. Given the playbook weight of "Acceptable to Deviate," this gap carries limited practical risk: the DRP disclosure plus SOC 2 Type II compliance together provide meaningful assurance that operational continuity is actively managed. Classification is YELLOW — the topic is substantively addressed through disaster recovery controls, but the broader BCP requirement is only partially and implicitly met.

> *"Disaster Recovery Plans: We maintain and regularly test disaster recovery plans to help ensure availability of information following interruption to, or failure of, critical business processes."*
> — Data Processing Agreement
> *"Fault tolerance: Backup and replication strategies are designed to ensure redundancy and fail-over protections during a significant processing failure. Customer data is backed up to multiple durable data stores and replicated across multiple availability zones."*
> — Data Processing Agreement
> *"You acknowledge that the Subscription Service is hosted by our hosting Sub-Processors who maintain independently validated security programs (including SOC 2 and ISO 27001) and that our systems are audited annually as part of SOC 2 compliance and regularly tested by independent third party penetration testing firms."*
> — Data Processing Agreement

## Termination Obligations

**AI Comment:** The terms address post-termination data handling across three documents but provide weaker and highly variable protections depending on the product tier subscribed to. The DPA §3.6 establishes the primary governing obligation — HubSpot will "delete or return" Customer Data upon termination, with specific procedures delegated to the Product Specific Terms. In practice, that delegation resolves as follows:

(1) HubSpot Smart CRM and Free Services (PST §1.3): Explicit denial of post-termination access. Customers must retrieve data before termination. No exceptions or windows provided.

(2) Marketing Hub Professional and Enterprise – Marketing Contacts (PST §3.3.3): A 30-day post-termination window is available. Upon written request within that window, HubSpot will provide temporary access or copies of all Customer Data. A re-activation fee may apply. After 30 days, no obligation remains.

(3) Other Hub Subscription Services — Sales Hub, Service Hub, etc. (PST §5.1.1): Identical outcome to Smart CRM/Free Services. Explicit denial of post-termination access; data must be retrieved before termination.

The playbook item requires the Vendor to "return or make available all of our data" upon termination. That requirement is partially met only for Marketing Hub Professional and Enterprise customers (30-day window, written request required, potential fee), and is explicitly not met for all other product configurations. Given the "Acceptable to Deviate" weight, this is an &ª Noted informational finding per the risk matrix. The practical implication is that customers must retrieve Customer Data before termination across most product tiers and must submit a timely written request within 30 days post-termination for Marketing Hub Pro/Enterprise to preserve any retrieval right.

— Superseding reasoning —
Multiple documents address post-termination data handling at different levels of specificity. General Terms §5.7 is a cross-reference only — it directs the reader to the DPA and Product Specific Terms and contains no substantive obligation. The DPA §3.6 is the primary governing provision, and it controls over General Terms §5.7 per the DPA's explicit hierarchy clause (§3.4: "this DPA will take precedence to the extent of such conflict or inconsistency"). The DPA §3.6 in turn explicitly delegates procedure to the Product Specific Terms ("in accordance with the procedures set out in our Product Specific Terms"). The PST sections (§1.3, §3.3.3, §5.1.1) therefore function as the operative controlling language for each product scope — they are the specific provisions that implement the general DPA obligation and determine whether "delete or return" in practice means deletion only (most products) or a 30-day retrieval window (Marketing Hub Pro/Enterprise). The PST sections are more specific-to-product and narrow-in-scope relative to the general DPA framework, and they govern for their respective product tiers.

— 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. "For information regarding the retention and deletion of Customer Data, please see the 'HubSpot Obligations' section of our DPA. You can learn more about your right to retrieve Customer Data from your …"
2. "We will delete or return all Customer Data, including Customer Personal Data (including copies thereof) Processed pursuant to this DPA, on termination or expiration of your Subscription Service in acc…"

> *"We strongly recommend retrieving your Customer Data prior to the end of your Subscription Term; for the HubSpot Smart CRM and Free Services, we will not provide you with any access to Customer Data after termination or expiration of your Subscription Term."*
> — Product Specific Terms
> *"For Marketing Hub Professional - Marketing Contacts and for Marketing Hub Enterprise - Marketing Contacts, if you make a written request within thirty (30) days after termination or expiration of your subscription, we will provide you with temporary access to the Subscription Service to retrieve, or we will provide you with copies of, all Customer Data then in our possession or control. If we provide you with temporary access to the account, we may charge a re-activation fee. Thirty (30) days after termination or expiration of your Subscription, we will have no obligation to maintain or provide you the Customer Data."*
> — Product Specific Terms
> *"We strongly recommend retrieving your Customer Data prior to the end of your Subscription Term; for the other Hub Subscription Services we will not provide you with any access to Customer Data after termination or expiration of your Subscription Term."*
> — Product Specific Terms

## Cyber Risk Insurance

**AI Comment:** The playbook item requires: (1) cyber risk insurance covering first-party and third-party losses at no less than $5M; (2) the customer to be named as an additional insured on HubSpot's policy; (3) an Additional Insured Endorsement to be provided after renewal and upon request; and (4) a subrogation waiver (preferred, not required).

Section 12.13 of the General Terms (Insurance) is the sole relevant provision. It requires HubSpot to maintain "Professional Liability (cyber/errors and omissions liability insurance), with a limit of $5,000,000." This meets the $5M minimum threshold — the core financial floor is satisfied.

However, three material gaps prevent GREEN:

1. **Coverage type and first-party losses**: The policy is labeled "Professional Liability (cyber/errors and omissions liability insurance)" rather than a standalone Cyber Risk Insurance policy. Professional Liability / E&O coverage is primarily a third-party liability instrument (protecting against claims by customers/third parties for professional errors or data incidents). First-party cyber coverage — costs of breach notification, forensic investigation, data recovery, and business interruption sustained directly by HubSpot — is not explicitly confirmed. While many cyber/E&O combined policies include first-party elements, the contract does not state this, leaving a gap against the playbook's explicit requirement for both first-party and third-party coverage.

2. **Additional insured — absent (required)**: The playbook explicitly requires that the customer be named as an additional insured on HubSpot's insurance policy. Section 12.13 contains no such provision. This is a required element, not merely a preference.

3. **Additional Insured Endorsement — absent (required)**: The playbook requires an Additional Insured Endorsement evidencing coverage to be provided after renewal and upon request. No such obligation appears anywhere in the document set.

4. **Subrogation waiver — absent (preferred)**: The playbook notes this as a preference. It is also unaddressed.

Because the $5M cyber/E&O coverage is present and meets the dollar minimum, a RED classification is not warranted. The topic is addressed but with weaker structural protection — the missing additional insured status and endorsement represent meaningful gaps from the acceptable position. YELLOW is the appropriate classification at High weight, requiring documented justification and negotiation to address the additional insured and endorsement deficiencies.

> *"During the term of this Agreement, we will, at our own cost and expense, obtain and maintain in full force and effect, with reputable insurers having A.M. best ratings of at least A (VII) or better, liability insurance with coverage and minimum limits of liability as follows: (i) Commercial General Liability Insurance (Primary & Umbrella) or equivalent, with minimum limits of $1,000,000 Each Occurrence and $2,000,000 Aggregate; (ii) Workers' Compensation & Employers Liability Insurance (as required by the state), with minimum limits of $500,000 Each Accident, $500,000 Disease-Policy Limit and $500,000 Disease-Each Employee; (iii) Professional Liability (cyber/errors and omissions liability insurance), with a limit of $5,000,000; and (iv) Umbrella/Excess Liability Insurance, with a minimum limit of $2,000,000."*
> — Customer Terms of Service

## Statutes (Laws, Regulations, etc.)

**AI Comment:** The HubSpot Customer Terms of Service (General Terms), Acceptable Use Policy (AUP), and Data Processing Agreement (DPA) collectively reference a broad but identifiable set of specific statutes and regulatory frameworks with which the customer must comply. The acceptable position requires that all referenced statutes, regulations, and legal requirements be ones the customer can abide by.

All specifically named instruments across all documents are established, real, and abidable:
- GT §2.9.2: COPPA, HIPAA, GLBA, FISMA (US federal, industry-specific)
- AUP §3.1: CAN-SPAM Act, TRAI, TCPA, CTIA/MMA guidelines (telephony/messaging)
- AUP §5.2(xv): CAN-SPAM Act (15 U.S.C. §7701), TCPA (47 U.S.C. §227), Do-Not-Call Implementation Act, GDPR, EU e-Commerce Directive (2000/31/EC), ePrivacy Directive (2002/58/EC), SEC regulations, NYSE/AMEX/NASDAQ rules, PIPEDA, CASL, Japan's Act on Regulation of Transmission of Specified Electronic Mail
- DPA §1: GDPR, CCPA/CPRA, UK GDPR, Swiss DPA, and data protection laws of Australia, Canada, Singapore, India, and Japan

Each has a well-documented compliance framework. None presents an impossibility of compliance for a standard commercial enterprise. Compliance obligations are consistently scoped by "applicable" qualifiers throughout, which limits the customer's obligation to statutes that actually govern their activities and jurisdiction — avoiding the need to comply with laws wholly outside the customer's regulatory perimeter.

The primary breadth concern is AUP §5.2(xv)'s catch-all extending to "any regulations having the force of law or laws in force in your or your email recipient's country of residence," which is theoretically unlimited in geographic scope. However, this provision is (i) prefaced by "any applicable local, state, national or international law or regulation," which provides a meaningful limiting principle; (ii) framed as a usage prohibition (you may not use the service in a way that violates applicable laws) rather than an affirmative warranty of universal foreign-law compliance; and (iii) consistent with the customer's pre-existing legal obligations rather than expanding them. This is standard language for a global marketing/CRM platform. One PIF is therefore flagged YELLOW for breadth awareness, but this does not drive the overall item to YELLOW given the operative "applicable" qualifier throughout.

No conflicts among the referenced statutes are identified. No statute referenced is impossible to comply with. The item is classified GREEN. Confidence is MODERATE rather than HIGH due to the AUP §5.2(xv) catch-all's theoretical scope for customers operating across many international markets with email recipients in diverse jurisdictions. No preference was specified; aiPreferenceMet is false accordingly.

— 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. "You may not use the Subscription Service in a way that would violate local or industry-specific regulations (for example, the Children's Online Privacy Protection Rule consistent with the requirements…"
2. "(xv) is in violation of any applicable local, state, national or international law or regulation, including all export laws and regulations and without limitation the Controlling the Assault of Non-So…"
3. ""Data Protection Laws" means all applicable worldwide legislation relating to data protection and privacy which applies to the Processing of Personal Data under the Agreement, including without limita…"

> *"You will comply with all applicable laws in your use of the Subscription Service and Consulting Services, including any applicable export or trade laws."*
> — Customer Terms of Service
> *"If you use the HubSpot Subscription Service to place telephone calls, text messages, or other supported messaging, you must comply with all applicable:*
>
> *(i) laws relating to telephone calling, texting, and any other message marketing, including applicable local, state, national or international laws (e.g., the CAN-SPAM Act, TRAI, TCPA or other similar laws and regulations applicable to you);*
>
> *(ii) laws related to the recording of phone calls and ensure all proper consent to record is obtained prior to making any such recording;*
>
> *(iii) policies and guidelines of third party service providers, such as network operators and carriers; and*
>
> *(iv) industry standards, including those applicable guidelines published by the CTIA and the Mobile Marketing Association."*
> — Acceptable Use Policy

## Insurance

**AI Comment:** The General Terms §12.13 (Insurance) explicitly and comprehensively addresses the playbook requirement that the vendor maintains adequate insurance. HubSpot commits to maintaining multiple lines of insurance throughout the Agreement term, with specified minimum limits and a named insurer quality floor (A.M. Best A VII or better). The four coverage lines are: (1) Commercial General Liability (Primary & Umbrella) at $1M per occurrence / $2M aggregate; (2) Workers' Compensation & Employers Liability at $500K each accident / disease policy limit / disease per employee; (3) Professional Liability (cyber/errors and omissions) at $5M — a particularly robust limit for a SaaS vendor; and (4) Umbrella/Excess Liability at $2M minimum. These levels collectively meet or exceed market standards for a cloud/SaaS vendor and satisfy the acceptable position of "vendor maintains adequate insurance." No ideal preference was specified, so aiPreferenceMet is set to false — there is no stated benchmark against which to confirm the ideal was reached, only that

the acceptable threshold is clearly met. Given the explicit, granular, and above-standard coverage commitments, and a playbook weight of Acceptable to Deviate, this item is classified GREEN with HIGH confidence. No silence gap, no competing clauses, and no superseding determination is required.

> *"During the term of this Agreement, we will, at our own cost and expense, obtain and maintain in full force and effect, with reputable insurers having A.M. best ratings of at least A (VII) or better, liability insurance with coverage and minimum limits of liability as follows: (i) Commercial General Liability Insurance (Primary & Umbrella) or equivalent, with minimum limits of $1,000,000 Each Occurrence and $2,000,000 Aggregate; (ii) Workers' Compensation & Employers Liability Insurance (as required by the state), with minimum limits of $500,000 Each Accident, $500,000 Disease-Policy Limit and $500,000 Disease-Each Employee; (iii) Professional Liability (cyber/errors and omissions liability insurance), with a limit of $5,000,000; and (iv) Umbrella/Excess Liability Insurance, with a minimum limit of $2,000,000."*
> — Customer Terms of Service

## Disaster Recovery Testing

**AI Comment:** The acceptable position requires (1) the existence of both disaster recovery and business continuity plans, and (2) regular testing of those plans at a specified minimum frequency of at least once annually. HubSpot's DPA Annex 2 (Security Measures, Section 5 – Availability Control) directly addresses this item: HubSpot confirms it "maintain[s] and regularly test[s] disaster recovery plans to help ensure availability of information following interruption to, or failure of, critical business processes." The provision satisfies the structural core of the requirement — plans exist and testing occurs — but falls short in two meaningful ways.

First, the contractual frequency commitment is "regularly," which is undefined. The acceptable position explicitly requires "at least once annually." "Regularly" could be interpreted as quarterly, semi-annually, or annually, but the contract does not bind HubSpot to a minimum cadence. This is a gap, not mere stylistic variance: without a specified floor, the customer has no contractual basis to demand at least annual testing.

Second, the provision uses "disaster recovery plans" only; there is no explicit reference to a separate "business continuity plan." While the DR plan language references "critical business processes" — which overlaps substantially with typical business continuity plan scope — the two are distinct disciplines in enterprise risk management (DR focuses on IT/systems restoration; BCP addresses broader operational continuity). The absence of explicit BCP language is a gap relative to the acceptable position.

Partially mitigating the annual frequency gap: HubSpot commits in DPA Section 7 to annual SOC 2 Type II audits. SOC 2's availability trust service criterion generally requires demonstrated DR plan testing as a control. This provides inferential support that annual testing is likely occurring in practice — but inferential support is not a contractual guarantee and requires an interpretive step.

Supporting infrastructure provisions in Annex 2 (backup/replication, multi-AZ redundancy, N+1 infrastructure, seamless failover architecture) are substantively strong and evidence mature DR capability, but these describe the technical foundation, not the testing cadence.

Overall classification: YELLOW. The topic is substantively addressed and HubSpot does commit to maintaining and regularly testing DR plans, but the absence of an explicit annual frequency commitment and the lack of explicit business continuity plan language leave the acceptable position only partially met. On a High-weight item, this warrants documented review and, if feasible, negotiation of explicit annual testing language or procurement of a current SOC 2 Type II report demonstrating DR testing controls.

> *"Disaster Recovery Plans: We maintain and regularly test disaster recovery plans to help ensure availability of information following interruption to, or failure of, critical business processes."*
> — Data Processing Agreement
> *"Backup and replication strategies are designed to ensure redundancy and fail-over protections during a significant processing failure. Customer data is backed up to multiple durable data stores and replicated across multiple availability zones."*
> — Data Processing Agreement
> *"We maintain and regularly test disaster recovery plans to help ensure availability of information following interruption to, or failure of, critical business processes.*
>
> *Our products are designed to ensure redundancy and seamless failover. The server instances that support the products are also architected with a goal to prevent single points of failure. This design assists our operations in maintaining and updating the product applications and backend while limiting downtime."*
> — Data Processing Agreement
> *"You acknowledge that the Subscription Service is hosted by our hosting Sub-Processors who maintain independently validated security programs (including SOC 2 and ISO 27001) and that our systems are audited annually as part of SOC 2 compliance and regularly tested by independent third party penetration testing firms."*
> — Data Processing Agreement

## Unauthorized Equipment Prevention

**AI Comment:** The playbook item requires HubSpot to prevent use/installation of unauthorized hardware and/or software when processing Customer Personal Data. The acceptable position calls for a dedicated, explicit control addressing both hardware and software dimensions.

HubSpot's DPA Annex 2 (Security Measures) contains the most relevant provisions. The "Endpoint Hardening" sub-section (§2.2) explicitly states that workstations are hardened per industry standards and protected by anti-malware and endpoint detection & response (EDR) tools with regular updates — this addresses the unauthorized *software* dimension materially. The network access controls sub-section (§2.2) further addresses unauthorized protocols reaching product infrastructure. For unauthorized *hardware*, the terms are less direct: HubSpot relies on its outsourced cloud infrastructure providers whose physical and environmental security controls are independently audited for SOC 2 Type II and ISO 27001 compliance (§2.1). Both certifications include controls that would typically cover unauthorized hardware device restrictions, but HubSpot does not articulate this control explicitly in its own terms.

The result is partial coverage: (i) unauthorized software prevention is addressed, albeit implicitly through endpoint hardening and anti-malware rather than a direct prohibition on unauthorized software installation; (ii) unauthorized hardware prevention is only addressed indirectly through reliance on sub-processor certifications, with no explicit HubSpot-level commitment. The General Terms §5.4 and DPA §3.3 establish the overarching obligation to maintain "commercially appropriate" and "appropriate technical and organizational measures," but neither provision articulates a specific unauthorized equipment prevention control.

For a High weight item, the absence of an explicit, standalone unauthorized hardware/software prevention commitment — and the reliance on implicit protections and third-party certifications — warrants a YELLOW classification. The protections described are real and meaningful, but the language does not cleanly meet a dedicated "unauthorized equipment prevention" acceptable position. Reviewers should consider requesting confirmation (e.g., via HubSpot's SOC 2 Type II report, available at trust.hubspot.com per DPA §7) that specific configuration management controls for unauthorized hardware and software restriction are in scope.

— 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. "Physical and environmental security: We host our product infrastructure with multi-tenant, outsourced infrastructure providers. We do not own or maintain hardware located at the outsourced infrastruct…"

> *"Endpoint Harding: Endpoints are hardened in accordance with industry standard practice. Workstations are protected using anti-malware and endpoint detection & response tools, receiving regular definition and signature updates."*
> — Data Processing Agreement
> *"Access controls: Network access control mechanisms are designed to prevent network traffic using unauthorized protocols from reaching the product infrastructure. The technical measures implemented differ between infrastructure providers and include Virtual Private Cloud (VPC) implementations, security group assignment, and traditional firewall rules."*
> — Data Processing Agreement
> *"We will implement and maintain appropriate technical and organizational measures to protect Customer Personal Data from Customer Personal Data Breaches, as described under Annex 2 to this DPA ("Security Measures"). Notwithstanding any provision to the contrary, we may modify or update the Security Measures at our discretion provided that such modification or update does not result in a material degradation in the protection offered by the Security Measures."*
> — Data Processing Agreement
> *"We will maintain commercially appropriate administrative, physical, and technical safeguards to protect Personal Data as described in the DPA, including our Security Measures in Annex 2 of our DPA."*
> — Customer Terms of Service

## Physical Security Controls

**AI Comment:** The playbook item requires the processor to have system controls and policies to prevent unauthorized physical access. The contract set addresses this requirement through multiple layers, with the operative language residing in DPA Annex 2's dedicated "Physical and environmental security" subsection.

HubSpot's approach reflects standard SaaS/cloud delivery architecture: physical security is implemented by outsourced cloud infrastructure providers rather than by HubSpot directly (HubSpot explicitly states it does not own or maintain hardware at its providers' data centers). Critically, HubSpot confirms that: (1) production servers and client-facing applications are logically and physically secured from internal corporate systems; (2) the infrastructure providers' physical and environmental security controls are independently audited for SOC 2 Type II and ISO 27001 compliance — both of which include rigorous physical security requirements; and (3) HubSpot maintains and adheres to an internal, written Information Security Policy. SOC 2 Type II reports are available upon request (confirmed in DPA §7 and trust.hubspot.com).

The obligation to impose equivalent protections on Sub-Processors is established in DPA §5, ensuring that the physical security obligations flow through the supply chain. The General Terms' Section 5.4 commitment to "commercially appropriate administrative, physical, and technical safeguards" is superseded in detail by DPA Annex 2 per the DPA's explicit precedence clause and CTOS §5.4's own cross-reference to the DPA.

This satisfies the acceptable position. Delegating physical security to certified cloud infrastructure providers with independently validated SOC 2 Type II and ISO 27001 programs — and making audit reports available — is functionally

equivalent to the processor maintaining direct physical security controls under this playbook item, and is the accepted industry standard for SaaS vendors. No ideal preference was specified, so aiPreferenceMet is not assessed as true.

— Superseding reasoning —
The DPA contains an explicit precedence clause: "In case of any conflict or inconsistency with other terms included in the Agreement, this DPA will take precedence to the extent of such conflict or inconsistency." Additionally, CTOS §5.4 itself defers to the DPA and its Annex 2 for the operative security measures. Accordingly, DPA Annex 2 (PIF index 0) supersedes the general physical safeguards language in CTOS §5.4 (PIF index 2) by document hierarchy and by the principle of specific over general. The remaining PIFs (DPA §3.3, DPA §7, and DPA Annex 2 §1 Information Security Policy) are consistent with and supportive of the governing DPA Annex 2 physical security provisions and are not in conflict with one another.

— 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. "Physical and environmental security: We host our product infrastructure with multi-tenant, outsourced infrastructure providers. We do not own or maintain hardware located at the outsourced infrastruct…"

> *"We will implement and maintain appropriate technical and organizational measures to protect Customer Personal Data from Customer Personal Data Breaches, as described under Annex 2 to this DPA ("Security Measures")."*
> — Data Processing Agreement
> *"We will maintain commercially appropriate administrative, physical, and technical safeguards to protect Personal Data as described in the DPA, including our Security Measures in Annex 2 of our DPA."*
> — Customer Terms of Service
> *"You acknowledge that the Subscription Service is hosted by our hosting Sub-Processors who maintain independently validated security programs (including SOC 2 and ISO 27001) and that our systems are audited annually as part of SOC 2 compliance and regularly tested by independent third party penetration testing firms."*
> — Data Processing Agreement
> *"We maintain and adhere to an internal, written Information Security Policy."*
> — Data Processing Agreement

## Publicity

**AI Comment:** The playbook's acceptable position requires that the customer must affirmatively give consent before HubSpot may use the customer's name or logo for marketing purposes. The ideal preference goes further: no license to use, copy, or display the customer's name or logo should exist without prior written consent (with a narrow carve-out for use necessary to provide the services).

HubSpot's Customer Terms of Service § 8.1 directly inverts this arrangement: by agreeing to the ToS, the customer automatically and immediately grants HubSpot "the right to add your name and company logo to our customer list and website." No prior consent is solicited, no written approval gate exists, and no service-necessity limitation is applied. The license is broad (customer list and website) and takes effect at contract execution.

Section 8.2 provides an opt-out mechanism via a web form, which is a partial practical mitigation — a customer who promptly exercises this right can curtail the publicity use going forward. However, an opt-out mechanism does not satisfy an opt-in consent requirement. The right vests automatically and operates as the contractual default; it is not conditional on the customer's prior approval. This structure directly contradicts the acceptable position.

The ideal preference is also not met: there is no prior-written-consent gate whatsoever, and no restriction limiting logo use to service-provision purposes.

Classification: RED. This is a High-weight item with an explicit contractual conflict against the acceptable position — not a silence gap, but an affirmative grant of rights that the playbook requires to be conditioned on prior customer consent. The opt-out mechanism is noted as a practical mitigant but does not alter the contractual classification.

— 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. "You can opt-out of this use by filling out the Publicity Opt-Out form at https://legal.hubspot.com/publicity-opt-out-1."

> *"You grant us the right to add your name and company logo to our customer list and website."*
> — Customer Terms of Service

## Password Encryption

**AI Comment:** The playbook item requires that passwords are always stored in encrypted form. The DPA Annex 2 (Security Measures) directly addresses password storage at-rest: "We store user passwords following policies that follow industry standard practices for security." A second sentence in the same provision commits to "a layered approach of at-rest encryption technologies to ensure Customer Data and Customer-identified Permitted Sensitive Data are appropriately encrypted."

The acceptable position is met via functional equivalence. "Industry standard practices for security" in the context of password storage is a well-understood term of art: it necessarily means cryptographic protection (i.e., secure hashing with salting, or equivalent techniques such as bcrypt, scrypt, or Argon2) — not plaintext storage. HubSpot's SOC 2 Type II compliance (acknowledged in DPA §7) provides additional assurance that this commitment is externally audited. The layered at-rest encryption statement reinforces that Customer Data, including credentials, receives cryptographic protection at rest.

One interpretive limitation worth noting: the playbook uses the word "encrypted," while industry standard password storage technically uses one-way hashing (not reversible encryption). This is a distinction without a practical difference from a risk standpoint — hashing is the more secure approach — but the language is not a verbatim match. Confidence is therefore MODERATE rather than HIGH. The General Terms §5.4 cross-reference to Annex 2 is subsidiary; the DPA Annex 2 is the operative governing provision (see superseding determination below).

Overall classification: GREEN — the vendor's Annex 2 language meets the acceptable threshold through functional equivalence. aiPreferenceMet is false because no ideal preference was specified, and the language is not a verbatim explicit commitment to the phrase "encrypted form."

— Superseding reasoning —
The General Terms §5.4 contains a general security commitment ("commercially appropriate administrative, physical, and technical safeguards") and expressly directs the reader to DPA Annex 2 as the operative source of Security Measures. DPA Annex 2 provides the specific, detailed password storage and at-rest encryption commitments. Per the specific-over-general principle, and reinforced by the DPA's own precedence clause (DPA §, intro: "In case of any conflict or inconsistency with other terms included in the Agreement, this DPA will take precedence"), the DPA Annex 2 language is the governing operative text for this item.

> *"At-rest: We store user passwords following policies that follow industry standard practices for security. We take a layered approach of at-rest encryption technologies to ensure Customer Data and Customer-identified Permitted Sensitive Data are appropriately encrypted."*
> — Data Processing Agreement
> *"We will maintain commercially appropriate administrative, physical, and technical safeguards to protect Personal Data as described in the DPA, including our Security Measures in Annex 2 of our DPA."*
> — Customer Terms of Service

## Automatic Renewal

**AI Comment:** The HubSpot Customer Terms of Service expressly address automatic renewal across three interlocking provisions: the default renewal mechanism (§4.1), the opt-out procedure (§4.2), and the fee-adjustment notice at renewal (§3.2).

Core mechanics: Subscriptions auto-renew by default for the shorter of the prior term or one year — a cap that limits maximum lock-in. Renewal is triggered passively unless the customer affirmatively disables it in Account & Billing settings before the Current Term ends. No advance renewal reminder is contractually guaranteed absent a fee change; HubSpot's only affirmative notice obligation at renewal is a 30-day warning when fees will increase, at which point the customer may elect to non-renew.

Because the playbook item carries an "Acceptable to Deviate" weight and the acceptable position is defined as "depends on use case," there is no fixed threshold against which to score GREEN or RED. Instead, the classification reflects the following observations for human review:

• POSITIVE: The renewal cap (shorter of prior term or one year) limits perpetual lock-in. The 30-day fee-increase notice gives the customer a meaningful window to non-renew if pricing is unacceptable. Self-service opt-out via account settings is accessible.

• WATCH ITEMS: No contractual obligation on HubSpot to send a proactive renewal reminder when fees are not changing — a customer who forgets to turn off auto-renew before term end is committed to another cycle. The opt-out mechanism is self-service (account settings toggle) rather than written notice to HubSpot, which may or may not align with the customer's internal governance controls. Amendment terms (§12.1) tie modified agreement terms to the renewal date, meaning a renewal can silently convert the customer to updated terms.

These mechanics are market-standard for SaaS but warrant evaluation against the customer's specific use case (e.g., budget-cycle rigidity, subscription duration, internal approval workflows for renewals). Classified YELLOW — terms are present and reasonably protective in some respects, but specific auto-renewal mechanics create practical risk depending on context. With "Acceptable to Deviate" weight, this is informational; a comment is recommended.

— 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. "Upon renewal, we may increase your Subscription Fees up to our then-current list price set out in our Product and Services Catalog. If this increase applies to you, we will notify you at least thirty …"
2. "If you do not agree with a modification to the Agreement, you must notify us in writing within thirty (30) days after we send notice of the revision. If you give us this notice, then your subscription…"

> *"Your Initial Term will be specified in your Order, and, unless otherwise specified in your Order, your subscription will automatically renew for the shorter of the same duration as your prior term or one year."*
> — Customer Terms of Service
> *"Unless otherwise specified in this Agreement or your Order, if you decide that you do not want your subscription to automatically renew, you must turn off the auto-renewal setting in the Account & Billing section of your HubSpot account prior to the end of your Current Term. If you do not turn off the auto-renewal setting in the Account & Billing section of your HubSpot account, your Subscription will renew automatically."*
> — Customer Terms of Service

## Employee Access Control

**AI Comment:** The playbook item requires that the vendor (HubSpot) only grant system access to its authorized personnel and strictly limit each person's access to what is required to fulfill their function — in essence, a principle of least privilege applied to vendor employees. The DPA's Annex 2 Section 2.3 directly and substantively addresses both elements of this requirement.

On "authorized personnel only": DPA Section 3.4 establishes that HubSpot will ensure all personnel authorized to process Customer Personal Data are subject to appropriate confidentiality obligations. Annex 2 Section 2.3 confirms that only a "subset of employees" has access to the products and customer data via controlled interfaces, for defined purposes (customer support, product development and research, troubleshooting, security incident response, and data security implementation).

On "strictly limit access as required to fulfill function": The JITA (just-in-time access) control mechanism is the key provision — privileged access is "controlled, monitored, and removed in a timely fashion" through JITA, meaning access is provisioned on demand for specific needs rather than permanently maintained. This is a strong and specific implementation of the least-privilege principle. Non-personal system accounts are stored in a secure vault with additional privilege elevation controls. Access is granted by role, all JITA requests are logged, high-risk privilege grants are reviewed daily, and administrative/high-risk permissions are reviewed at least every six months.

One minor limitation: the semi-annual review cadence for administrative/high-risk permissions is less frequent than some security frameworks' quarterly recommendations. However, the compensating controls — JITA provisioning, daily review of new high-risk grants, and logging of all access requests — substantially mitigate this gap. The overall framework meets the acceptable position for this High-weight item. No ideal preference was specified, so aiPreferenceMet is set to false.

— 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. "Privileged Access Management: Privileged access in our product environment is controlled, monitored, and removed in a timely fashion through "just in time access" (or "JITA") controls. Non-personal ac…"

> *"Product access: A subset of our employees have access to the products and to customer data via controlled interfaces. The intent of providing access to a subset of employees is to provide effective customer support, product development and research, to troubleshoot potential problems, to detect and respond to security incidents and implement data security. Access is enabled through JITA requests for access; all such requests are logged. Employees are granted access by role, and reviews of high risk privilege grants are initiated daily. Administrative or high risk access permissions are reviewed at least once every six months."*
> — Data Processing Agreement
> *"We will ensure that any personnel whom we authorize to Process Customer Personal Data on our behalf is subject to appropriate confidentiality obligations (whether a contractual or statutory duty) with respect to that Customer Personal Data."*
> — Data Processing Agreement
> *"We will implement and maintain appropriate technical and organizational measures to protect Customer Personal Data from Customer Personal Data Breaches, as described under Annex 2 to this DPA ("Security Measures"). Notwithstanding any provision to the contrary, we may modify or update the Security Measures at our discretion provided that such modification or update does not result in a material degradation in the protection offered by the Security Measures."*
> — Data Processing Agreement

## Cybersecurity Prevention Systems

**AI Comment:** HubSpot's contract documentation addresses the requirement for adequate systems and processes to prevent unauthorized access to, disclosure of, or loss of customer data through four evidentiary layers: (1) a binding contractual security commitment (DPA §3.3); (2) specific enumerated technical controls in DPA Annex 2; (3) third-party validated certifications (SOC 2 Type II, ISO 27001); and (4) breach notification obligations (DPA §3.5).

The primary governing provision is DPA §3.3, which commits HubSpot to "appropriate technical and organizational measures to protect Customer Personal Data from Customer Personal Data Breaches," with the detailed Security Measures in Annex 2 constituting the specific implementation of that commitment. The General Terms §5.4 cross-references these same DPA Annex 2 measures under a "commercially appropriate" standard — consistent with, but governed by, DPA §3.3 pursuant to DPA §3.4's express precedence clause. Both provisions are fully consistent; no conflict exists. DPA §3.3 is designated the controlling provision per document hierarchy.

Annex 2 directly addresses all three risk vectors in the playbook requirement:
- Unauthorized access: authentication (uniform password policy, mandatory UI authentication before accessing Customer Personal Data), authorization (role/permission-based access, no direct infrastructure access), privilege management (JITA controls), and network security (WAF, access control mechanisms).
- Unauthorized disclosure: TLS/HTTPS encryption in transit across all login interfaces and hosted sites; layered at-rest encryption for Customer Data.
- Data loss: daily vulnerability scanning, annual independent penetration testing, a written Incident Response Plan, and regularly tested Disaster Recovery Plans.

SOC 2 Type II annual audits and ISO 27001 certifications of hosting Sub-Processors provide independent verification that controls operate effectively, with audit reports (SOC 2 and penetration test summaries) available to customers on request.

The 72-hour breach notification obligation (DPA §3.5) addresses detection and response to any disclosure or loss event.

One notable provision: DPA §3.3 reserves the right to modify Security Measures "at our discretion provided that such modification or update does not result in a material degradation in the protection offered." This is standard and acceptable SaaS practice — the "material degradation" floor preserves the substantive protection level over time.

The "commercially appropriate" / "appropriate technical and organizational measures" standards employed by HubSpot are functionally equivalent to "adequate" in the playbook item, and are further operationalized through enumerated Annex 2 controls and externally audited certifications. No ideal preference was specified in the playbook item, so aiPreferenceMet is false by default (no ideal benchmark to assess against). Classification: GREEN.

— Superseding reasoning —
DPA §3.4 establishes that "In case of any conflict or inconsistency with other terms included in the Agreement, this DPA will take precedence to the extent of such conflict or inconsistency." Both General Terms §5.4 and DPA §3.3 require security safeguards and are consistent with each other — no conflict exists. Nevertheless, per this document hierarchy, DPA §3.3 is the operative, governing security obligation for Customer Personal Data, with General Terms §5.4 serving as a high-level cross-reference to the same DPA Annex 2 standard. The Annex 2 Security Measures are the specific implementation body of DPA §3.3 and are not separately superseding — they constitute the content of the Security Measures referenced in §3.3.

— 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. "Authentication: We implement a uniform password policy for our customer products. Customers who interact with the products via the user interface must authenticate before accessing Customer Personal D…"

> *"We will maintain commercially appropriate administrative, physical, and technical safeguards to protect Personal Data as described in the DPA, including our Security Measures in Annex 2 of our DPA."*
> — Customer Terms of Service
> *"We will implement and maintain appropriate technical and organizational measures to protect Customer Personal Data from Customer Personal Data Breaches, as described under Annex 2 to this DPA ("Security Measures"). Notwithstanding any provision to the contrary, we may modify or update the Security Measures at our discretion provided that such modification or update does not result in a material degradation in the protection offered by the Security Measures."*
> — Data Processing Agreement
> *"In-transit: We require HTTPS encryption (also referred to as SSL or TLS) on all login interfaces and for free on every customer site hosted on the HubSpot products. Our HTTPS implementation uses industry standard algorithms and certificates.*
>
> *At-rest: We store user passwords following policies that follow industry standard practices for security. We take a layered approach of at-rest encryption technologies to ensure Customer Data and Customer-identified Permitted Sensitive Data are appropriately encrypted."*
> — Data Processing Agreement
> *"Intrusion detection and prevention: We implement a Web Application Firewall (WAF) solution to protect hosted customer websites and other internet-accessible applications. The WAF is designed to identify and prevent attacks against publicly available network services."*
> — Data Processing Agreement
> *"Vulnerability scanning: We perform daily vulnerability scanning on our products using technology and detection standards aligned with industry standards.*
>
> *Penetration testing: We maintain relationships with industry-recognized penetration testing service providers for penetration testing of both the HubSpot web application and internal corporate network infrastructure at least annually. The intent of these penetration tests is to identify security vulnerabilities and mitigate the risk and business impact they pose to the in-scope systems."*
> — Data Processing Agreement
> *"Incident Response Plan: We maintain a written Incident Response Plan, playbooks, and other necessary processes and procedures to fulfill the standards and obligations reflected therein."*
> — Data Processing Agreement
> *"You acknowledge that the Subscription Service is hosted by our hosting Sub-Processors who maintain independently validated security programs (including SOC 2 and ISO 27001) and that our systems are audited annually as part of SOC 2 compliance and regularly tested by independent third party penetration testing firms. Upon request, we will supply (on a confidential basis) our SOC 2 report and summary copies of our penetration testing report(s) to you so that you can verify our compliance with this DPA."*
> — Data Processing Agreement
> *"We will notify you without undue delay, but no later than seventy-two (72) hours, after we become aware of any Customer Personal Data Breach and will provide timely information relating to the Customer Personal Data Breach as it becomes known or reasonably requested by you."*
> — Data Processing Agreement

## Termination for Convenience

**AI Comment:** The playbook item has three distinct requirements: (1) the customer may terminate for convenience; (2) HubSpot may not terminate for convenience; and (3) a pro rata refund of unused fees is owed if a convenience termination occurs. The HubSpot Customer Terms of Service conflict with all three prongs.

**Prong 1 — Customer termination for convenience (FAILS):** §4.1 expressly prohibits the customer from canceling "prior to the end of your Current Term," with prepaid fees declared non-refundable through that term. The only exit rights available to the customer short of term-end are: (a) non-renewal at term end (§4.2); (b) termination for cause (§4.3); and (c) a limited termination remedy if HubSpot materially degrades functionality (§2.6) or fails to cure a warranty non-conformance (§10.1). None of these constitute termination for convenience.

**Prong 2 — Vendor termination for convenience (FAILS):** HubSpot holds several exit rights that are either explicit "any reason" rights or functionally equivalent. §4.3's second paragraph grants HubSpot the right to terminate on 30 days' notice if it "determines" the customer "may negatively reflect on or affect us, our prospects, or our customers" — a subjective, unilateral standard so broad it operates as a quasi-convenience termination right. §4.4.4 grants HubSpot an explicit right to terminate Free Services "for any reason at any time without notice." The Product Specific Terms extend an equivalent "any reason" termination right over Beta Services (§8.11). HubSpot's exit rights are thus substantively unconstrained in these scopes, while the customer's are tightly restricted.

**Prong 3 — Pro rata refund upon convenience termination (FAILS):** §4.5 limits refunds of prepaid fees solely to customer-initiated terminations for cause. The clause expressly states "Fees are otherwise non-refundable." Since neither party holds an operative termination-for-convenience right over paid subscriptions, there is no contractual refund mechanism for a convenience exit scenario. Similarly, §8.1.3 of the Product Specific Terms declares Consulting Services fees entirely non-refundable.

**Risk calibration:** The weight is "Acceptable to Deviate," placing this RED classification in the &ª Noted tier (comment recommended, not a dealbreaker). The structural asymmetry — customer locked in, vendor with multiple unilateral exit paths — is notable for comment even at this weight level.

— 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. "We may also terminate this Agreement for cause on thirty (30) days' notice if we determine that you are acting, or have acted, in a way that has or may negatively reflect on or affect us, our prospect…"

> *"Except as specifically provided for in this Agreement, you may not cancel your subscription prior to the end of your Current Term, and we will not provide any refunds of prepaid fees or unused Subscription Fees through the end of your Current Term."*
> — Customer Terms of Service
> *"You may choose to cancel your subscription at the end of the Current Term by providing notice as specified in this section."*
> — Customer Terms of Service
> *"We may suspend, limit, or terminate the Free Services for any reason at any time without notice."*
> — Customer Terms of Service
> *"If we terminate this Agreement for cause, you will promptly pay all unpaid fees due. Fees are otherwise non-refundable."*
> — Customer Terms of Service
> *"we may suspend, limit, or terminate the Beta Services for any reason at any time without notice"*
> — Product Specific Terms
> *"Consulting Services are non-cancellable and all fees for Consulting Services are non-refundable."*
> — Product Specific Terms

## Authorized Equipment Usage

**AI Comment:** The playbook item requires that the Processor's employees process Controller data only using authorized business equipment — i.e., an explicit restriction to company-managed or company-approved devices, comparable to a BYOD prohibition at the contractual level.

Searching across all five documents, no provision expressly states that HubSpot employees may only access or process Customer Personal Data on authorized business equipment, nor is there an explicit prohibition on use of personal or unmanaged devices.

The closest relevant language appears in DPA Annex 2 (Security Measures). Section 2.2 ("Preventing Unauthorized Product Use") includes an endpoint hardening provision stating that workstations are protected using anti-malware and endpoint detection & response tools and are hardened in accordance with industry standard practice. This implies HubSpot deploys and manages corporate endpoints, but the commitment is framed as a security hardening measure rather than an explicit authorized-equipment-only restriction. The provision does not state that these workstations are the exclusive permissible devices, nor does it address personal device use.

Section 2.3 ("Limitations of Privilege and Authorization Requirements") establishes that employee access to customer data is exclusively via controlled interfaces with JITA (just-in-time access) logging, role-based grants, and regular privilege reviews. This constrains the access pathway (controlled interfaces, not direct data-layer access) but is silent on the physical device from which that access originates.

Section 3.3 of the DPA establishes a general obligation to implement and maintain "appropriate technical and organizational measures," incorporating Annex 2 by reference. This provides the overarching commitment from which the Annex 2 controls derive their legal weight, but does not independently supply the required authorized-equipment standard.

Together, these provisions paint an implicit picture of a managed endpoint environment — suggesting that in practice employees likely use company-managed devices — but the contractual commitment falls short of the explicit authorized-equipment-only restriction the playbook item requires. An organization relying on this contract for assurance cannot point to a clear, enforceable clause stating that processing is restricted to authorized business equipment. This gap carries real risk: if an employee were to access Customer Data from a personal or unmanaged device, there is no contractual basis for the customer to assert a breach of this specific obligation.

Classification: YELLOW. The topic is addressed implicitly through layered security controls, but without the explicit authorized-equipment restriction required by the acceptable position. For a High weight item, this requires review and documented assessment per the risk matrix.

> *"We will implement and maintain appropriate technical and organizational measures to protect Customer Personal Data from Customer Personal Data Breaches, as described under Annex 2 to this DPA ("Security Measures"). Notwithstanding any provision to the contrary, we may modify or update the Security Measures at our discretion provided that such modification or update does not result in a material degradation in the protection offered by the Security Measures."*
> — Data Processing Agreement
>
> *"Endpoint Harding: Endpoints are hardened in accordance with industry standard practice. Workstations are protected using anti-malware and endpoint detection & response tools, receiving regular definition and signature updates."*
> — Data Processing Agreement
>
> *"Product access: A subset of our employees have access to the products and to customer data via controlled interfaces. The intent of providing access to a subset of employees is to provide effective customer support, product development and research, to troubleshoot potential problems, to detect and respond to security incidents and implement data security. Access is enabled through JITA requests for access; all such requests are logged. Employees are granted access by role, and reviews of high risk privilege grants are initiated daily. Administrative or high risk access permissions are reviewed at least once every six months."*
> — Data Processing Agreement

## User Authentication Policies

**AI Comment:** The playbook item requires confirmation that HubSpot, as processor, maintains policies for user authentication and password protection. The DPA Annex 2 (Security Measures) directly and comprehensively addresses this requirement across multiple sub-sections.

First and most squarely on point, the DPA Annex 2 §2.1 states: "We implement a uniform password policy for our customer products" and mandates that users "authenticate before accessing Customer Personal Data." This explicit acknowledgment of a named, organization-wide password policy — combined with a stated pre-access authentication gate — directly satisfies the acceptable position.

Second, the DPA Annex 2 §3 (Transmission Control) addresses password storage: passwords are stored "following policies that follow industry standard practices for security," and a "layered approach of at-rest encryption technologies" is applied to Customer Data. This confirms password protection controls at rest.

Third, the DPA Annex 2 §2.3 addresses privileged internal access, the higher-risk authentication surface: privileged access is governed by "just in time access" (JITA) controls, non-personal system accounts are stored in a "secure vault," and high-risk access permissions are reviewed "at least once every six months." These controls go beyond baseline authentication to a tiered, audited model.

Fourth, for API-based access paths, OAuth authorization and private app tokens are explicitly required, extending authenticated access controls beyond the UI layer.

Finally, the DPA §7 (Demonstration of Compliance) confirms that HubSpot's systems are audited annually under SOC 2, which independently validates that the stated authentication and password controls are operational and not merely aspirational. While the specific technical parameters of the password policy (e.g., minimum complexity requirements, mandatory MFA) are not enumerated in the public-facing terms, SOC 2 Type II audit coverage provides reasonable assurance that implemented controls meet recognized industry standards.

Classification is GREEN: the vendor terms confirm the existence of documented, audited policies for user authentication and password protection, satisfying the High-weight playbook item. No ideal preference was specified, so aiPreferenceMet is false. Confidence is HIGH — the DPA Annex 2 directly and explicitly addresses both authentication and password protection with specific operational language.

— 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. "Privileged Access Management: Privileged access in our product environment is controlled, monitored, and removed in a timely fashion through "just in time access" (or "JITA") controls. Non-personal ac…"

> *"Authentication: We implement a uniform password policy for our customer products. Customers who interact with the products via the user interface must authenticate before accessing Customer Personal Data in their HubSpot account."*
> — Data Processing Agreement

> *"At-rest: We store user passwords following policies that follow industry standard practices for security. We take a layered approach of at-rest encryption technologies to ensure Customer Data and Customer-identified Permitted Sensitive Data are appropriately encrypted."*
> — Data Processing Agreement
> *"Application Programming Interface (API) access: Public product APIs may be accessed using Oauth authorization or private app tokens."*
> — Data Processing Agreement
> *"You acknowledge that the Subscription Service is hosted by our hosting Sub-Processors who maintain independently validated security programs (including SOC 2 and ISO 27001) and that our systems are audited annually as part of SOC 2 compliance and regularly tested by independent third party penetration testing firms."*
> — Data Processing Agreement

## Warranty

**AI Comment:** The playbook item requires that products and services include a warranty relevant to the services. HubSpot's Customer Terms of Service § 10.1 ("Performance Warranty") directly satisfies this acceptable position: it warrants that (i) the Subscription Service and Consulting Services will be provided in a manner consistent with generally accepted industry standards, and (ii) HubSpot will not knowingly introduce malicious code. This is a warranty directly relevant to the core services. The remedy for non-conformance is also commercially reasonable — a 60-day cure period followed by bilateral termination rights and a pro-rated refund of unused fees.

The § 10.2 "Disclaimer of Warranties" is broad but explicitly carves out the § 10.1 Performance Warranty; the two sections are harmonious, not conflicting. The practical effect is that the warranty is limited to what is expressly stated in § 10.1 — all implied warranties (merchantability, fitness for a particular purpose, etc.) are disclaimed. The Product Specific Terms § 9.2 further supplements the warranty position with a specific, measurable service uptime commitment of 99.95% per calendar month, with a defined credit remedy for consecutive months of non-compliance.

Notable limitations: (a) the § 10.1 warranty does not apply to Free Services; (b) Beta Services carry an explicit "as is" / no-warranty disclaimer (Product Specific Terms § 8.11); (c) Third-Party Products are fully disclaimed (General Terms § 10.5). These carve-outs are standard SaaS market practice and do not undermine the GREEN classification, particularly at the "Acceptable to Deviate" weight level. The playbook preference was not specified, so aiPreferenceMet is false — the ideal benchmark is undefined and cannot be confirmed met. Confidence is HIGH: the language is unambiguous and directly addresses the playbook requirement.

— 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. "In the event of non-conformance with this warranty, we will use commercially reasonable efforts to correct such non-conformance. If we cannot correct such non-conformance within sixty (60) days from t…"
2. "EXCEPT AS SET FORTH IN THE 'PERFORMANCE WARRANTY' SECTION AND WITHOUT LIMITING OUR OBLIGATIONS IN THE 'PROTECTION OF CUSTOMER DATA' SECTION OF THIS AGREEMENT, WE AND OUR AFFILIATES AND AGENTS MAKE NO …"
3. "If we make beta access to some or all of the Subscription Service available to you (i) the Beta Services are provided "as is" and without warranty of any kind, (ii) we may suspend, limit, or terminate…"

> *"We warrant that: (i) the Subscription Service and Consulting Services will be provided in a manner consistent with generally accepted industry standards, and (ii) we will not knowingly introduce any viruses or other forms of malicious code into the Subscription Service; provided however, this warranty will not apply to you if you only use the Free Services."*
> — Customer Terms of Service
> *"We will use commercially reasonable efforts to meet a Service Uptime of 99.95% for our Subscription Service in a given calendar month."*
> — Product Specific Terms

## Data Subject Rights Assistance

**AI Comment:** The HubSpot Data Processing Agreement (DPA), Section 4 — "Data Subject Requests" — directly and substantively addresses both components of this playbook item: (1) the notification requirement and (2) the assistance requirement.

**Notification (§4, sentences 3–4 of the section):** When a DSR is received directly by HubSpot, the DPA obligates HubSpot to "promptly inform" the customer and simultaneously redirect the data subject back to the customer to submit their request. This satisfies the "vendor shall first notify us" requirement. The notification is unconditional and prompt.

**Assistance (§4, sentences 1–2 of the section):** HubSpot commits to providing "reasonable assistance" to the customer in responding to DSRs or data protection authority requests, triggered upon the customer's written request, when the customer is unable to independently address the DSR through the Subscription Service. This satisfies the "promptly assist us" requirement. The Subscription Service also provides self-service controls (retrieve, correct, delete, restrict) for the customer to fulfil many DSRs independently.

**Conditions and caveats (not classification-determinative):** The assistance is subject to three standard conditions: (a) the customer must first attempt to address the request through the Subscription Service's built-in controls; (b) the customer must submit a written request for assistance; and (c) the customer reimburses HubSpot for commercially reasonable costs, with advance notice of those costs. These conditions are consistent with standard SaaS DPA market practice and do not materially weaken the underlying protection. Cost reimbursement for assisted DSR responses is an expected commercial term.

**Acceptable position met:** The acceptable position — "vendor shall first notify us of rights request and promptly assist us in fulfilling data subject's rights requests" — is met by the DPA's prompt notification obligation and the conditional reasonable-assistance framework. Classification: **GREEN**. No ideal preference was specified, so aiPreferenceMet remains false.

> *"To the extent that you are unable to independently address a Data Subject Request through the Subscription Service, then upon your written request we will provide reasonable assistance to you to respond to any Data Subject Requests or requests from data protection authorities relating to the Processing of Customer Personal Data under the Agreement."*
> — Data Processing Agreement
> *"You will reimburse us for the commercially reasonable costs arising from this assistance, and we will notify you of these costs in advance."*
> — Data Processing Agreement
> *"If a Data Subject Request or other communication regarding the Processing of Customer Personal Data under the Agreement is made directly to us, we will promptly inform you and will advise the Data Subject to submit their request to you."*
> — Data Processing Agreement
> *"You will be solely responsible for responding substantively to any such Data Subject Requests or communications involving Customer Personal Data."*
> — Data Processing Agreement
> *"The Subscription Service provides you with a number of controls that you can use to retrieve, correct, delete, or restrict Customer Personal Data, which you can use to assist you in connection with your obligations under Data Protection Laws, including your obligations relating to responding to requests from Data Subjects to exercise their rights under Data Protection Laws ("Data Subject Requests")."*
> — Data Processing Agreement

## Assignment

**AI Comment:** The playbook's acceptable position has two components: (1) both parties may freely assign to successors in interest via merger or acquisition without consent, and (2) the vendor may assign to any other party only with prior customer consent. HubSpot's §12.9 Assignment clause partially satisfies this position.

On the customer side, the provision aligns with the playbook: the customer cannot assign without HubSpot's prior written consent, with a carve-out for successors via merger, reorganization, sale of all or substantially all assets, change of control, or operation of law. This is consistent with the acceptable position.

On the vendor side, the provision deviates in one material respect. HubSpot may assign freely to "any HubSpot Affiliate" — a broad class that is not limited to M&A successors — without requiring any customer consent. The playbook's acceptable position requires prior customer consent for vendor assignments outside of the merger/acquisition successor context. Assignment to an affiliate is a category of assignment distinct from an M&A successor-in-interest transaction, and the HubSpot terms do not condition affiliate assignments on customer approval.

The M&A carve-out on the vendor side (merger, reorganization, asset sale, change of control, operation of law) is consistent with the playbook. The gap is the unrestricted affiliate assignment right without consent.

Given that this item is weighted "Acceptable to Deviate," the deviation — while a technical gap against the acceptable position — does not constitute a high-risk finding. Assignment to affiliates within a corporate family is standard SaaS market practice, and in most cases the substantive counterparty risk does not materially change. Nonetheless, the deviation from the acceptable position warrants a YELLOW classification, as the topic is addressed but the vendor side provides broader assignment rights than the acceptable position permits.

> *"You will not assign or transfer this Agreement without our prior written consent, except that you may assign this Agreement to a successor by reason of merger, reorganization, sale of all or substantially all of your assets, change of control or operation of law. We may assign this Agreement to any HubSpot Affiliate or in the event of merger, reorganization, sale of all or substantially all of our assets, change of control or operation of law."*
> — Customer Terms of Service

## License Grant – Vendor to Our Company

**AI Comment:** The playbook item requires an adequate and sufficient license from HubSpot to the customer. HubSpot's terms take a deliberately SaaS-oriented approach that warrants careful analysis: rather than granting a software license, the agreement provides contractual access rights during the Subscription Term (§2.1). Crucially, §6.1 explicitly disclaims any software license: "you are not granted a license to any software by this Agreement." This is a meaningful statement that directly implicates a playbook item framed around license grants.

In a SaaS context, access-based models are industry-standard — the §2.1 access grant is functionally the operational equivalent of a license for SaaS purposes, allowing Users to use the Subscription Service for the duration of the term, and §2.1.1 extends access to Affiliate Users as a positive element. However, the absence of a formal license creates real legal risk if the customer ever needs to assert license-based rights (e.g., in a dispute, insolvency of vendor, or regulatory context where "license" has specific meaning).

More substantively for the adequacy standard, §2.6 grants HubSpot broad unilateral rights to modify the service during the Subscription Term, explicitly including the right to add or remove features, functions, Limits, and Add-Ons. While §2.6 includes a non-material degradation protection ("modifications we make will not materially degrade the overall functionality of the Subscription Service during the Current Term"), this protection is carved out for: (i) Free Services; (ii) changes outside HubSpot's control, including Third-Party Product changes — a broad exception given HubSpot's extensive ecosystem of

integrations; (iii) as specified in Product Specific Terms; and (iv) Beta Services. The sole remedy for a material degradation that HubSpot cannot remedy within 60 days is termination and pro-rated refund — not repair of the access rights.

The combination of the explicit no-license characterization and the unilateral feature-removal right creates meaningful uncertainty about whether the access rights will remain "adequate and sufficient" throughout the engagement, particularly for customers who rely on specific HubSpot features or integrations. Classification is YELLOW: the topic is addressed and functional access is provided, but the explicit license disclaimer and modification rights prevent GREEN under this High-weight playbook item. Documented justification is required for acceptance per the risk matrix.

— 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. "We may modify the Subscription Service during the Subscription Term, including by adding or removing features, functions, Limits, or Add-Ons that apply to your subscription. Any modifications we make …"

> *"During the Subscription Term, we will provide your Users access to use the Subscription Service as described in this Agreement and the applicable Order."*
> — Customer Terms of Service
> *"You may provide access and use of the Subscription Service to your Affiliate's Users or allow them to receive the Consulting Services purchased under an Order; provided that, all such access, use and receipt by your Affiliate's Users is subject to and in compliance with the Agreement and you will at all times remain liable for your Affiliates' compliance with the Agreement."*
> — Customer Terms of Service
> *"This is an agreement for access to and use of the Subscription Service, and you are not granted a license to any software by this Agreement."*
> — Customer Terms of Service

## Our Rights to deliverables

**AI Comment:** The playbook requires that custom deliverables must be owned by the customer. The contract directly and explicitly contradicts this requirement. General Terms §6.1 vests "all intellectual property rights" in "the Consulting Services, and any other products or services provided under this Agreement" with HubSpot. "Consulting Services" is defined to include professional services such as training, installation, integration, and other consulting work — precisely the engagement type that produces custom deliverables. Notably, the Product Specific Terms §8.1.2 uses the word "deliverables" explicitly in the context of Consulting Services, yet contains no IP assignment to the customer; it governs only delivery timing. The customer's contractual IP rights are confined to two narrow carve-outs: (i) Customer Materials and Customer Data (General Terms §5.1), defined as materials the customer itself provides or uploads — not work product HubSpot creates; and (ii) AI Output (Product Specific Terms §7.4), scoped exclusively to outputs from HubSpot's AI features. The existence of these deliberate, explicit carve-outs — with no equivalent carve-out for consulting deliverables — reinforces the conclusion that HubSpot's retention of IP in Consulting Services is intentional. There is no work-for-hire clause, no deliverables IP assignment clause, and no perpetual license-back that would give the customer meaningful ownership or equivalent rights over custom deliverables. This is a direct and material conflict with the playbook's acceptable position. Weight is High, making this a high-risk finding requiring senior legal justification before the relationship can proceed.

— 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. "If there are deliverables included in the Consulting Services purchased, it is estimated that those deliverables will be completed within the time period indicated as the delivery period in the applic…"

> *"We retain all intellectual property rights to the HubSpot Content, the Subscription Service, the Consulting Services, and any other products or services provided under this Agreement."*
> — Customer Terms of Service
> *"You own and retain all rights to the Customer Materials and Customer Data. You grant permission to us and our licensors to use the Customer Materials and Customer Data as necessary to provide the Subscription Service and Consulting Services to you, as permitted by this Agreement, and as permitted by applicable law."*
> — Customer Terms of Service
> *"Between you and HubSpot, you retain all rights you may have to use and exploit your AI Output."*
> — Product Specific Terms

## Warranty Breach Remedy

**AI Comment:** Section 10.1 (Performance Warranty) of the General Terms directly and substantively addresses the warranty breach remedy scenario contemplated by this playbook item. HubSpot warrants that the Subscription Service will be provided consistent with generally accepted industry standards. Upon non-conformance, HubSpot is obligated to use commercially reasonable efforts to correct the issue — satisfying the 'repair' prong of the playbook requirement at no cost to the customer. If correction cannot be achieved within the 60-day Remedy Period, either party may terminate, and HubSpot will 'promptly refund any prepaid but unused fees covering use of the Subscription Service after termination.' A refund of prepaid but unused fees is functionally equivalent to a pro-rata refund: it returns the exact economic value of service paid for but not yet consumed, which is the precise protection the playbook requires. The 60-day cure period before the refund right triggers is a standard and commercially reasonable grace interval that does not materially undermine the playbook requirement. Section 2.6 (Modifications) separately provides an explicit 'pro-rated refund of unused fees' in a related context (material degradation from service modifications), further confirming that HubSpot's remedy framework employs pro-rata refund mechanics broadly. With a playbook weight of 'Acceptable to Deviate,' even a marginal gap would be low risk; here, the language is substantive and meets the acceptable position through functional equivalence. Classification: GREEN.

— 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. "In the event of non-conformance with this warranty, we will use commercially reasonable efforts to correct such non-conformance. If we cannot correct such non-conformance within sixty (60) days from t…"

> *"If the modification materially degrades the overall functionality of the Subscription Service and HubSpot is unable to provide you with substantially similar functionality, your sole and exclusive remedy for our breach of this section is termination of your Subscription Services and a pro-rated refund of unused fees."*
> — Customer Terms of Service

## Data Protection Officer (DPO)

**AI Comment:** The playbook item requires the Processor (HubSpot) to (1) designate a DPO and (2) ensure that person possesses sufficient qualifications for the role. Analysis of all five documents reveals a clear but partial response to this requirement.

**Designation — met.** DPA Annex 1(A), the primary contractual instrument governing HubSpot's Processor obligations, explicitly identifies "Nicholas Knoop, Data Protection Officer, HubSpot, Inc." as the named contact person for all data processing activities performed on the Customer's behalf. This is a binding contractual commitment within the DPA, which by its own terms "takes precedence" over conflicting Agreement provisions (DPA § 4). The same individual is listed in Annex 1(B) (Controller context) and the Privacy Policy corroborates the DPO role's existence. The designation element is clearly and contractually satisfied.

**Qualifications — not addressed.** No language anywhere in the Customer Terms of Service, Product Specific Terms, DPA (including all Annexes), AUP, or Privacy Policy speaks to the professional qualifications, expertise, or selection criteria for the designated DPO. There is no representation that Nicholas Knoop — or any successor DPO — holds expert knowledge of data protection law and practice, as required by GDPR Article 37(5) and as the playbook's acceptable position demands. The documents simply name the titleholder without any qualification commitment.

**Classification rationale.** Because only one of the two components of the acceptable position is met — designation yes, qualifications no — a GREEN classification is not warranted. The topic is addressed (a DPO is named), but the contract is weaker than the acceptable position requires (no qualification assurance). This is a YELLOW finding. For a High-weight item, the absence of a contractual qualification commitment is a meaningful gap, particularly for customers subject to GDPR, UK GDPR, or similar regimes that impose specific DPO competency standards by law. Notably, for EU/UK customers, GDPR Article 37(5) fills the qualifications requirement by statute; however, since the default governing jurisdiction here is Massachusetts and no customer location was provided, this statutory fill cannot be presumed to apply.

— 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. "Contact person's name, position and contact details: Nicholas Knoop, Data Protection Officer, HubSpot, Inc., Two Canal Park, Cambridge, MA 02141 USA

Activities relevant to the data transferred under …"
2. "HubSpot Ireland Limited is the data controller of your Personal Data. HubSpot's Data Protection Officer can be contacted here."

> *"Annex 1(B) - Details of Processing - HubSpot as Controller](https://legal.hubspot.com/dpa#annex-1b)"*
> — Data Processing Agreement

## Our liability

**AI Comment:** HubSpot's Customer Terms of Service § 10.4 expressly caps the aggregate liability of each party and its affiliates at "the total amounts paid or payable for the Subscription Service in the twelve month period preceding the event giving rise to a claim." This directly satisfies the playbook's acceptable position — customer ("our") liability limited to amount paid — through the industry-standard SaaS formulation of a 12-month look-back fee cap. The cap is mutual (applies to both parties) and bilateral in its scope.

Three carve-outs in § 10.4 expose the customer to uncapped liability beyond this floor: (i) payment of fees owed — commercially essential and universally expected; (ii) indemnification obligations under § 9.1, which are broad and cover unauthorized use, breach of the agreement, use of third-party products, and unauthorized use by persons operating under the customer's credentials; and (iii) customer violations of HubSpot's intellectual property rights. All three are standard SaaS carve-outs consistent with market norms. Notably, HubSpot's own IP indemnification liability is also carved out from the cap (§ 10.4(iii)), meaning HubSpot's exposure for IP infringement claims is also uncapped — a provision that benefits the customer.

Section § 10.3 provides a complementary bilateral exclusion of all indirect, incidental, punitive, and consequential damages (including loss of profits, revenue, data, and business opportunities), further constraining the customer's total exposure regardless of the aggregate cap.

The DPA § 12.3 confirms that all liability arising under the DPA and Standard Contractual Clauses is subject to the same aggregate cap in the General Terms. However, a data protection rights carve-out ("In no event will either party's liability be limited with respect to any individual's data protection rights") means neither party's liability — including the customer's — is capped in the context of individual data protection rights violations. This carve-out is legally required under GDPR Article 82

and equivalent statutes and is not practically negotiable.

No conflicts exist between the General Terms and the DPA on this topic: the DPA expressly defers to and incorporates the General Terms cap rather than creating an alternative or competing limit. No superseding determination is required.

Given the weight of Acceptable to Deviate, the explicit 12-month fee cap meeting the core playbook requirement and the standard, legally-required nature of all identified carve-outs support a GREEN classification at 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. "TO THE EXTENT PERMITTED BY LAW, AND EXCEPT FOR (i) YOUR LIABILITY FOR PAYMENT OF FEES, (ii) YOUR LIABILITY ARISING FROM YOUR OBLIGATIONS UNDER THE 'INDEMNIFICATION' SECTION, (iii) OUR LIABILITY ARISIN…"
2. "Each party and each of their Affiliates' liability, taken in aggregate, arising out of or related to this DPA (including any other data processing agreements between the parties) and the Standard Cont…"

> *"TO THE EXTENT PERMITTED BY LAW, IN NO EVENT WILL EITHER PARTY OR ITS AFFILIATES BE LIABLE FOR ANY INDIRECT, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES, OR LOSS OF PROFITS, REVENUE, DATA OR BUSINESS OPPORTUNITIES ARISING OUT OF OR RELATED TO THIS AGREEMENT, WHETHER AN ACTION IS IN CONTRACT OR TORT AND REGARDLESS OF THE THEORY OF LIABILITY."*
> — Customer Terms of Service

## Payment Terms

**AI Comment:** HubSpot's General Terms address both payment scenarios contemplated by this playbook item. For invoice payments, §3.4 establishes a 30-day payment window measured from the "date of the invoice," which meets the playbook's acceptable position of at least 30 days from receipt of invoice. A minor technical distinction exists between "date of invoice" and "receipt of invoice": if an invoice is dated before it is actually delivered, the effective payment window would be marginally shorter than 30 days from receipt. In practice, HubSpot operates an electronic billing system for a SaaS platform, where invoice date and receipt are functionally simultaneous, making this distinction negligible. One structural variable is the "unless otherwise specified in the Order Form" carve-out in §3.4, which permits individual Order Forms to deviate from the 30-day standard — this should be verified at contract execution for any specific engagement. For credit card payments, §3.3 establishes an autopay structure (automatic charge to the Authorized Payment Method), directly satisfying the playbook's carve-out permitting less than 30 days for credit card autopay. A potentially ambiguous general statement in §3.5 — "All fees are due and payable in advance throughout the Subscription Term" — refers to HubSpot's advance-billing cycle structure (invoiced at the start of each term or billing period, not in arrears), and is compatible with the 30-day payment window in §3.4. Read harmoniously, these provisions address different aspects of payment: when invoices are issued (§3.5: advance billing) versus when invoiced amounts are due (§3.4: 30 days from invoice date). Overall, the standard terms meet the playbook's acceptable position for both invoice and credit card payment scenarios.

> *"All amounts invoiced are due and payable within thirty (30) days from the date of the invoice, unless otherwise specified in the Order Form."*
> — Customer Terms of Service
> *"If you are paying by credit card, you authorize us to charge your Authorized Payment Method for all fees payable during the Subscription Term."*
> — Customer Terms of Service
> *"All fees are due and payable in advance throughout the Subscription Term."*
> — Customer Terms of Service

## Anti-Virus Solution

**AI Comment:** The playbook item requires that all authorized computer systems have an anti-virus solution. HubSpot addresses this in Annex 2 of the DPA (Security Measures), Section 2.2 "Preventing Unauthorized Product Use," under the "Endpoint Hardening" sub-section: "Workstations are protected using anti-malware and endpoint detection & response tools, receiving regular definition and signature updates."

Applying the functional equivalence standard: "anti-malware and endpoint detection & response (EDR) tools" with "regular definition and signature updates" is functionally equivalent to — and by modern security standards, superior to — a traditional anti-virus solution. Anti-malware + EDR covers the same threat-detection and remediation objectives as anti-virus while providing broader behavioral detection capabilities. The requirement for regular definition/signature updates mirrors the operational hallmark of anti-virus maintenance.

The slight ambiguity is that the clause explicitly names "Workstations" for the anti-malware protection, while the playbook item references "all authorized computer systems" (which could encompass servers and other infrastructure). However, the governing header "Endpoint Hardening" and the preceding sentence ("Endpoints are hardened in accordance with industry standard practice") indicate the hardening posture applies to endpoints broadly, with workstations called out as a specific category. Server-level protection is addressed implicitly through the broader endpoint hardening language and the layered security controls described elsewhere in Annex 2 (e.g., access controls, WAF, intrusion detection). On balance, the language meets the acceptable position for this High-weight item, warranting a GREEN classification with MODERATE confidence due to the workstation-specific callout for anti-malware rather than an explicit all-systems declaration.

No preference was specified in the playbook item, so aiPreferenceMet is set to false — the acceptable threshold is met but ideal preference cannot be assessed.

> *"Endpoint Harding: Endpoints are hardened in accordance with industry standard practice. Workstations are protected using anti-malware and endpoint detection & response tools, receiving regular definition and signature updates."*

— Data Processing Agreement

## Data Backup & Restoration

**AI Comment:** The playbook item requires two distinct obligations: (1) creation of backups of data, and (2) regular restoration tests of those backups at a minimum annually.

**Backup Creation (GREEN component):** HubSpot's terms address this element comprehensively and clearly. CToS §5.5 confirms Customer Data is replicated for disaster recovery and backup purposes within the regional Hosting Location. DPA Annex 2 §5 (the controlling document per DPA §4's precedence clause) provides further technical detail: Customer Data is backed up to multiple durable data stores and replicated across multiple availability zones, with all databases backed up and maintained using at least industry-standard methods. This clearly satisfies the backup creation limb.

**Restoration Testing (YELLOW component — controlling classification):** This is where the terms fall short of the playbook's acceptable position. The only provision addressing testing is DPA Annex 2 §5, which states HubSpot "maintain[s] and regularly test[s] disaster recovery plans." This falls short in two material respects:

(i) **No minimum annual frequency is committed to.** "Regularly" is undefined throughout the contract. The playbook's acceptable position explicitly requires a minimum annual cadence for restoration tests. HubSpot's terms provide no such floor — "regularly" could be interpreted to mean quarterly, semi-annually, or even less frequently.

(ii) **"Testing disaster recovery plans" is not synonymous with "restoration tests of backups."** Disaster recovery plan testing is a broader category that can encompass testing failover procedures, communication trees, personnel escalation chains, and incident response workflows — without necessarily verifying that backups can be successfully restored to a usable state. The specific backup restoration test commitment the playbook requires is not explicit.

**Overall:** YELLOW. The topic is addressed, backup creation clearly meets the requirement, and some form of DR plan testing is committed to. However, the restoration testing obligation is addressed with language that is materially weaker and less specific than the playbook's acceptable position — the minimum annual frequency is absent and the restoration-specific commitment is ambiguous. The DPA Annex 2 §5 provisions govern per DPA §4's explicit precedence clause, superseding the high-level CToS §5.5 backup reference.

— Superseding reasoning —
The General Terms §5.5 provides a high-level statement that Customer Data is replicated for disaster recovery and backup purposes within the regional Hosting Location. The DPA Annex 2 §5 (Availability Control section) contains three distinct provisions providing more specific and detailed backup and DR testing commitments on the same topic. Per DPA §4 — "In case of any conflict or inconsistency with other terms included in the Agreement, this DPA will take precedence to the extent of such conflict or inconsistency" — the DPA Annex 2 provisions govern backup and restoration obligations. Additionally, the SPECIFIC_OVER_GENERAL principle applies: DPA Annex 2 is specifically the enumerated security measures document, with granular technical commitments that supersede the general backup mention in CToS §5.5. All three DPA Annex 2 PIFs (indices 1, 2, 3) supersede the CToS §5.5 PIF (index 0). The governing standard for this playbook item is drawn from the combined DPA Annex 2 §5 provisions.

> *"Your Customer Data will be replicated for disaster recovery and back-up purposes within your regional Hosting Location."*
> — Customer Terms of Service
> *"Fault tolerance: Backup and replication strategies are designed to ensure redundancy and fail-over protections during a significant processing failure. Customer data is backed up to multiple durable data stores and replicated across multiple availability zones."*
> — Data Processing Agreement
> *"Online replicas and backups: Where feasible, production databases are designed to replicate data between no less than 1 primary and 1 secondary instance. All databases are backed up and maintained using at least industry standard methods."*
> — Data Processing Agreement
> *"Disaster Recovery Plans: We maintain and regularly test disaster recovery plans to help ensure availability of information following interruption to, or failure of, critical business processes."*
> — Data Processing Agreement

## Data Retention & Deletion

**AI Comment:** The playbook's acceptable position requires (1) deletion of requested data from production systems within 10 days of request, and (2) backup data cycling out within a maximum of 364 days. HubSpot's terms address retention and deletion across the DPA, General Terms, and Product Specific Terms but materially fail both quantitative thresholds.

**Production deletion (10-day requirement — NOT MET):** The governing provision is DPA §3.6, which conditions HubSpot's deletion obligation on "termination or expiration of your Subscription Service." No document in the set establishes a contractual obligation for HubSpot to delete data from production systems within 10 days of a customer's ad-hoc deletion request made during an active subscription term. The most specific post-termination timeline in the entire document set is PST §3.3.3 (Marketing Hub Professional/Enterprise only): HubSpot grants a 30-day retrieval window after termination, and commits to delete Customer Data after that window — making the earliest possible production deletion Day 31 post-termination, more than three times the 10-day acceptable position and applicable only post-termination, not to mid-subscription requests. For Smart CRM/Free Services (PST §1.3) and Other Hubs (PST §5.1.1), no post-termination deletion timeline is committed to at all. DPA §4 confirms that self-service deletion controls exist within the Subscription Service, which customers can use to delete their own Customer Personal Data — potentially near-instantaneously in practice — but no contractual commitment from HubSpot to process or confirm production deletion within 10 days of any

request exists anywhere in the document set.

**Backup cycling (364-day maximum — NOT MET):** DPA §3.6 carves out "archived Customer Data on back-up systems," committing only to "securely isolate and protect from any further Processing and delete in accordance with our deletion practices." The phrase "deletion practices" references an undisclosed internal policy. No maximum timeframe of any kind — let alone 364 days — is specified contractually. PST §3.3.3 incorporates this DPA backup carve-out explicitly ("save as set out in the Deletion or Return of Customer Personal Data section of the DPA"), confirming the open-ended backup cycling standard applies across all product tiers.

**Overall:** Both required quantitative thresholds are unmet. The production deletion gap is twofold: no mid-subscription deletion-on-request commitment exists, and the only specific post-termination timeline (30+ days, Marketing Hub Pro/Enterprise only) materially exceeds the acceptable position. The backup cycling requirement is entirely open-ended with no contractual ceiling. For a High-weight item, both gaps are material. Classification: RED, Confidence: HIGH.

— Superseding reasoning —
The DPA contains an express precedence clause stating: "In case of any conflict or inconsistency with other terms included in the Agreement, this DPA will take precedence to the extent of such conflict or inconsistency." Accordingly, DPA §3.6 governs deletion obligations and supersedes the General Terms §5.7 cross-reference on this topic. The relationship between DPA §3.6 and PST §3.3.3 is cooperative rather than conflicting: DPA §3.6 explicitly delegates product-specific deletion procedures to the Product Specific Terms ("in accordance with the procedures set out in our Product Specific Terms"), and PST §3.3.3 in turn defers back to DPA §3.6 for backup-deletion exceptions ("save as set out in the Deletion or Return of Customer Personal Data section of the DPA"). The governing framework is DPA §3.6 as implemented by PST §3.3.3 for Marketing Hub Professional/Enterprise customers, and by DPA §3.6 alone for all other product tiers.

— 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. "We will delete or return all Customer Data, including Customer Personal Data (including copies thereof) Processed pursuant to this DPA, on termination or expiration of your Subscription Service in acc…"
2. "For Marketing Hub Professional - Marketing Contacts and for Marketing Hub Enterprise - Marketing Contacts, if you make a written request within thirty (30) days after termination or expiration of your…"
3. "For information regarding the retention and deletion of Customer Data, please see the 'HubSpot Obligations' section of our DPA. You can learn more about your right to retrieve Customer Data from your …"

> *"We strongly recommend retrieving your Customer Data prior to the end of your Subscription Term; for the HubSpot Smart CRM and Free Services, we will not provide you with any access to Customer Data after termination or expiration of your Subscription Term."*
> — Product Specific Terms
> *"We strongly recommend retrieving your Customer Data prior to the end of your Subscription Term; for the other Hub Subscription Services we will not provide you with any access to Customer Data after termination or expiration of your Subscription Term."*
> — Product Specific Terms
> *"The Subscription Service provides you with a number of controls that you can use to retrieve, correct, delete, or restrict Customer Personal Data, which you can use to assist you in connection with your obligations under Data Protection Laws, including your obligations relating to responding to requests from Data Subjects to exercise their rights under Data Protection Laws ("Data Subject Requests")."*
> — Data Processing Agreement

## Employee Offboarding Access

**AI Comment:** The playbook requires HubSpot (as Processor) to have explicit policies and systems ensuring employee access is offboarded or adjusted — in no event later than 24 hours — upon termination or job function change. HubSpot's DPA Annex 2 (Security Measures, §2.3) addresses related access control concepts through JITA (just-in-time access) controls and role-based access with review processes, but the contract language falls materially short of the acceptable position in four respects:

1. **No specific timeframe committed**: The JITA language states access is removed "in a timely fashion" — a vague standard that does not satisfy the 24-hour maximum required by the playbook. "Timely" is undefined and unenforceable against a specific SLA.

2. **No explicit termination trigger**: The contract does not expressly state that employee termination triggers immediate or time-bound access revocation. The JITA framework appears designed around access grants and privilege escalation, not offboarding workflows.

3. **No explicit job-function-change trigger**: There is no language addressing access modification when an employee changes roles or job function — only that access is "granted by role," which describes the model but not the process for updating access when the role changes.

4. **Semi-annual review cycle creates a material gap**: The clause stating "Administrative or high risk access permissions are reviewed at least once every six months" directly conflicts with a 24-hour offboarding obligation. A periodic review model is structurally inconsistent with prompt, event-triggered access revocation.

The JITA architecture and daily review of high-risk privilege grants are operationally positive indicators, but they do not translate into a contractual commitment meeting the playbook's acceptable position. For a High-weight item, this gap

warrants documented assessment and likely negotiation of a more specific SLA commitment in a security exhibit or DPA addendum. Classification: YELLOW.

— 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. "Privileged Access Management: Privileged access in our product environment is controlled, monitored, and removed in a timely fashion through "just in time access" (or "JITA") controls. Non-personal ac…"

> *"Product access: A subset of our employees have access to the products and to customer data via controlled interfaces. The intent of providing access to a subset of employees is to provide effective customer support, product development and research, to troubleshoot potential problems, to detect and respond to security incidents and implement data security. Access is enabled through JITA requests for access; all such requests are logged. Employees are granted access by role, and reviews of high risk privilege grants are initiated daily. Administrative or high risk access permissions are reviewed at least once every six months."*
> — Data Processing Agreement

## Termination for Cause

**AI Comment:** The playbook item requires that the customer retain a right to terminate the agreement if the vendor (HubSpot) breaches. Section 4.3 of the General Terms expressly provides a mutual termination-for-cause right: "Either party may terminate this Agreement for cause" upon 30 days' written notice of a material breach remaining uncured, or immediately upon insolvency events. This unambiguously satisfies the acceptable position.

Supporting provisions further bolster the customer's position: §4.5 confirms that upon the customer's termination for cause, HubSpot will promptly refund prepaid but unused fees — a meaningful financial remedy. Section 10.1 (Performance Warranty) provides an additional discrete termination right when HubSpot fails to cure a warranty non-conformance within 60 days. Section 2.6 (Modifications) provides a further specific termination right if HubSpot's service modifications materially degrade overall functionality, though that provision designates termination as the "sole and exclusive remedy" for that specific breach scenario (limiting damages claims arising from modification-related breaches specifically — relevant for a separate limitation-of-liability review but not dispositive here).

One asymmetry worth flagging for awareness (not scored against this item): §4.3 also grants HubSpot a unilateral additional termination-for-cause right upon 30 days' notice if HubSpot determines the customer is acting in a way that "may negatively reflect on or affect" HubSpot. This is a vendor-favoring asymmetric right that does not have a customer-side counterpart, but it does not restrict the customer's own termination rights.

The 30-day cure period before termination becomes effective is standard market practice and does not meaningfully weaken the customer's position. Weight is "Acceptable to Deviate," meaning deviation would only be noted; however, HubSpot's terms affirmatively meet the acceptable position, resulting in a GREEN classification. No preference was specified, so aiPreferenceMet is set to false.

— Superseding reasoning —
No superseding conflict exists among the identified references. Section 4.3 is the general mutual termination-for-cause provision. Sections 2.6 and 10.1 are narrower, scenario-specific termination rights that operate in addition to §4.3 for their respective breach scenarios, consistent with the specific-over-general principle. All references support the customer's termination right and classify GREEN; no precedence determination changes 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. "Either party may terminate this Agreement for cause, as to any or all Subscription Services: (i) upon thirty (30) days' notice to the other party of a material breach if such breach remains uncured at…"
2. "If we cannot correct such non-conformance within sixty (60) days from the date when you notified us of the non-conformity (the "Remedy Period"), then either party may terminate this Agreement by provi…"

> *"If you terminate this Agreement for cause, we will promptly refund any prepaid but unused fees covering use of the Subscription Service after termination."*
> — Customer Terms of Service
> *"If the modification materially degrades the overall functionality of the Subscription Service and HubSpot is unable to provide you with substantially similar functionality, your sole and exclusive remedy for our breach of this section is termination of your Subscription Services and a pro-rated refund of unused fees."*
> — Customer Terms of Service

## Exclusivity

**AI Comment:** The playbook item requires that no exclusivity obligations be accepted — i.e., the vendor must not impose any restriction preventing the customer from using competing or comparable services. A comprehensive review of all five HubSpot documents (General Terms, Product Specific Terms, Data Processing Agreement, Acceptable Use Policy, and Privacy Policy) confirms that no exclusivity provision of any kind exists anywhere in the contract suite.

Specifically, none of the documents:
(1) Require the customer to use HubSpot as their sole or exclusive vendor for CRM, marketing automation, or any other service category;
(2) Prohibit or restrict the customer from simultaneously subscribing to, evaluating, or deploying competing products or services;

(3) Grant HubSpot any form of exclusive rights over the customer's business relationships, revenue opportunities, or technology choices.

**Classification rationale — why GREEN despite silence:** The standard silence-default-RED framework applies when a contract fails to include a protection that the playbook item *requires to be present*. This item operates in the opposite direction: it identifies a clause type the customer *does not want*. Silence here means the undesired clause is absent, which is the acceptable (and optimal) outcome. Accordingly, the silence is fully favorable and GREEN is the correct classification. The RED-default for silence does not apply in this circumstance.

**Peripheral provisions reviewed and distinguished:**
- **§ 6.2 (Suggestions):** HubSpot takes ownership of customer feedback and suggestions. This is an irrevocable IP rights grant on feedback, not an exclusivity obligation on the customer's business operations.
- **§ 8.1 (Publicity Rights):** HubSpot may list the customer's name/logo as a reference customer (opt-out available per § 8.2). This is a publicity right, not exclusivity.
- **§ 12.9 (Assignment):** Customer requires HubSpot's prior written consent to assign the agreement (except in M&A contexts). This is an assignment restriction affecting contract transferability, not a restriction on using competing services.
- **AUP § 5.5 (Prohibited Use):** Prohibits the customer from reselling or sublicensing the HubSpot service to third parties. This is a standard no-resale restriction that applies *to HubSpot's own service*, not an exclusivity obligation preventing the customer from using other vendors.

None of these provisions, individually or in combination, constitute exclusivity obligations on the customer.

**Confidence:** HIGH — the finding is clear and unambiguous across all five documents. No interpretive ambiguity is present.

## External Links

**AI Comment:** HubSpot's agreement suite contains at least 20 distinct external links to additional terms, policies, and legal documents that are incorporated by reference as binding contractual obligations. The playbook's ideal preference of no external links is entirely unmet. The acceptable position — that all external links be reviewed — cannot be fully satisfied within this review because the following incorporated documents were not included in the review set: Sensitive Data Terms, Jurisdiction Specific Terms appendices for all applicable regions (Canada, Colombia, Europe, Germany, France, Spain, Netherlands, UK, Australia, Japan, India, Asia-Pacific), Code of Business Conduct and Ethics, Product and Services Catalog, HubSpot Payments Terms of Use (referenced in both the General Terms and the Product Specific Terms), Beta Terms, Stripe Payment Processing Terms, Anti-Spam Policy, Developer Terms, Marketplace Terms of Use, WhatsApp Business Solution Terms, EU Standard Contractual Clauses (Commission Decision 2021/914), and the UK International Data Transfer Addendum. The Sub-Processors Page is incorporated into the DPA but is a dynamic document subject to change.

Three structural risks compound the external link exposure: (1) The Agreement is defined to include "all materials referred or linked to in here" (§ 1 Definitions) without limitation, making every hyperlink in the contract suite a binding contractual obligation regardless of whether it was individually reviewed or negotiated; (2) Several external documents can be modified unilaterally with reduced or no notice — the Code of Business Conduct and Ethics "may be updated without additional notice to you," the Product and Services Catalog is updated "from time-to-time" with no express notice requirement for Catalog-level changes (distinct from the 30-day renewal notice for fee increases), and the Anti-Spam Policy may be updated "from time to time"; and (3) The applicable Jurisdiction Specific Terms are location-dependent and cannot be determined without a confirmed customer Company Address — which was not provided in the intake brief — making it impossible to identify which JST governs this customer's agreement and what jurisdiction-specific obligations apply.

Third-party terms from Google (Customer Data Policies, Privacy Policy), YouTube (Terms of Service), and WhatsApp/Meta (Business Solution Terms) are incorporated by reference for specific feature activations, creating binding obligations to documents governed by unrelated entities that can be modified entirely outside the HubSpot-Customer contractual relationship.

Under the High weight classification, RED requires senior legal justification. Each external link identified in the PIFs below should be individually retrieved and reviewed by legal counsel prior to execution. The customer should request a consolidated, integrated contract document or seek exhibit attachments for all incorporated documents to facilitate comprehensive review.

— Note —
The AI cited 18 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. ""Agreement" or "Customer Terms of Service" means these General Terms and all materials referred or linked to in here, unless otherwise stated."
2. "You will comply with our Acceptable Use Policy at http://legal.hubspot.com/acceptable-use ("AUP")."
3. "The HubSpot Sensitive Data Terms available at https://legal.hubspot.com/sensitive-data-terms are incorporated into this Agreement if you enable the Sensitive Data functionality in your HubSpot Account…"
4. "The terms of the DPA are hereby incorporated by reference and will apply to the extent any Customer Data includes Personal Data."
5. ""Product and Services Catalog" means HubSpot's Product and Services Catalog, which is incorporated into this Agreement and as updated by us from time-to-time and available at http://legal.hubspot.com/…"
6. "We will comply with our Code of Business Conduct and Ethics which can be found on our Investor Relations page on

hubspot.com; the Code of Business Conduct and Ethics is incorporated into this Agreemen…"
7. "Additional jurisdiction specific requirements are available at the Jurisdiction Specific Terms Appendix to these General Terms and will apply to your Agreement."
8. "For the avoidance of doubt, this refund does not include any fees owed from your use of HubSpot Payments, which is separately governed under the HubSpot Payments Terms of Use."
9. "The HubSpot Subscription Services may be provided to you as a Beta Service and where the HubSpot Beta Terms at https://legal.hubspot.com/hubspot-beta-terms will also apply."
10. "By using the Google Enhanced Conversions feature, one of the ad conversion tools offered by HubSpot, you authorize us to provide necessary data to Google in order to make this functionality available …"
11. "Your use of HubSpot's YouTube integration is subject to the YouTube Terms of Service available at https://www.youtube.com/t/terms and the Google Privacy Policy available at http://www.google.com/polic…"
12. "If you use Stripe payment processing as your payment processing option, please note that Stripe payment processing is an additional service available outside the scope of our Subscription Services, an…"
13. "If you use HubSpot payments as your payment processing option, please note that HubSpot payments is an additional service available outside the scope of our Subscription Services and subject to the 'C…"
14. "If you use the HubSpot Directory (as defined in the HubSpot Marketplace Terms of Use), you agree to comply with the HubSpot Marketplace Terms of Use available at https://legal.hubspot.com/marketplace-…"
15. "If you connect your WhatsApp Business account to HubSpot, you also agree to WhatsApp's Business Solution Terms available at https://www.whatsapp.com/legal/business-solution-terms/."
16. "You will comply with the HubSpot Anti-Spam Policy available at https://legal.hubspot.com/anti-spam-policy, as updated by us from time to time."
17. "If you use any of our developer tools including Application Programming Interfaces (APIs), developer tools, or associated software, you will comply with our Developer Terms at https://legal.hubspot.co…"
18. "A list of our Sub-Processors and our purpose for engaging them is located on our HubSpot Sub-Processors Page available at https://legal.hubspot.com/sub-processors-page, which is incorporated into this…"

> *"The Standard Contractual Clauses will be incorporated by reference and apply to the Restricted Transfer as follows:"*
> — Data Processing Agreement

> *"the Standard Contractual Clauses will be modified and interpreted in accordance with the UK Addendum, which will be incorporated by reference and form an integral part of the Agreement"*
> — Data Processing Agreement

## Employee Confidentiality Agreements

**AI Comment:** The playbook requires that HubSpot employees who access data enter into written confidentiality agreements. Two provisions across the document set directly address this obligation, and they are inconsistent with each other.

General Terms §7.1 explicitly requires that access to Confidential Information be limited to employees, contractors, and agents "who have signed confidentiality agreements with the Receiving Party containing protections no less stringent than those herein." Customer Data is expressly deemed Confidential Information under the General Terms (§1.45: "Customer Data will be considered Confidential Information under this Agreement regardless of whether or not it is designated as confidential"). Standing alone, the General Terms §7.1 provision satisfies the playbook requirement — it requires signed (written) agreements as a condition of access.

DPA §3.4, however, imposes a materially different and weaker standard for the specific context of Customer Personal Data processing: HubSpot "will ensure that any personnel whom we authorize to Process Customer Personal Data on our behalf is subject to appropriate confidentiality obligations (whether a contractual or statutory duty)." The parenthetical "whether a contractual or statutory duty" expressly contemplates statutory obligations (e.g., arising under employment law, trade secret law, or GDPR Article 29 personnel duties) as a sufficient alternative to written contractual agreements. Written agreements are not strictly required.

The DPA contains an explicit precedence clause: "In case of any conflict or inconsistency with other terms included in the Agreement, this DPA will take precedence to the extent of such conflict or inconsistency." The requirement in General Terms §7.1 for signed agreements is inconsistent with the DPA §3.4 permission to rely on statutory duties alone. Under the DPA's precedence clause, DPA §3.4 is the governing provision for personnel who Process Customer Personal Data — the primary concern driving this playbook item.

Under the governing DPA language, written confidentiality agreements are not strictly required: a statutory duty may suffice. Statutory duties vary in scope, enforceability, and content across jurisdictions and do not provide the same documented, specific, enforceable commitment that a signed written agreement delivers. This falls short of the playbook's acceptable position of "written confidentiality agreements."

General Terms §7.1 continues to govern access to Confidential Information outside the DPA's scope (e.g., non-personal data Confidential Information such as business plans or pricing), and in that context, written agreements are required. However, for the data-protection concern motivating this playbook item — the personal data processing context — DPA §3.4's weaker formulation is the controlling language.

Classification: YELLOW. The topic is affirmatively addressed across both instruments, and HubSpot does require some form of confidentiality obligation on personnel. However, the governing DPA §3.4 provision does not strictly require written confidentiality agreements, accepting statutory duties as adequate alternatives. This is weaker than the playbook's acceptable position and creates a meaningful gap: there is no contractual guarantee that all personnel accessing Customer Data have executed a written confidentiality agreement.

— Superseding reasoning —
DPA §3.4 supersedes General Terms §7.1 for the specific context of personnel processing Customer Personal Data, on two independent grounds: (1) Document hierarchy — the DPA contains an explicit precedence clause ("In case of any conflict or inconsistency with other terms included in the Agreement, this DPA will take precedence to the extent of such conflict or inconsistency"), and the General Terms §7.1 requirement for signed confidentiality agreements is inconsistent with DPA §3.4's express permission to satisfy the obligation through statutory duties alone; (2) Specificity — DPA §3.4 is a narrower provision that specifically addresses personnel authorized to Process Customer Personal Data, while General Terms §7.1 addresses Confidential Information access broadly across both parties. The governing language is DPA §3.4: "appropriate confidentiality obligations (whether a contractual or statutory duty)." General Terms §7.1 continues to govern access to Confidential Information that falls entirely outside the DPA's scope.

> *"limit access to Confidential Information of the Disclosing Party to those of its and its Affiliates' employees, contractors and agents who need such access for purposes consistent with this Agreement and who have signed confidentiality agreements with the Receiving Party containing protections no less stringent than those herein."*
> — Customer Terms of Service
> *"We will ensure that any personnel whom we authorize to Process Customer Personal Data on our behalf is subject to appropriate confidentiality obligations (whether a contractual or statutory duty) with respect to that Customer Personal Data."*
> — Data Processing Agreement

## Need-to-Know Access

**AI Comment:** The playbook item requires that vendor employees access customer data only on a need-to-know basis. HubSpot's agreement addresses this requirement through a layered, mutually reinforcing framework spanning the General Terms and the DPA Security Annex.

**Layer 1 — Contractual Need-to-Know Obligation (General Terms §7.1):** The confidentiality provision expressly limits access to Confidential Information — which per General Terms §1.45 expressly includes "Customer Data...regardless of whether or not it is designated as confidential" — to employees, contractors, and agents "who need such access for purposes consistent with this Agreement." This is a direct contractual embodiment of the need-to-know principle, scoped to all Customer Data, not merely Personal Data.

**Layer 2 — Personnel Confidentiality Obligations (DPA §3.4):** HubSpot commits that all personnel authorized to process Customer Personal Data are subject to "appropriate confidentiality obligations (whether a contractual or statutory duty)." This reinforces access limitations with individual-level accountability.

**Layer 3 — Technical and Operational Controls (DPA Annex 2 §2.3):** The Security Annex provides substantive operational specifics: only a subset of employees may access customer data; access is granted exclusively via Just-in-Time Access (JITA) controls (meaning access is temporary and request-specific, not standing); access is role-based; all access requests are logged; high-risk privilege grants are reviewed daily; administrative and high-risk permissions are audited at least semi-annually. This combination of JITA + role-based access + logging + periodic review constitutes a technically robust implementation of the need-to-know principle.

The acceptable position is fully met. No provisions were identified that contradict or dilute these controls. The provisions are complementary across documents — the General Terms establish the contractual obligation, the DPA establishes personnel-level confidentiality duties, and the DPA Security Annex provides the technical enforcement mechanisms. Since no ideal preference was specified, aiPreferenceMet is set to false.

— 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. "Privileged Access Management: Privileged access in our product environment is controlled, monitored, and removed in a timely fashion through "just in time access" (or "JITA") controls. Non-personal ac…"

> *"limit access to Confidential Information of the Disclosing Party to those of its and its Affiliates' employees, contractors and agents who need such access for purposes consistent with this Agreement and who have signed confidentiality agreements with the Receiving Party containing protections no less stringent than those herein."*
> — Customer Terms of Service
> *"Subject to the foregoing exclusions, Customer Data will be considered Confidential Information under this Agreement regardless of whether or not it is designated as confidential."*
> — Customer Terms of Service
> *"We will ensure that any personnel whom we authorize to Process Customer Personal Data on our behalf is subject to appropriate confidentiality obligations (whether a contractual or statutory duty) with respect to that Customer Personal Data."*
> — Data Processing Agreement
> *"Product access: A subset of our employees have access to the products and to customer data via controlled interfaces. The intent of providing access to a subset of employees is to provide effective customer support, product development and research, to troubleshoot potential problems, to detect and respond to security incidents and implement data security. Access is enabled through JITA requests for access; all such requests are logged. Employees are granted access by role, and reviews of high risk privilege grants are initiated daily. Administrative or high risk access permissions are reviewed at least once every six months."*
> — Data Processing Agreement

## Non Solicitation of Employees

**AI Comment:** The HubSpot Customer Terms of Service (General Terms), Product Specific Terms, Data Processing Agreement, Acceptable Use Policy, and Privacy Policy are completely silent on non-solicitation of employees. No provision in any document restricts either party from soliciting, recruiting, or hiring the other party's personnel during or after the Subscription Term.

Acceptable Position Assessment: The acceptable position requires that, if a non-solicitation clause exists, it must include a carve-out disclaiming instances where applicants respond to general public job postings. Because no non-solicitation clause exists at all, there is nothing to evaluate against this threshold — and the threshold is exceeded by the complete absence of any restriction.

Ideal Preference Assessment: The ideal preference is for no limitations on solicitation whatsoever, with an additional disclaimer for recruiter referrals. Complete contractual silence achieves this ideal in full: the Customer faces zero contractual prohibition on soliciting, recruiting, or hiring HubSpot employees through any channel — direct solicitation, public job postings, or recruiter referrals alike. This outcome is strictly more favorable to the Customer than even the ideal preference contemplates.

Silence Framework Note: The standard silence-defaults-to-RED framework applies where a required protective provision is absent. This item is structurally different: the preferred outcome IS the absence of a restriction. Applying a RED classification for silence here would be analytically incorrect — it would penalize the Customer for the most favorable possible contractual outcome. Classification is therefore GREEN with the ideal preference met.

Governing Jurisdiction Note: Under Massachusetts law (the default governing jurisdiction per §11.2 of the General Terms), non-solicitation of employee agreements are generally enforceable when reasonable in scope and duration. The absence of any such clause contractually frees the Customer to hire HubSpot personnel without restriction, which is fully consistent with Massachusetts law and the Customer's interests.

Amendment Risk: Per §12.1 of the General Terms, HubSpot may modify the Agreement unilaterally with notice. If HubSpot were to introduce a non-solicitation clause in a future amendment, the Customer has 30 days to object and, if it cannot operate under the modification, terminate with a pro-rated refund. This forward-looking risk does not affect the current classification but is noted for awareness.

Confidence: HIGH. All five documents were reviewed in full. No non-solicitation, non-hire, or employee solicitation restriction language was identified in any document at any section level.

## Vendor Audit Rights

**AI Comment:** The DPA's "Demonstration of Compliance" section (§7) addresses audit rights across four distinct provisions, but collectively imposes three material limitations that fall short of an unconditional right to audit the vendor's systems and DPA compliance as the playbook's acceptable position requires.

**Limitation 1 — Direct inspections conditioned on applicable law:** The operative grant of direct inspection rights reads: "allow for and contribute to audits, including inspections conducted by you or your auditor in order to assess compliance with this DPA, **where required by applicable law**." The phrase "where required by applicable law" subordinates the contractual inspection right to a statutory trigger rather than making it an unconditional bargained-for right. For European customers subject to GDPR Article 28(3)(h), this trigger is effectively always present. For the default governing jurisdiction here (Commonwealth of Massachusetts, U.S.A.), no analogous statute mandates an unconditional vendor audit right, which means the practical scope of direct system access is materially constrained under the default jurisdiction.

**Limitation 2 — Prescribed (channeled) mechanism, not free-form access:** Even where applicable law would activate the right, the customer is expressly required to exercise audit rights "by instructing [HubSpot] to comply with the audit measures described in this 'Demonstration of Compliance' section" — i.e., receiving SOC 2 reports, penetration test summaries, and written questionnaire responses. This is an indirect, document-based compliance verification mechanism, not direct access to vendor systems or records.

**Limitation 3 — Annual frequency cap on written information requests:** The written-response mechanism is capped at once per calendar year "unless you have reasonable grounds to suspect noncompliance." This imposes a further constraint on the customer's ability to verify compliance on demand.

The SOC 2 Type II certification and independent penetration testing provide meaningful third-party compliance assurance and are not without value. However, they substitute for — rather than constitute — a direct contractual audit right. The SCC channeling provision (§11.2(E)) further confirms that even SCC Clause 8.9-triggered audit rights are funneled through the same constrained mechanism.

No silence downgrade applies; the topic is addressed but with materially weaker and narrower protections than the playbook item requires. At HIGH weight, this finding requires documented assessment.

> *"We will make all information reasonably necessary to demonstrate compliance with this DPA available to you and allow for and contribute to audits, including inspections conducted by you or your auditor in order to assess compliance with this DPA, where required by applicable law."*
>
> — Data Processing Agreement
>
> *"You acknowledge and agree that you will exercise your audit rights under this DPA by instructing us to comply with the audit measures described in this 'Demonstration of Compliance' section."*

— Data Processing Agreement
*"You acknowledge that the Subscription Service is hosted by our hosting Sub-Processors who maintain independently validated security programs (including SOC 2 and ISO 27001) and that our systems are audited annually as part of SOC 2 compliance and regularly tested by independent third party penetration testing firms. Upon request, we will supply (on a confidential basis) our SOC 2 report and summary copies of our penetration testing report(s) to you so that you can verify our compliance with this DPA."*
— Data Processing Agreement
*"Further, at your written request, we will provide written responses (on a confidential basis) to all reasonable requests for information made by you necessary to confirm our compliance with this DPA, provided that you will not exercise this right more than once per calendar year unless you have reasonable grounds to suspect noncompliance with the DPA."*
— Data Processing Agreement
*"You also acknowledge and agree that you will exercise your audit rights under Clause 8.9 of the Standard Contractual Clauses by instructing us to comply with the measures described in the 'Demonstration of Compliance' section of this DPA."*
— Data Processing Agreement

## Data Ownership

**AI Comment:** HubSpot's General Terms §5.1 explicitly states "You own and retain all rights to the Customer Materials and Customer Data," and since "Customer Data" is defined as all information submitted or collected via the Subscription Service (General Terms §1, "Customer Data" definition), and "Personal Data" is defined as a subset of that category, the baseline ownership affirmation covers Personal Data. This would support GREEN for a general data-ownership requirement. However, the playbook item requires that ALL Personal Data remains the SOLE property of the customer — i.e., exclusive rights with no independent vendor entitlement — and this heightened standard is not fully satisfied under the standard terms for three distinct reasons:

1. AI TRAINING DEFAULT (§5.3.1): HubSpot's default position is that it may use Customer Data (which includes Personal Data) to develop and train its AI models. Opt-out is available, but it must be actively exercised by the customer. A "sole property" standard implies that any use of the customer's Personal Data for the vendor's own purposes requires an affirmative grant; the opt-out structure inverts this, creating a default entitlement in HubSpot's favor.

2. TRACKING CODE DATA (§5.3.2): HubSpot reserves the right to use Website Data collected via the HubSpot Tracking Code — expressly including Personal Data such as IP addresses and online identifiers — "to provide, maintain, append, improve, enhance, and develop [HubSpot's] commercial dataset." This is an independent commercial use of Personal Data with no customer opt-out mechanism in the standard terms.

3. ENRICHMENT CONTEXT — EXPLICIT SUPERSEDING CLAUSE + RECLASSIFICATION AS HUBSPOT CONTENT (PST §6.5(ii), PST §6.3, General Terms §6.1): For customers using enrichment products, PST §6.5(ii) explicitly authorizes HubSpot to use Enrichment Data (including Professional Enrichment Data, defined as Personal Data such as email addresses) to develop its commercial dataset. Critically, this provision declares it "supersedes any prior or conflicting terms," overriding the general ownership affirmation in §5.1 for this context. Once Personal Data is incorporated into Enrichment Outputs or HubSpot's commercial dataset, PST §6.3 reclassifies it as "HubSpot Content," and General Terms §6.1 vests all IP rights in that Content in HubSpot. The DPA's Controller-to-Controller framework (§10.2) further formalizes HubSpot's status as an independent Controller over certain Personal Data in the enrichment/tracking code context, giving it autonomous data rights that are structurally inconsistent with the customer holding "sole" ownership.

The ownership affirmation in §5.1 is genuine and contractually meaningful for the core service delivery context. But the combination of the AI training default, tracking code data commercialization, and the enrichment-context explicit superseding/reclassification chain means the standard terms do not ensure that "all Personal Data remains sole property of our company" across all in-scope scenarios. YELLOW is the appropriate classification: the playbook's baseline ownership threshold is met, but the "sole property" standard is not.

— Superseding reasoning —
PST §6.5(ii) (PIF index 3) contains an express superseding clause: "this authorization is necessary for the functionality of enrichment products and supersedes any prior or conflicting terms." This language explicitly displaces the general customer ownership affirmation in General Terms §5.1 (PIF index 0) for the enrichment product context. Additionally, the DPA preamble states "In case of any conflict or inconsistency with other terms included in the Agreement, this DPA will take precedence to the extent of such conflict or inconsistency" — meaning the Controller-to-Controller structure in DPA §10.2 (PIF index 5) governs over any general ownership language when enrichment products or the HubSpot Tracking Code (with Intent data sharing) are in use. These represent two separate superseding chains, both operating to limit the customer's "sole property" claim in defined contexts.

— 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. "We may use data collected through the HubSpot Tracking Code, which may include Personal Data such as IP addresses and other online identifiers ("Website Data") to provide, maintain, append, improve, e…"
*"You own and retain all rights to the Customer Materials and Customer Data."*
— Customer Terms of Service
*"We may use Customer Data to develop, support, and improve HubSpot AI features and functionality. We may also use Customer Data to train our AI models in compliance with our obligations under the Agreement. You may opt out of having your Customer Data used for this purpose by updating your settings in your HubSpot account."*
— Customer Terms of Service

> *"You acknowledge we may use Enrichment Data to provide, maintain, append, improve, enhance, and develop our commercial dataset and the Subscription Services; this authorization is necessary for the functionality of enrichment products and supersedes any prior or conflicting terms."*
> — Product Specific Terms
> *"For the avoidance of doubt, our commercial dataset and Enrichment Outputs are considered HubSpot Content."*
> — Product Specific Terms
> *"The parties acknowledge and agree that they act as Controllers of Controller Personal Data and will comply with their respective obligations under Data Protection Laws when Processing Controller Personal Data."*
> — Data Processing Agreement

## Arbitration or other dispute resolution process

**AI Comment:** The acceptable position for this item is "no limitation as to method of dispute resolution" — meaning the customer objects to mandatory arbitration or other alternative dispute resolution (ADR) clauses that would foreclose traditional court-based litigation.

HubSpot's Customer Terms of Service do not contain a mandatory arbitration clause, class-action waiver, or any requirement to use ADR as a precondition to or substitute for court litigation. Section 11.2 expressly routes disputes to the courts of Boston, Massachusetts — a court-based mechanism — without requiring or even mentioning arbitration, mediation, or any other ADR method. This satisfies the acceptable position: the method of dispute resolution is not limited away from court litigation.

One related provision warrants notation: §12.3 (Actions Permitted) imposes a one-year contractual limitation period for most claims (excluding nonpayment and IP breaches). This shortens the default statutory window within which a party may bring an action, regardless of forum. It does not change the METHOD of dispute resolution, but it does narrow dispute resolution rights in a meaningful temporal sense. For this item specifically — which addresses method, not timing — it is classified separately as a secondary, peripheral finding.

Because the weight is "Acceptable to Deviate," the exclusive forum clause (Boston, MA courts) is noted as a practical consideration (it may be burdensome for non-Massachusetts customers) but does not constitute a limitation on the METHOD of dispute resolution and does not degrade the GREEN classification. No ideal preference was specified, so aiPreferenceMet is false.

— 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. "If your (i) Customer Location is in North America or South America, (ii) you are located in a geographic region that does not otherwise fall into one of the designations described in the Jurisdiction …"
2. "Except for actions for nonpayment or breach of a party's proprietary rights, no action, regardless of form, arising out of or relating to this Agreement may be brought by either party more than one (1…"

## Indemnification – Vendor to Our Company

**AI Comment:** The playbook item requires vendor indemnification covering two distinct categories: (1) intellectual property infringement claims and (2) data breaches. HubSpot's terms address only one of these two requirements.

**IP Indemnification — Partially Met.** Section 9.2 of the General Terms provides a vendor-side IP indemnification obligation covering claims that the Subscription Service infringes a valid patent (in PCT member states), a registered trademark, or a registered copyright. The covered-party scope is broad (customer and its officers, directors, employees, agents, service providers, licensors, and affiliates), and critically, the General Terms' §10.4 liability cap expressly carves out HubSpot's IP indemnification obligations — meaning IP indemnification claims are not subject to the standard 12-month-fees aggregate cap. These are meaningful structural protections. However, five carve-outs in §9.2 materially narrow the obligation's practical reach: combinations with non-HubSpot hardware/software, modifications, out-of-scope use, functions traditionally used in marketing/sales/services software that are not commercially unique to HubSpot's offering (a potentially broad exclusion given HubSpot's product category), and user interface elements not provided by HubSpot. The "sole and exclusive remedy" limitation also forecloses supplemental theories of recovery for IP claims.

**Data Breach Indemnification — Absent.** No provision across the General Terms, DPA, Product Specific Terms, AUP, or Privacy Policy indemnifies the customer for losses, costs, or third-party claims arising from a data breach. The DPA §3.5 addresses data breach response through a 72-hour notification obligation and assistance with regulator/data-subject notifications — obligations that are related to breach response but are not indemnification. DPA §12.3 further confirms that all DPA-related liability (including any breach-related liability) is subject to the General Terms' 12-month aggregate cap, reinforcing that no standalone data breach indemnification exists.

**Weight Consideration.** The item is weighted "Acceptable to Deviate," placing this in the informational/low-priority tier. Nonetheless, the combination of (a) meaningful carve-outs qualifying the IP indemnification and (b) the complete absence of data breach indemnification prevents a GREEN classification. The overall finding is YELLOW: the topic is addressed, but with weaker protection and a gap on the data breach component.

— 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. "We will indemnify, defend and hold you harmless, at our expense, against any Action brought against you (and your officers, directors, employees, agents, service providers, licensors, and Affiliates) …"

> *"We will not have any obligation or liability under this section if the alleged Action is caused by or based on: (i) any combination of the Subscription Service with any hardware, software, equipment, or data not provided by us, (ii) modification of the Subscription Service by anyone other than us, or modification of the Subscription Service by us in accordance with specifications or instructions that you provided, (iii) use of the Subscription Service in violation of or outside the scope of this Agreement, (iv) an allegation that the Subscription Service consists of a function, system or method traditionally utilized in marketing, sales or services software that is not commercially unique to the Subscription Service, and the commercially unique aspects of the Subscription Service are not identified in the allegation giving rise to the Action, or (v) user interface or related user design elements not provided by us."*
> — Customer Terms of Service

## Indemnification – Our Company to Vendor

**AI Comment:** The customer indemnification obligation in HubSpot's Customer Terms of Service (§9.1) meets the acceptable position established by this playbook item. The obligation is explicitly and unambiguously limited to "third-party claims, suits, actions, or proceedings… brought against us… by a third party not affiliated with us or our Affiliates." There is no first-party or direct indemnification obligation imposed on the customer — the structure is classic third-party-claim-only indemnification.

The four indemnification triggers are: (i) unauthorized or illegal use of the Subscription Service; (ii) noncompliance with or breach of the Agreement; (iii) use of Third-Party Products; and (iv) unauthorized use by any person using the customer's User credentials. Trigger (ii) — breach of the Agreement — is broad and could encompass many scenarios, but it remains constrained by the "third-party claim" gateway. Trigger (iii) — Third-Party Products — is somewhat unusual: it requires the customer to indemnify HubSpot for claims arising from the customer's use of third-party integrations, which could sweep in claims that are more properly attributable to the third-party product itself. However, it remains within the third-party-claim scope.

One significant ancillary concern: §10.4 (Limitation of Liability) explicitly carves out the customer's indemnification obligations from the aggregate liability cap (twelve months of fees). This means the customer's indemnification exposure under §9.1 is effectively uncapped. This is a common SaaS market position but materially increases the risk profile of the obligation and should be noted at contract review.

The settlement restriction in §9.1 (requiring HubSpot's prior written consent for any settlement that imposes obligations, admissions, or restrictions on HubSpot) is commercially standard.

Because the acceptable position — "any obligation should be limited to third-party claims" — is met, and because the item weight is Acceptable to Deviate, the overall classification is GREEN. The aspirational ideal of "no indemnification obligation" is not achieved (aiPreferenceMet = false), but the acceptable threshold is satisfied.

— 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. "TO THE EXTENT PERMITTED BY LAW, AND EXCEPT FOR (i) YOUR LIABILITY FOR PAYMENT OF FEES, (ii) YOUR LIABILITY ARISING FROM YOUR OBLIGATIONS UNDER THE 'INDEMNIFICATION' SECTION, (iii) OUR LIABILITY ARISIN…"

> *"You will indemnify, defend and hold us and our Affiliates harmless, at your expense, against any third-party claim, suit, action, or proceeding (each, an "Action") brought against us (and our officers, directors, employees, agents, service providers, licensors, and Affiliates) by a third party not affiliated with us or our Affiliates to the extent that such Action is based upon or arises out of*
>
> *(i) unauthorized or illegal use of the Subscription Service by you or your Affiliates,*
>
> *(ii) your or your Affiliates' noncompliance with or breach of this Agreement,*
>
> *(iii) your or your Affiliates' use of Third-Party Products, or*
>
> *(iv) the unauthorized use of the Subscription Service by any other person using your User information."*
> — Customer Terms of Service
> *"We will: notify you in writing within thirty (30) days of our becoming aware of any such Action; give you sole control of the defense or settlement of such Action; and provide you (at your expense) with any and all information and assistance reasonably requested by you to handle the defense or settlement of the Action. You will not accept any settlement that (i) imposes an obligation on us; (ii) requires us to make an admission; or (iii) imposes liability not covered by these indemnifications or places restrictions on us without our prior written consent."*
> — Customer Terms of Service

## Modification of Terms

**AI Comment:** The acceptable position — that the customer can access some form of the modified terms — is clearly met across all components of the HubSpot agreement. HubSpot: (1) posts revised terms publicly at legal.hubspot.com effective the next business day after posting; (2) notifies customers via in-app notification or email; (3) maintains a publicly accessible archive of prior versions at legal.hubspot.com/archive; and (4) applies the same notification mechanism consistently to the DPA and AUP. A customer can always locate both current and historical agreement text.

However, the ideal preference — advance written notice plus a customer-initiated right to terminate with a pro-rata refund upon disagreement — is NOT met on either prong:

1. Advance Notice Gap: The revised terms become "effective and binding the next business day after it is posted" (§12.1). Notice is dispatched at or around the time of posting, meaning the advance window before binding effectiveness is essentially one business day. This does not constitute meaningful advance notice that would allow a customer to evaluate and act on material changes before they take effect.

2. No Customer-Initiated Termination + Pro-Rata Refund Right: The customer's sole contractual remedy upon disagreement is to notify HubSpot in writing within 30 days and thereby preserve the old terms through the end of the current renewal period — after which the new terms apply regardless. A pro-rata refund of unused prepaid fees is only available in the narrow circumstance where HubSpot itself determines it "can no longer reasonably provide the subscription" under the prior terms (e.g., a legally required change). This is HubSpot's unilateral determination, not a customer-exercisable termination right. Customers who object to a modification but cannot benefit from that narrow carve-out are left with the choice of accepting new terms at renewal or non-renewing at term end — no mid-term exit with refund is available simply because they disagree with a change.

Overall classification: GREEN (acceptable position met). Weight: High. Alignment is sufficient for the minimum acceptable threshold. The ideal preference gap — particularly the absence of a customer-initiated termination-plus-refund right — should be noted as a negotiation point for higher-stakes renewals.

— 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. "We may modify any part or all of the Agreement by posting a revised version at http://legal.hubspot.com/. The revised version will become effective and binding the next business day after it is posted…"
2. "If you do not agree with a modification to the Agreement, you must notify us in writing within thirty (30) days after we send notice of the revision. If you give us this notice, then your subscription…"
3. "We update these terms from time to time. If you have an active HubSpot subscription, we will let you know when we update the terms via in-app notification or by email (if you subscribe to receive emai…"
4. "Notwithstanding anything else to the contrary in the Agreement and without prejudice to the 'Compliance with Instructions' or 'Security' sections of this DPA, we reserve the right to make any updates …"
5. "We may update and change any part or all of this AUP. If we update or change this AUP, the updated AUP will be posted at http://legal.hubspot.com/acceptable-use. If you have a HubSpot subscription, we…"

## Vendor's liability

**AI Comment:** The playbook item requires a risk assessment of vendor liability given the type of data shared, with a preference for uncapped vendor liability and, at minimum, vendor maintaining some form of liability for data breaches (High weight).

HubSpot's terms create a two-layer limitation that significantly constrains practical recovery in a data breach scenario:

**Layer 1 — Exclusion of indirect/consequential damages (§10.3):** Data breach losses typically include notification costs, regulatory fines, business disruption, and reputational harm. The bulk of these are indirect or consequential in nature and are entirely excluded — for both parties — under §10.3. This is the more consequential restriction because it operates before the cap is even reached.

**Layer 2 — 12-month fee cap (§10.4):** Residual direct damages are capped at fees paid in the 12 months preceding the claim. Critically, HubSpot's IP indemnification is carved out from this cap (i.e., uncapped), but data breach liability is not similarly carved out. This asymmetry — unlimited IP liability, capped data breach liability — represents a risk allocation that disfavors the customer on privacy-related claims.

**Partial mitigation — DPA §12.3 carve-out:** The DPA's limitation of liability clause explicitly incorporates the General Terms cap for DPA-related claims, but adds a meaningful exception: "In no event will either party's liability be limited with respect to any individual's data protection rights under this DPA." This carve-out preserves uncapped liability for individual data subject rights claims (e.g., under GDPR Article 82, CCPA, or analogous statutes). For a default Massachusetts-governed agreement, the practical scope of this carve-out is more limited than it would be under EU/UK law, but it represents a genuine protective element.

**DPA §3.5 — Breach notification:** HubSpot commits to 72-hour breach notification with ongoing assistance obligations, demonstrating that accountability for data incidents is not entirely disclaimed.

**Acceptable-threshold assessment:** The acceptable threshold — vendor maintains *some form* of liability for data breaches — is technically met: liability is not zeroed out, and the DPA carve-out for data protection rights provides a meaningful uncapped pathway for individual-rights claims. However, the practical utility of this protection is materially undermined by the consequential damages exclusion, which would likely eliminate the largest components of breach-related loss. The ideal of uncapped vendor liability is not met.

**Classification rationale:** YELLOW — the acceptable threshold is technically satisfied but practically weakened by the consequential damages exclusion, and the ideal (uncapped) is not met. For a High weight item, this gap warrants documented review. The customer should consider whether the 12-month cap provides adequate financial cover given actual subscription fees relative to the potential cost of a data incident, and whether the DPA's data-protection-rights carve-out provides sufficient protection under the applicable jurisdiction.

— Superseding reasoning —
DPA §12.3 explicitly incorporates the General Terms §10.4 liability cap for all DPA-related claims, then adds a specific carve-out: "In no event will either party's liability be limited with respect to any individual's data protection rights under this DPA." This carve-out, combined with the DPA's general precedence clause (DPA §3.4: "In case of any conflict or inconsistency with other terms included in the Agreement, this DPA will take precedence"), means that for the specific class of individual data protection rights claims, the DPA §12.3 carve-out supersedes the general 12-month cap in General Terms §10.4. For all other DPA-related claims, the General Terms cap governs by the DPA's own explicit incorporation. The consequential damages exclusion in §10.3 is not displaced by the DPA and continues to apply across all claim types (the DPA does not address or conflict with it).

— 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. "TO THE EXTENT PERMITTED BY LAW, AND EXCEPT FOR (i) YOUR LIABILITY FOR PAYMENT OF FEES, (ii) YOUR LIABILITY ARISING FROM YOUR OBLIGATIONS UNDER THE 'INDEMNIFICATION' SECTION, (iii) OUR LIABILITY ARISIN…"
2. "Each party and each of their Affiliates' liability, taken in aggregate, arising out of or related to this DPA (including any other data processing agreements between the parties) and the Standard Cont…"

> *"TO THE EXTENT PERMITTED BY LAW, IN NO EVENT WILL EITHER PARTY OR ITS AFFILIATES BE LIABLE FOR ANY INDIRECT, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES, OR LOSS OF PROFITS, REVENUE, DATA OR BUSINESS OPPORTUNITIES ARISING OUT OF OR RELATED TO THIS AGREEMENT, WHETHER AN ACTION IS IN CONTRACT OR TORT AND REGARDLESS OF THE THEORY OF LIABILITY."*
> — Customer Terms of Service

## Background Check Requirements

**AI Comment:** The playbook item has three operative components: (1) confirm the vendor performs background checks on its own personnel; (2) confirm no requirement is imposed on the customer to perform background checks; and (3) confirm that any customer-facing background check obligation does not extend to subprocessors.

**Component 1 — Vendor performs background checks: CONFIRMED.** DPA Annex 2, Section 7 (Personnel Management) explicitly states that HubSpot employees undergo third-party background or reference checks where permitted by applicable law, and that in the United States employment offers are contingent on a third-party background check result. This is a clear, affirmative statement of vendor practice.

**Component 2 — Customer not required to perform background checks: CONFIRMED.** A thorough review of all four documents (Customer ToS, Product Specific Terms, DPA, and AUP) reveals no language anywhere that imposes a background check obligation on the customer, either as a standalone requirement or as a condition of using the Subscription Service.

**Component 3 — Customer obligation does not extend to subprocessors: MOOT.** Because no background check requirement exists on the customer at all, the sub-processor carve-out concern does not arise in practice.

**Ancillary observation (not a playbook deficiency):** The Annex 2 background check language is scoped to "HubSpot employees." It does not expressly state whether HubSpot contractually requires its Sub-Processors to conduct background checks on their own personnel. DPA Section 5 does require HubSpot to impose data protection terms on Sub-Processors providing "at least the same level of protection" as the DPA, which could arguable encompass the Annex 2 security measures — but this is not made explicit for background checks specifically. This is noted as an observation; it does not bear on the playbook item's acceptable position (which is focused on obligations on the customer, not on sub-processor personnel vetting).

**Classification: GREEN.** All components of the acceptable position are satisfied. Weight is Acceptable to Deviate, confirming minimal risk impact. aiPreferenceMet is false as no ideal preference was specified.

> *"Background checks: Where permitted by applicable law, HubSpot employees undergo a third-party background or reference check. In the United States, employment offers are contingent upon the results of a third-party background check. All HubSpot employees are required to conduct themselves in a manner consistent with company guidelines, non-disclosure requirements, and ethical standards."*
> — Data Processing Agreement

## Security Training

**AI Comment:** The acceptable position requires that vendor employees who access data attend security training at least annually. HubSpot's DPA Annex 2 (Annex 2, Section 7 — Personnel Management) addresses employee security training, confirming that "all employees" are trained "on security policy, processes, and standards relevant to their role and in accordance with industry practice." This establishes that a security training program exists and that it applies broadly to all employees — which encompasses those with access to customer data.

However, the clause falls short of the playbook's acceptable position in two respects: (1) it specifies no frequency — neither annual nor any other cadence — and (2) the governing standard is the open-ended phrase "in accordance with industry practice," which is a flexible benchmark rather than a binding minimum commitment. "Industry practice" could encompass a range of frequencies (e.g., annual, biennial, ad hoc), but nothing in the agreement locks HubSpot to the annual floor the playbook requires.

Because the topic is substantively addressed — an all-employee security training obligation exists and is contractually committed — a RED classification is not warranted. However, because the governing language provides meaningfully weaker protection than the acceptable position (no annual commitment, no frequency floor), YELLOW is the appropriate classification. No other document in the set addresses this topic, so no superseding analysis is required. The contract is not silent; it is partially responsive with insufficient specificity.

> *"PERSONNEL MANAGEMENT*
>
> *We staff qualified personnel to develop, maintain, and enhance our security program. We train all employees on security policy, processes, and standards relevant to their role and in accordance with industry practice.*
>
> *"*
>
> — Data Processing Agreement

## Subprocessor Audit Rights

**AI Comment:** The playbook item requires a direct right to audit Subprocessors' systems and their compliance with the DPA. The HubSpot DPA addresses subprocessor oversight in multiple places, but does not grant the customer any direct right to inspect or audit Subprocessors' systems.

What the DPA provides instead is a layered, indirect oversight framework: (1) HubSpot imposes equivalent data protection obligations on Subprocessors (§5) and remains liable for their acts and omissions; (2) customers may request HubSpot's own SOC 2 report and penetration test summaries to verify HubSpot's compliance (§7); (3) customers may submit written information requests to HubSpot once per calendar year (§7); and (4) SCC Clause 8.9 audit rights — which under the standard contractual clauses would normally include broader access rights — are explicitly channeled by HubSpot into this same document-based Demonstration of Compliance framework (§11.2), rather than permitting direct access to Subprocessors.

Critically, the DPA acknowledges HubSpot "may be restricted from disclosing Sub-Processor agreements" (§11.2), which further limits practical transparency into Subprocessor arrangements. Subprocessor infrastructure providers maintain independent SOC 2 Type II and ISO 27001 certifications, which HubSpot presents as a proxy for direct customer audit access.

The overall structure means that all audit activity flows through HubSpot as an intermediary — customers audit HubSpot; HubSpot oversees Subprocessors. This is a materially weaker position than the playbook requirement, which calls for a direct customer right to audit Subprocessors' systems and DPA compliance. The topic is substantively addressed, and HubSpot's retained responsibility for Subprocessor compliance provides meaningful indirect protection, but the specific direct audit right is absent. Classification is YELLOW. Given the High weight, this gap requires documented justification before acceptance.

— Superseding reasoning —
PIF at index 6 (DPA §11.2 — SCC Clause 8.9 channeling) is more specific than PIF at index 0 (DPA §7 — general audit language). Section §7 contains broad language about HubSpot allowing "audits, including inspections conducted by you or your auditor." However, §11.2 explicitly and specifically directs that any audit rights arising under SCC Clause 8.9 must be exercised exclusively through the Demonstration of Compliance mechanism (SOC 2 reports, written responses). Because §11.2 is the specific provision governing the exercise of the customer's audit entitlements — including those flowing from the incorporated SCCs — it governs over the general §7 language for the purpose of determining what audit mechanisms are actually available in practice. The effective audit right is therefore the document-based framework (SOC 2 reports, pen test summaries, written questionnaires capped at once per year), not on-site inspection of HubSpot or its Subprocessors.

— 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. "We will remain responsible for each Sub-Processor's compliance with the obligations of this DPA and for any acts or omissions of such Sub-Processor that cause us to breach any of its obligations under…"

> *"We will make all information reasonably necessary to demonstrate compliance with this DPA available to you and allow for and contribute to audits, including inspections conducted by you or your auditor in order to assess compliance with this DPA, where required by applicable law."*
> — Data Processing Agreement
> *"You acknowledge that the Subscription Service is hosted by our hosting Sub-Processors who maintain independently validated security programs (including SOC 2 and ISO 27001) and that our systems are audited annually as part of SOC 2 compliance and regularly tested by independent third party penetration testing firms."*
> — Data Processing Agreement
> *"Upon request, we will supply (on a confidential basis) our SOC 2 report and summary copies of our penetration testing report(s) to you so that you can verify our compliance with this DPA."*
> — Data Processing Agreement
> *"Further, at your written request, we will provide written responses (on a confidential basis) to all reasonable requests for information made by you necessary to confirm our compliance with this DPA, provided that you will not exercise this right more than once per calendar year unless you have reasonable grounds to suspect noncompliance with the DPA."*
> — Data Processing Agreement
> *"Where we engage Sub-Processors, we will impose data protection terms on the Sub-Processors that provide at least the same level of protection for Customer Personal Data as those in this DPA, to the extent applicable to the nature of the services provided by such Sub-Processors."*
> — Data Processing Agreement

> *"You also acknowledge and agree that you will exercise your audit rights under Clause 8.9 of the Standard Contractual Clauses by instructing us to comply with the measures described in the 'Demonstration of Compliance' section of this DPA."*
> — Data Processing Agreement
> *"For the purposes of Clause 9(c) of the Standard Contractual Clauses, you acknowledge that we may be restricted from disclosing Sub-Processor agreements but we will use reasonable efforts to require any Sub-Processor we appoint to permit it to disclose the Sub-Processor agreement to you and will provide (on a confidential basis) all information we reasonably can."*
> — Data Processing Agreement

## Vendor Rights

**AI Comment:** The acceptable position requires the vendor to transfer ownership of any custom deliverables to the customer. HubSpot's terms do the opposite: §6.1 of the General Terms explicitly states that HubSpot "retain[s] all intellectual property rights to the HubSpot Content, the Subscription Service, the Consulting Services, and any other products or services provided under this Agreement." Consulting Services — the category of service under which custom deliverables would be produced — is expressly called out as IP that HubSpot retains. No assignment, work-for-hire, or ownership-transfer clause exists anywhere in the agreement set. The contract is not silent on this topic; it actively and explicitly conflicts with the acceptable position.

§6.2 compounds the problem: customer feedback and suggestions incorporated into any HubSpot service are also assigned to HubSpot, without payment or attribution, foreclosing even an implied ownership path for customer-originated improvements.

The only provision that moves in the customer's favor is §7.4 of the Product Specific Terms, which confirms that the customer "retain[s] all rights [they] may have to use and exploit [their] AI Output." This is a narrow carve-out limited to AI-generated content produced by HubSpot AI features in response to customer AI Input; it does not extend to consulting deliverables or other custom work product created by HubSpot personnel.

§5.1 confirms that the customer owns Customer Materials and Customer Data — i.e., what the customer puts into the platform — but this does not address what HubSpot creates on the customer's behalf.

The ideal preference ("Vendor may retain rights to its own IP") contemplates a clean IP separation where HubSpot keeps its background/platform IP while the customer receives ownership of bespoke deliverables. HubSpot's terms go materially further: HubSpot retains IP over both its own platform and any custom deliverables produced through Consulting Services, defeating both the acceptable position and the spirit of the preferred arrangement. Accordingly, aiPreferenceMet is false.

Classification: RED — the contract explicitly contradicts the acceptable position. At HIGH weight, this requires senior legal justification to proceed and should be a negotiation priority if custom deliverables are anticipated (e.g., under a Consulting Services engagement).

> *"We retain all intellectual property rights to the HubSpot Content, the Subscription Service, the Consulting Services, and any other products or services provided under this Agreement."*
> — Customer Terms of Service
> *"This is an agreement for access to and use of the Subscription Service, and you are not granted a license to any software by this Agreement."*
> — Customer Terms of Service
> *"You agree that all such comments and suggestions will be non-confidential and that we own all rights to use and incorporate them into the Subscription Service or Consulting Services, without payment or attribution to you."*
> — Customer Terms of Service
> *"Between you and HubSpot, you retain all rights you may have to use and exploit your AI Output."*
> — Product Specific Terms
> *"You own and retain all rights to the Customer Materials and Customer Data."*
> — Customer Terms of Service

## Audit Logging

**AI Comment:** The playbook item requires that it be possible to examine whether and by whom personal data has been entered into, modified, or removed from data processing systems — a comprehensive PII audit trail capability, often associated with GDPR Article 32 accountability and analogous frameworks.

HubSpot's documents address logging across several provisions of DPA Annex 2 and the Demonstration of Compliance section, but they fall meaningfully short of explicitly committing to a customer-accessible audit trail for tracking the customer's own users' individual actions on personal data.

**What the contract establishes:**
1. Broad infrastructure-level logging — HubSpot commits to logging "extensive information about the system behavior, traffic received, system authentication, and other application requests" (DPA Annex 2 §4). This satisfies the "whether" component of the requirement at an infrastructure level.
2. Explicit per-event logging of HubSpot employee access — all JITA (just-in-time access) requests by HubSpot personnel to customer data are logged, with daily reviews of high-risk grants (DPA Annex 2 §2.3). This directly satisfies the "by whom" component, but only for HubSpot's own employees accessing PII — not the customer's own users.
3. Role-based authorization controls — the product enforces access governance by validating user permissions against data sets (DPA Annex 2 §2.1). Permission enforcement is a prerequisite for meaningful audit trails, but is not itself equivalent to retrospective logging of individual access events.

4. SOC 2 Type II compliance with reports available on request (DPA §7). SOC 2 Type II audits typically require implemented audit trail controls as part of the Common Criteria (CC7.x Monitoring), providing structural but indirect assurance that logging capabilities meeting industry standards exist.

**Critical gap — the customer-user dimension:**
None of the provisions explicitly commit to making audit logs available to the customer that record which of the customer's own users (as distinct from HubSpot employees) entered, modified, or removed specific personal data records during their use of the Subscription Service. The logging described is primarily (a) HubSpot's internal infrastructure monitoring and (b) HubSpot employee access to customer systems. The requirement's core use case — a customer or their auditor examining PII access events at the application-user level — is implied by the SOC 2 reference and authorization model, but is not contractually guaranteed as a customer-facing deliverable.

**Classification rationale:** YELLOW is appropriate because the topic is substantively addressed (extensive logging infrastructure is described, SOC 2 compliance provides structural assurance, and HubSpot employee access to PII is explicitly logged), but the protection is narrower than the acceptable position requires. The "by whom" requirement is met only for HubSpot's own personnel; an equivalent commitment for the customer's own users is absent. No log retention periods are specified. No express right to retrieve user-level PII access logs is granted. Given the High weight of this item, this gap warrants negotiation: customers should seek explicit contractual assurance that user-level PII access audit logs are retained and accessible to them for compliance and incident investigation purposes.

— 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. "Customer Data is stored in multi-tenant storage systems accessible to Customers via only application user interfaces and application programming interfaces. Customers are not allowed direct access to …"

> *"We designed our infrastructure to log extensive information about the system behavior, traffic received, system authentication, and other application requests. Internal systems aggregate log data and alert appropriate employees of malicious, unintended, or anomalous activities. Our personnel, including security, operations, and support personnel, are responsive to known incidents."*
> — Data Processing Agreement
> *"Product access: A subset of our employees have access to the products and to customer data via controlled interfaces. The intent of providing access to a subset of employees is to provide effective customer support, product development and research, to troubleshoot potential problems, to detect and respond to security incidents and implement data security. Access is enabled through JITA requests for access; all such requests are logged. Employees are granted access by role, and reviews of high risk privilege grants are initiated daily. Administrative or high risk access permissions are reviewed at least once every six months."*
> — Data Processing Agreement
> *"We will make all information reasonably necessary to demonstrate compliance with this DPA available to you and allow for and contribute to audits, including inspections conducted by you or your auditor in order to assess compliance with this DPA, where required by applicable law. You acknowledge and agree that you will exercise your audit rights under this DPA by instructing us to comply with the audit measures described in this 'Demonstration of Compliance' section. You acknowledge that the Subscription Service is hosted by our hosting Sub-Processors who maintain independently validated security programs (including SOC 2 and ISO 27001) and that our systems are audited annually as part of SOC 2 compliance and regularly tested by independent third party penetration testing firms. Upon request, we will supply (on a confidential basis) our SOC 2 report and summary copies of our penetration testing report(s) to you so that you can verify our compliance with this DPA."*
> — Data Processing Agreement
> *"We will maintain commercially appropriate administrative, physical, and technical safeguards to protect Personal Data as described in the DPA, including our Security Measures in Annex 2 of our DPA."*
> — Customer Terms of Service

## Regulatory Disclosure Procedure

**AI Comment:** The playbook item requires three cumulative protections: (1) Vendor must forward any regulatory/legal authority contact to the Customer; (2) unless legally prohibited from doing so; and (3) Vendor must await Customer's instructions before acting on the request. The contract partially addresses all three elements but falls short on the critical third element — the explicit commitment to hold action pending Customer direction.

The primary governing provision is §7.2 of the General Terms (Confidential Information Disclosure). It satisfies element (1) — HubSpot must "refer the request to the Disclosing Party" — and element (2) — the notification obligation is excused "if such notice is prohibited by law." It also provides meaningful supplementary protections: prompt notice "sufficient to allow the Disclosing Party to object to the request and/or seek an appropriate protective order," and an obligation to provide reasonable assistance in opposing disclosure. These are substantively aligned with the playbook's intent.

However, §7.2 does not satisfy element (3). The provision does not commit HubSpot to awaiting Customer instructions before complying with the regulatory/legal request. The "sufficient to allow" notice language implies a window for customer response but stops short of a standing obligation to hold compliance pending instruction. Critically, sub-clause (iii) of §7.2 implicitly distinguishes government agency disclosures from disclosures to other third parties — it imposes a court-order requirement only for non-government recipients, which implies government agency requests may be acted upon without a court order and, by implication, without awaiting Customer instructions.

A competing general provision — §12.5 of the General Terms — broadly reserves HubSpot's right to disclose "at all times" to satisfy "any law, regulation, legal process or governmental request," with no notification or referral requirement stated.

Under specific-over-general superseding logic, §7.2 governs for Confidential Information disclosure scenarios, making §12.5's silence on procedure less operative; however, §12.5 reinforces that HubSpot preserves the right to act on governmental requests, without tying that right to customer instruction-first.

The DPA §3.2 provides a supplementary protection for personal data matters: when a legal requirement prevents HubSpot from Processing per Customer instructions, HubSpot must notify and "cease all Processing… until such time as you issue new Instructions." This is the closest language in the document set to an "await instructions" requirement. However, it is scoped to processing-instruction conflicts rather than affirmative government disclosure requests — it does not squarely obligate HubSpot to withhold compliance with a regulatory request pending Customer direction.

Taken together, the contract addresses the regulatory disclosure topic with meaningful notice and referral protections, but the explicit "await our instructions before acting" element — the procedural control that allows the Customer to seek protective orders or manage regulatory exposure — is absent. For a High weight item, this gap is material. Classification: YELLOW.

— Superseding reasoning —
Section 7.2 of the General Terms specifically addresses the procedure governing how HubSpot must handle requests from legal and regulatory authorities to disclose Confidential Information (which expressly includes Customer Data per §1.45). Section 12.5 is a general compliance reservation that addresses HubSpot's overall right to disclose to satisfy governmental requests, without specifying procedure. Under the specific-over-general principle, §7.2 governs the regulatory disclosure procedure for Confidential Information, with §12.5 confirming the underlying right to comply with law rather than overriding the specific notification and referral obligations. The DPA §3.4 further provides that the DPA takes precedence over the General Terms for data conflicts, making DPA §3.2 the operative provision for personal data processing conflicts (though not squarely for affirmative disclosure requests).

— 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 if required to do so under any federal, state, or local law, statute, rule or regulation, subpoena or legal process; p…"

> *"We reserve the right at all times to disclose any information as necessary to satisfy any law, regulation, legal process or governmental request."*
> — Customer Terms of Service
> *"If we become aware that we cannot Process Customer Personal Data in accordance with your Instructions due to a legal requirement under any applicable law, we will (i) promptly notify you of that legal requirement to the extent permitted by the applicable law; and (ii) where necessary, cease all Processing (other than merely storing and maintaining the security of the affected Customer Personal Data) until such time as you issue new Instructions with which we are able to comply."*
> — Data Processing Agreement

## Encryption at Rest

**AI Comment:** The contract addresses encryption at rest but does so at a lower level of specificity than the playbook's acceptable position requires. The playbook requires either AES-256 or an explicit commitment to the then-current industry standard.

The operative language is found in DPA Annex 2 §3 (Transmission Control): HubSpot commits to "a layered approach of at-rest encryption technologies to ensure Customer Data and Customer-identified Permitted Sensitive Data are appropriately encrypted." This confirms that encryption at rest exists and covers Customer Data — but it does not name the encryption algorithm, cite AES-256, or invoke any named industry standard for at-rest encryption.

The contrast with HubSpot's in-transit language is telling: for in-transit encryption the same Annex 2 §3 states "Our HTTPS implementation uses industry standard algorithms and certificates" — an explicit industry-standard reference that is notably absent from the at-rest sub-section. For passwords specifically, Annex 2 does say "industry standard practices for security," but this phrase is scoped to password storage only and does not extend to the broader at-rest encryption obligation for Customer Data.

The General Terms §5.4 incorporates the DPA Annex 2 security measures under the qualifier "commercially appropriate," which is a lower bar than AES-256 or the then-current industry standard. DPA §3.3 provides the general security commitment but defers specifics to Annex 2, adding only that HubSpot may modify Security Measures "provided that such modification or update does not result in a material degradation in the protection offered." This non-degradation qualifier is a useful protection but cannot substitute for an express commitment to a specific encryption standard.

HubSpot's SOC 2 Type II and ISO 27001 certifications (referenced in DPA §7) provide some indirect practical assurance that recognized encryption standards are in use, but: (a) these certifications do not themselves require AES-256 specifically; (b) they are referenced as audit artifacts available for review rather than as binding contractual commitments on encryption algorithm; and (c) SOC 2 compliance is cited as a characteristic of HubSpot's hosting Sub-Processors, not a direct contractual obligation as to encryption standard.

The gap is clear and specific: the contract confirms at-rest encryption exists but does not contractually commit to AES-256 or the then-current industry standard as the encryption level. This is a meaningful gap relative to the playbook's acceptable position for a High-weight item, warranting YELLOW classification. Remediation path: seek an amendment or Order Form

side-letter expressly stating that Customer Data at rest is encrypted using AES-256 (or the then-current industry standard), or obtain a written representation from HubSpot's security team to that effect and confirm it is incorporated into the agreement.

> *"At-rest: We store user passwords following policies that follow industry standard practices for security. We take a layered approach of at-rest encryption technologies to ensure Customer Data and Customer-identified Permitted Sensitive Data are appropriately encrypted."*
> — Data Processing Agreement
> *"We will implement and maintain appropriate technical and organizational measures to protect Customer Personal Data from Customer Personal Data Breaches, as described under Annex 2 to this DPA ("Security Measures"). Notwithstanding any provision to the contrary, we may modify or update the Security Measures at our discretion provided that such modification or update does not result in a material degradation in the protection offered by the Security Measures."*
> — Data Processing Agreement
> *"We will maintain commercially appropriate administrative, physical, and technical safeguards to protect Personal Data as described in the DPA, including our Security Measures in Annex 2 of our DPA."*
> — Customer Terms of Service
> *"You acknowledge that the Subscription Service is hosted by our hosting Sub-Processors who maintain independently validated security programs (including SOC 2 and ISO 27001) and that our systems are audited annually as part of SOC 2 compliance and regularly tested by independent third party penetration testing firms. Upon request, we will supply (on a confidential basis) our SOC 2 report and summary copies of our penetration testing report(s) to you so that you can verify our compliance with this DPA."*
> — Data Processing Agreement

## Subprocessor Change Notification

**AI Comment:** HubSpot's DPA Section 5 addresses sub-processor change notification and objection rights but falls short of the playbook's acceptable position in two material respects, warranting a YELLOW classification.

**1. Notification Mechanism — Opt-In, Not Automatic (Material Gap)**
The playbook acceptable position requires that the Service Provider notify the Data Controller of new or replacement Sub-Processors. HubSpot's DPA provides 30-day advance notice of sub-processor changes, but only to customers who have proactively enrolled in email notifications via a separate subscription form. Without opt-in enrollment, customers receive no automatic direct notification — they would need to independently monitor HubSpot's publicly maintained Sub-Processors Page. The ideal preference ("at least 30 days notice to us") is not met because the mechanism is customer-initiated, not vendor-initiated push notification. This is a meaningful gap: a customer who has not opted in may have no practical awareness of a sub-processor change until after it has occurred.

**2. Remedy Upon Valid Objection — Discretionary, Not Automatic (Material Gap)**
The playbook acceptable position states that if the Service Provider proceeds with a new or replacement Sub-Processor despite the Data Controller's objection, the Data Controller "may immediately terminate the Agreement via written notice" and is entitled to a prorated refund of remaining unused prepaid fees. HubSpot's DPA instead grants HubSpot "sole discretion" to choose the remedy upon unresolved objection: either (a) not appoint the new Sub-Processor, or (b) permit the customer to suspend or terminate the affected Subscription Service. The customer does not hold an automatic, exercisable termination right — the decision rests with HubSpot. Additionally, the prorated refund of unused prepaid fees is not explicitly guaranteed in this specific scenario; the parenthetical carve-out ("without prejudice to any fees incurred by you prior to suspension or termination") addresses already-incurred fees but does not expressly address prepaid unused fees. A refund could be inferred by cross-referencing General Terms §4.5 (which provides a refund of prepaid unused fees upon customer-initiated termination for cause), but this is an inferential step across documents, not the clear contractual guarantee the acceptable position requires.

**3. Objection Window — Aligned**
HubSpot does provide a 30-day window to object upon notification, which aligns with the playbook acceptable position. The "reasonable grounds" qualifier (limiting objection to grounds relating to protection of Customer Personal Data) is consistent with standard DPA drafting and does not materially narrow the right beyond what the playbook contemplates.

**4. Deemed Acceptance — Not Explicit, But Implied**
The playbook specifies that failure to respond within 30 days, or objection without termination, results in deemed acceptance of the new Sub-Processor. HubSpot's DPA does not contain an explicit deemed-acceptance provision, though this is a reasonable implication of the structure (30-day window expires, engagement proceeds). This gap is low risk in practice but represents a technical absence relative to the acceptable position.

**Governing Document:** The DPA expressly takes precedence over the General Terms in case of conflict (DPA §4 / General Terms §5.4 incorporating the DPA by reference). The DPA Section 5 is the definitive provision for sub-processor change management. Note also that for customers subject to European Data Protection Laws, the Standard Contractual Clauses incorporated under DPA §11.2 apply Option 2 for Clause 9 sub-processor authorization, with SCC changes cross-referenced back to the DPA Sub-Processors section — preserving the same opt-in notification structure for European Data. This means the opt-in gap exists even where SCCs apply.

**Summary:** The topic is substantively addressed. The 30-day notification period and 30-day objection window both align with the playbook threshold. However, the opt-in delivery mechanism for notifications and the discretionary (rather than customer-automatic) termination remedy represent materially weaker protections than the acceptable position requires for a High-weight item. YELLOW — requires documented legal assessment.

— 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. "You may subscribe to receive notifications by email if we make changes to the HubSpot Sub-Processors Page by completing the form available at https://legal.hubspot.com/subscribe-subprocessor-updates. …"

> *"We will give you the opportunity to object to the engagement of new Sub-Processors on reasonable grounds relating to the protection of Customer Personal Data within 30 days of notifying you."*
> — Data Processing Agreement
> *"If you do notify us of such an objection, the parties will discuss your concerns in good faith with a view to achieving a commercially reasonable resolution. If no such resolution can be reached, we will, at our sole discretion, either not appoint the new Sub-Processor, or permit you to suspend or terminate the affected Subscription Service in accordance with the termination provisions of the Agreement without liability to either party (but without prejudice to any fees incurred by you prior to suspension or termination)."*
> — Data Processing Agreement

## Expenses (travel or otherwise)

**AI Comment:** The playbook item's acceptable position requires either (a) written pre-approval of expenses, or (b) if expenses are left open, a reasonable cap. The ideal preference is written pre-approval. One relevant provision is found across the document set — Section 8.1.2 of the Product Specific Terms — which addresses expense reimbursement for on-site Consulting Services. It limits reimbursable amounts to "reasonable costs," which constitutes a reasonableness-based limitation but falls short of both the ideal and the acceptable positions in the playbook: there is no written pre-approval right, and "reasonable costs" is a qualitative standard of review rather than a defined reasonable cap. The provision also narrows when the expense obligation arises at all: on-site consulting is the exception (the default is remote delivery), and even then only applies when both parties have separately agreed to on-site performance. No other provision across the Customer Terms of Service, DPA, AUP, or Privacy Policy addresses general travel or consulting-related expense reimbursement. Given the "Acceptable to Deviate" weight, the risk is low-priority and informational. The gap warrants a YELLOW classification because the topic is addressed but with weaker protection than the acceptable position contemplates — neither pre-approval nor a defined cap is present, only a reasonableness standard.

> *"For Consulting Services performed on-site, you will reimburse us our reasonable costs for all expenses incurred in connection with the Consulting Services. Any invoices or other requests for reimbursements will be due and payable within thirty (30) days of the date of the invoice."*
> — Product Specific Terms

## Breach Notification Timeline

**AI Comment:** The playbook's acceptable position requires notification within a maximum of 24 hours of (i) an actual or potential Data Security Breach, and (ii) any other actual or potential breach of DPA terms. HubSpot's DPA materially fails this standard on three compounding dimensions:

**1. Timeline — 72 hours vs. 24-hour maximum.** DPA § 3.5 commits to notification "no later than seventy-two (72) hours" after HubSpot becomes aware of a Customer Personal Data Breach. This ceiling is three times the 24-hour maximum required by the playbook. The qualifier "without undue delay" does not cure this deficiency — the enforceable outer bound is 72 hours, and the playbook expressly requires "in no event more than 24 hours." This alone warrants RED on a High weight item.

**2. "Potential" breaches excluded by definition.** The playbook requires notification of *potential* data security breaches. HubSpot's DPA defines "Customer Personal Data Breach" to explicitly exclude "unsuccessful attempts or activities that do not compromise the security of Customer Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems." Events that present a risk of compromise — but have not yet resulted in confirmed unauthorized access or disclosure — fall outside HubSpot's contractual notification obligation. This is a meaningful scope gap against the playbook's "actual or potential" standard.

**3. DPA term breach notifications — entirely absent.** The playbook's second prong requires notification of "any other actual or potential breach of the terms of the DPA" (i.e., compliance failures beyond data security incidents). HubSpot's DPA § 3.5 is scoped exclusively to Customer Personal Data Breaches. No provision in any of the reviewed documents imposes a notification obligation on HubSpot for other DPA term violations (e.g., unauthorized sub-processor appointment, failure to process only per customer instructions, etc.). This prong is entirely unaddressed — a silence gap within an otherwise partially-addressed item.

**Industry norm note:** The 72-hour ceiling is widely used in the SaaS industry and aligns with GDPR Article 33 controller-to-supervisory-authority notification obligations (though GDPR Article 33(2) does not set a specific processor-to-controller deadline — it merely requires notification "without undue delay"). This norm does not justify a downgrade here because the playbook has explicitly set a stricter 24-hour standard, and downgrade by industry norm would be inappropriate where the playbook has a clearly specified acceptable position that the vendor's terms fail to reach.

**Overall:** A High weight item with a 3× timeline overshoot, explicit exclusion of potential breaches, and complete silence on DPA-term-violation notifications yields a RED classification. This finding requires senior legal justification to accept.

— 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. ""Customer Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Personal Data transmi…"

> *"We will notify you without undue delay, but no later than seventy-two (72) hours, after we become aware of any Customer Personal Data Breach and will provide timely information relating to the Customer Personal Data Breach as it becomes known or reasonably requested by you."*
> — Data Processing Agreement

## License Grant to Data – Our Company to Vendor

**AI Comment:** **Acceptable Position (non-exclusive) — MET; Ideal Preference (revocable, only for service) — NOT MET.**

**Core License — §5.1 (General Terms):** The primary license grant reads: "You grant permission to us and our licensors to use the Customer Materials and Customer Data as necessary to provide the Subscription Service and Consulting Services to you, as permitted by this Agreement, and as permitted by applicable law." The word "non-exclusive" is not used, but under Massachusetts common law (the governing jurisdiction for North American customers per §11.2), a permission/license that does not expressly grant exclusivity is interpreted as non-exclusive by default. Critically, the customer expressly "own[s] and retain[s] all rights" to Customer Data and Materials, leaving no basis to imply exclusivity. The scope is anchored to service provision — satisfying the non-exclusive acceptable threshold. The DPA §3.1 reinforces this further for Personal Data specifically, committing HubSpot to process Customer Personal Data only as described in the DPA or per customer instructions; the DPA takes precedence over conflicting Agreement terms per DPA §3.4.

**Scope Expansions Beyond Service Provision (Ideal Not Met):**

*AI Training — §5.3.1 (General Terms):* HubSpot asserts an additional, DEFAULT-ON right to use Customer Data "to develop, support, and improve HubSpot AI features and functionality" and "to train our AI models." This goes beyond the ideal preference of "only to provide the service." An opt-out is available in account settings, but absent that opt-out, the license scope exceeds service provision. The use remains non-exclusive but is broader than ideal.

*Commercial Dataset (Tracking Code) — §5.3.2 (General Terms):* Conditional on the customer deploying the HubSpot Tracking Code, HubSpot asserts rights to use collected Website Data (including Personal Data like IP addresses) "to provide, maintain, append, improve, enhance, and develop our commercial dataset and Subscription Services." Commercial dataset development extends beyond direct service provision to the customer.

*Commercial Dataset (Enrichment Data) — PST §6.5 (Product Specific Terms):* For customers using enrichment products, PST §6.5(ii) grants HubSpot the right to use Enrichment Data "to provide, maintain, append, improve, enhance, and develop our commercial dataset and the Subscription Services" and expressly declares this authorization "supersedes any prior or conflicting terms" — overriding the narrower service-provision scope of General Terms §5.1 for this data subset. This is the broadest grant and applies in the enrichment product context.

*Suggestions — §6.2 (General Terms):* For the narrow category of product suggestions and comments, HubSpot takes full ownership ("we own all rights to use and incorporate them") — an assignment, not a license. For this content subset, HubSpot receives exclusive rather than non-exclusive rights. This is a standard SaaS clause and is limited to voluntary feedback about the product, not Customer Data broadly.

**Revocability — Not Provided:** No provision in any document establishes an independent right to revoke the data license short of terminating the Agreement. Revocability is entirely absent, meaning the ideal preference is not met on this ground as well.

**Summary:** The acceptable threshold (non-exclusive) is met by the core §5.1 grant, which preserves all customer ownership rights and is scoped to service provision. The ideal preference fails on two elements: (1) the license is not explicitly revocable; and (2) default-on AI training rights (§5.3.1) and conditional commercial dataset rights (§5.3.2, PST §6.5) extend scope materially beyond "only to provide the service." Customers using enrichment products or the HubSpot Tracking Code with intent data sharing face the broadest departures from the ideal. For customers using neither feature, the departure is limited to the opt-outable AI training use.

— Superseding reasoning —
PST §6.5(ii) contains an explicit self-superseding clause — "this authorization is necessary for the functionality of enrichment products and supersedes any prior or conflicting terms" — that overrides General Terms §5.1's narrower service-provision scope for the specific subset of Enrichment Data. The Product Specific Terms is the more specific instrument governing enrichment product behavior, and its express superseding language conclusively resolves any conflict in favor of the broader commercial-dataset-development purpose for Enrichment Data. General Terms §5.1 continues to govern the core license for all Customer Data that does not fall within the enrichment products and tracking-code regime.

— 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. "We may use data collected through the HubSpot Tracking Code, which may include Personal Data such as IP addresses and other online identifiers ("Website Data") to provide, maintain, append, improve, e…"
2. "(i) You agree we may use information collected through the HubSpot Tracking Code, which may include Personal Data such as IP addresses and other online identifiers ("Website Data"), to provide, mainta…"

> *"You own and retain all rights to the Customer Materials and Customer Data. You grant permission to us and our licensors to use the Customer Materials and Customer Data as necessary to provide the Subscription Service and Consulting Services to you, as permitted by this Agreement, and as permitted by applicable law."*
> — Customer Terms of Service

> *"We may use Customer Data to develop, support, and improve HubSpot AI features and functionality. We may also use Customer Data to train our AI models in compliance with our obligations under the Agreement. You may opt out of having your Customer Data used for this purpose by updating your settings in your HubSpot account."*
> — Customer Terms of Service
> *"You agree that all such comments and suggestions will be non-confidential and that we own all rights to use and incorporate them into the Subscription Service or Consulting Services, without payment or attribution to you."*
> — Customer Terms of Service

## Breach Indemnification

**AI Comment:** The playbook requires the vendor to provide indemnification for its own breaches and for breaches committed by its subprocessors. HubSpot's contractual framework does not meet this requirement in either respect.

**Vendor Breach Indemnification — Absent.** HubSpot's sole express indemnification obligation running in favor of the customer (General Terms §9.2) is explicitly and exclusively limited to third-party IP infringement claims. There is no indemnification provision covering HubSpot's own contractual breaches, data protection failures, or security incidents. In the absence of breach indemnification, the customer's primary recourse for a HubSpot breach is a general damages claim subject to the 12-month aggregate liability cap (General Terms §10.4). A capped-liability regime is legally distinct from indemnification: indemnification creates a proactive duty to defend, hold harmless, and compensate — including coverage of the indemnitee's legal defense costs — whereas a liability cap merely limits the damages recoverable after the customer proves a breach claim at its own cost and risk. Notably, General Terms §10.4's carve-outs from the cap are limited to: (i) customer fee payment obligations, (ii) customer indemnification obligations, (iii) HubSpot's IP Indemnification, and (iv) customer IP violations — HubSpot's own general breach liability is not carved out.

**Subprocessor Breach Indemnification — Absent; Vicarious Responsibility Only.** DPA §5 states that HubSpot "will remain responsible" for each sub-processor's DPA compliance failures and for any sub-processor acts or omissions that cause HubSpot to breach the DPA. This vicarious responsibility prevents HubSpot from deflecting liability onto sub-processors, which is meaningful. However, it is not indemnification: (1) the customer must still initiate and prove a breach claim against HubSpot; (2) there is no proactive duty to defend or hold harmless; (3) any recovery remains subject to the applicable liability cap; and (4) this responsibility is expressly limited to DPA obligations — it does not extend to all contractual breach scenarios.

**Partial Mitigations.** (1) DPA §12.3 carves out individual data protection rights violations from the aggregate liability cap, providing uncapped exposure for HubSpot on personal data protection rights claims — materially stronger than a purely capped regime for those claims. This provision supersedes General Terms §10.4 on this point by operation of the DPA's express precedence clause. (2) HubSpot contractually requires sub-processors to maintain DPA-equivalent data protection protections (DPA §5), providing upstream structural safeguards. (3) Security commitments detailed in DPA Annex 2 (SOC 2, ISO 27001 infrastructure, penetration testing, breach notification within 72 hours) reduce breach probability and impact.

Despite these partial mitigations, none constitute indemnification — they are liability-limiting and risk-reducing measures only. The playbook's requirement for affirmative breach indemnification (and sub-processor breach indemnification) is not met. For a High-weight item, this is a RED finding requiring senior legal justification to accept.

— Superseding reasoning —
The DPA contains an express precedence clause (DPA preamble): "In case of any conflict or inconsistency with other terms included in the Agreement, this DPA will take precedence to the extent of such conflict or inconsistency." General Terms §10.4 caps aggregate liability at 12 months' paid fees, with carve-outs only for: (i) customer fee obligations, (ii) customer indemnification obligations, (iii) HubSpot's IP Indemnification, and (iv) customer IP violations. No carve-out for data protection rights violations appears in §10.4. DPA §12.3, however, expressly provides that "in no event will either party's liability be limited with respect to any individual's data protection rights under this DPA." This directly conflicts with §10.4's general cap (which would otherwise subsume data protection rights claims). By the DPA's precedence clause, DPA §12.3 governs for data protection rights violations — they are uncapped. This superseding determination elevates the severity of HubSpot's breach exposure on personal data protection claims but does not alter the core finding: neither document provides affirmative breach indemnification.

— 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. "We will indemnify, defend and hold you harmless, at our expense, against any Action brought against you (and your officers, directors, employees, agents, service providers, licensors, and Affiliates) …"
2. "TO THE EXTENT PERMITTED BY LAW, AND EXCEPT FOR (i) YOUR LIABILITY FOR PAYMENT OF FEES, (ii) YOUR LIABILITY ARISING FROM YOUR OBLIGATIONS UNDER THE 'INDEMNIFICATION' SECTION, (iii) OUR LIABILITY ARISIN…"
3. "We will remain responsible for each Sub-Processor's compliance with the obligations of this DPA and for any acts or omissions of such Sub-Processor that cause us to breach any of its obligations under…"
4. "Each party and each of their Affiliates' liability, taken in aggregate, arising out of or related to this DPA (including any other data processing agreements between the parties) and the Standard Cont…"

> *"THIS SECTION STATES OUR ENTIRE LIABILITY AND YOUR SOLE AND EXCLUSIVE REMEDY WITH RESPECT TO ANY ACTION PROVIDED FOR UNDER THIS SECTION."*
> — Customer Terms of Service

## Processing Limitation

**AI Comment:** The playbook item requires that processing be limited to fulfilling contractual obligations and written instructions. The DPA § 3.1 substantially addresses this requirement for Customer Personal Data, expressly limiting processing to "purposes described in this DPA or as otherwise agreed within the scope of your lawful Instructions." The DPA also establishes explicit supremacy over conflicting Agreement terms. On the strength of these provisions alone, a GREEN classification would be supportable.

However, three structural features collectively prevent a GREEN finding:

1. **Default-on AI/ML Training (General Terms § 5.3.1):** HubSpot reserves the right to use Customer Data for AI model training and feature development — a purpose extending beyond direct service provision. This is permitted by default and requires affirmative customer action (opt-out) to restrict. The opt-out mechanism is accessible and meaningful, but the baseline posture allows processing for purposes beyond fulfilling the subscription contract.

2. **Broad "Instructions" Definition (DPA § 2.2):** HubSpot defines the customer's "complete Instructions" as the entire Agreement (including the General Terms). This is circular: by agreeing to the Agreement, customers are deemed to have "instructed" all uses described therein, including the AI training carve-out. This dilutes the traditional function of an instruction-based processing limitation, which is to confine the processor to customer-specific directives rather than vendor-drafted terms.

3. **AI Service Provider Data Sharing (Product Specific Terms § 7.5):** Customer Data provided as AI Input/Output may be shared with third-party AI service providers for "other business purposes consistent with this Agreement" — language broader than service fulfillment.

The DPA precedence clause provides partial mitigation: if the AI training provision is read as conflicting with § 3.1's processing limitation, the DPA should govern. However, because HubSpot structures the AI training as "in compliance with our obligations under the Agreement" and defines Instructions as the Agreement itself, no clear conflict may be recognized, leaving the DPA's protective effect uncertain as applied to this specific tension.

The CCPA-specific provision (DPA § 9.3) provides stronger language for California Personal Information, requiring processing "strictly for the purpose of performing the Subscription Services," but this applies only to that jurisdictional subset.

Overall: the processing limitation topic is addressed with substantive DPA language, but the AI training carve-out operating on a default opt-in basis and the broad Instructions definition mean the contract does not fully satisfy the strict standard of "processing limited to fulfilling contractual obligations and written instructions" without affirmative customer action to opt out and a favorable interpretation of the DPA conflict clause.

— Superseding reasoning —
The DPA expressly states it prevails over other Agreement terms in the event of conflict. If General Terms § 5.3.1 (AI training using Customer Data beyond service provision) is read as conflicting with the DPA § 3.1 processing limitation, the DPA would govern and processing would be confined to DPA-described purposes and lawful Instructions. However, this superseding outcome is genuinely uncertain: HubSpot structures AI training as occurring "in compliance with our obligations under the Agreement" and defines the Instructions as the Agreement itself (DPA § 2.2), which may eliminate any cognizable conflict between the two provisions. This ambiguity is flagged for human review and is a contributing factor to the YELLOW classification.

— 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 agree that the Agreement (including this DPA), together with your use of the Subscription Service in accordance with the Agreement, constitute your complete Instructions to us in relation …"

> *"We will only Process Customer Personal Data for the purposes described in this DPA or as otherwise agreed within the scope of your lawful Instructions, except where and to the extent otherwise required by applicable law."*
> — Data Processing Agreement
> *"We will use Customer Data in order to provide the Subscription Service and Consulting Services to you, as permitted by this Agreement, and as permitted by applicable law."*
> — Customer Terms of Service
> *"We may use Customer Data to develop, support, and improve HubSpot AI features and functionality. We may also use Customer Data to train our AI models in compliance with our obligations under the Agreement. You may opt out of having your Customer Data used for this purpose by updating your settings in your HubSpot account."*
> — Customer Terms of Service
> *"In case of any conflict or inconsistency with other terms included in the Agreement, this DPA will take precedence to the extent of such conflict or inconsistency."*
> — Data Processing Agreement
> *"We certify that we will Process California Personal Information as a Service Provider strictly for the purpose of performing the Subscription Services and Consulting Services under the Agreement (the "Business Purpose") or as otherwise permitted by the CCPA, including as described in the 'Usage Data' section of our Privacy Policy. Further, we certify that we will not (i) Sell or Share California Personal Information; (ii) Process California Personal Information outside the direct business relationship between the parties, unless required by applicable law; or (iii) combine California Personal Information included in Customer Data with Personal Data that we collect or receive from another source*

*(other than information we receive from another source in connection with our obligations as a Service Provider under the Agreement)."*
— Data Processing Agreement
*"You acknowledge that your AI Input and AI Output, including Customer Data, will be shared with and processed by our AI service providers, in order to enable your use of HubSpot AI, content moderation, and other business purposes consistent with this Agreement."*
— Product Specific Terms

## Restrictions on Use

**AI Comment:** HubSpot's contractual framework imposes a comprehensive set of use restrictions across the General Terms, Product Specific Terms, and Acceptable Use Policy. The bulk of these restrictions — mandatory AUP compliance, prohibitions on reverse engineering and unlawful use, requirements to comply with applicable law, and limitations on commercial exploitation or resale of the service — are standard, objectively-defined SaaS-vendor restrictions that fall squarely within the acceptable position that reasonable restrictions on use are permitted. These alone would support a GREEN classification.

However, three provisions introduce restrictions that go beyond what is ordinarily considered "reasonable" and create meaningful ambiguity about the customer's ability to use the service as intended:

(1) General Terms §4.3 grants HubSpot the right to terminate for cause on 30 days' notice whenever it "determines" the customer's conduct "has or may negatively reflect on or affect" HubSpot, its prospects, or its customers. This standard is entirely subjective, unilateral, and untethered to any objective AUP or legal violation — it relies solely on HubSpot's self-assessment of reputational impact, with no proportionality or independent verification requirement. This creates uncertainty about what constitutes permissible use that is not mitigated by the 30-day notice period.

(2) PST §7.6, using explicit "notwithstanding anything to the contrary" override language, grants HubSpot sole discretion to make changes to HubSpot AI features that materially reduce functionality at any time during the subscription term, with no notice requirement and no remedy mechanism. This supersedes the General Terms §2.6 non-degradation commitment for AI features (see superseding analysis), and for customers who rely on HubSpot AI as part of their intended use, this effectively eliminates the service-level protection for a material category of functionality.

(3) AUP §6 grants HubSpot a unilateral right to discontinue service for customers in a non-exhaustive list of restricted industries (including cryptocurrency, pharmaceuticals, gambling, multi-level marketing, and others). The non-exhaustive framing means HubSpot could expand this list without advance notice. For customers in or adjacent to these industries, this provision could prevent intended use of the platform entirely.

The overall classification is YELLOW: the core restrictions framework is reasonable and largely standard, but these three provisions introduce one-sided discretion — particularly the subjective reputational harm termination trigger and the AI feature sole-discretion override — that exceeds what the acceptable position of "reasonable restrictions on use are allowed" envisions. The acceptable position is partially met; the ideal preference is not reached.

— Superseding reasoning —
One superseding determination applies within this item analysis. The Product Specific Terms §7.6 ("Availability and Modifications" for HubSpot AI) explicitly overrides the General Terms §2.6 service modification commitment for the scope of HubSpot AI features. PST §7.6 opens with "Notwithstanding anything to the contrary in our Terms of Service or these Product Specific Terms" — an express textual override clause that leaves no interpretive ambiguity. Where General Terms §2.6 implicitly protects all Subscription Service features from material degradation (with a termination + refund remedy if that commitment is breached), PST §7.6 explicitly carves out HubSpot AI features from that protection and grants HubSpot sole discretion to materially reduce AI functionality at any time without any remedy. General Terms §2.6 remains the controlling provision for all non-AI service features.

— 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. "You will comply with our Acceptable Use Policy at http://legal.hubspot.com/acceptable-use ("AUP"). You will not use the Subscription Service in any way that violates the terms of the AUP or for any pu…"
2. "We may also terminate this Agreement for cause on thirty (30) days' notice if we determine that you are acting, or have acted, in a way that has or may negatively reflect on or affect us, our prospect…"
3. "We may suspend any User's access to any or all Subscription Services without notice for:

(i) use of the Subscription Service in a way that violates applicable local, state, federal, or foreign laws o…"
4. "Some industries have higher than average abuse complaints, which can directly impact our ability to provide the HubSpot Service to other customers. To protect our customers, we reserve the right to di…"

*"You will not (i) directly or indirectly reverse engineer, decompile, disassemble or otherwise attempt to uncover or discover the source code, object code or underlying structure, ideas, know-how or algorithms relevant to the Subscription Services or any software, documentation or data related to the Subscription Services; (ii) modify, translate, or create derivative works based on the Subscription Services (except to the extent expressly permitted by us); (iii) or remove any proprietary notices or labels."*
— Customer Terms of Service
*"We may modify the Subscription Service during the Subscription Term, including by adding or removing features, functions, Limits, or Add-Ons that apply to your subscription. Any modifications we make will not materially degrade the overall functionality of the Subscription Service during the Current Term to which you subscribe except as follows:*

*(i) modifications to Free Services;*

*(ii) modifications resulting from changes outside of our control, such as a change to applicable law, changes related to Third-Party Products, etc.;*

*(iii) as otherwise specified in our Product Specific Terms; or*

*(iv) modifications to any Beta Services.*

*If the modification materially degrades the overall functionality of the Subscription Service and HubSpot is unable to provide you with substantially similar functionality, your sole and exclusive remedy for our breach of this section is termination of your Subscription Services and a pro-rated refund of unused fees."*
— Customer Terms of Service
*"Notwithstanding anything to the contrary in our Terms of Service or these Product Specific Terms, we may make changes to HubSpot AI features that materially reduce the functionality provided to you during the Subscription Term or change the Limits that apply to you at any time in our sole discretion."*
— Product Specific Terms
*"You will use the HubSpot Service for your internal business purposes and will not:*

*(i) willfully tamper with the security of the HubSpot Service or tamper with our customer accounts;*

*(ii) access data on the HubSpot Service not intended for you;*

*(iii) log into a server or account on the HubSpot Service that you are not authorized to access;*

*(iv) attempt to probe, scan or test the vulnerability of any HubSpot Service or to breach the security or authentication measures without proper authorization;*

*(v) willfully render any part of the HubSpot Service unusable;*

*(vi) lease, distribute, license, sell or otherwise commercially exploit the HubSpot Service or make the HubSpot Service available to a third party other than as contemplated in your subscription to the HubSpot Service;*

*(vii) use the HubSpot Service for timesharing or service bureau purposes or otherwise for the benefit of a third party; or*

*(viii) provide to third parties any evaluation version of the HubSpot Service without our prior written consent."*
— Acceptable Use Policy

## Governing Law

**AI Comment:** HubSpot explicitly addresses governing law through a location-dependent framework. For customers in North America or South America — or where no customer location is registered in the HubSpot account — the default governing law is the Commonwealth of Massachusetts, U.S.A., with exclusive forum in the courts of Boston, Massachusetts (General Terms § 11.2). The DPA tracks the same governing law by explicit cross-reference (DPA § 12.4).

The playbook's acceptable positions are: (1) Michigan, (2) Delaware, (3) New York, or (4) any jurisdiction with nexus to the customer. Massachusetts satisfies none of the three specifically named positions. Whether it qualifies under position (4) — "any Jurisdiction with nexus" — is interpretively ambiguous. Massachusetts clearly has nexus to HubSpot (its global headquarters is Cambridge, MA), but the "nexus" formulation in the playbook more naturally refers to nexus to the customer's operations. Since no customer location was provided in the intake brief, it cannot be confirmed that Massachusetts has nexus to the customer, and a customer based in Michigan, Delaware, or New York would find Massachusetts a foreign jurisdiction for litigation purposes.

YELLOW is the appropriate classification because: (a) the topic is explicitly addressed — this is not a silence gap; (b) Massachusetts is a well-established U.S. commercial law jurisdiction, meaning the practical risk of unfavorable or unpredictable law is moderate rather than severe; (c) the "nexus" prong introduces genuine interpretive uncertainty that prevents a definitive RED finding absent knowledge of the customer's location; and (d) the weight is Acceptable to Deviate, making this finding informational per the risk matrix. The practical exposure for a North American customer is primarily litigation burden — being required to litigate exclusively in Boston — rather than a materially unfavorable substantive law.

— 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. "Your physical address (entered into your HubSpot Account as the "Company Address") will determine (i) the HubSpot entity entering into this Agreement, (ii) the address to which you should direct noti…"
2. "If your (i) Customer Location is in North America or South America, (ii) you are located in a geographic region that does not otherwise fall into one of the designations described in the Jurisdiction …"
3. "This DPA will be governed by and construed in accordance with the 'Contracting Entity; 'Applicable Law; Notice' sections of the Jurisdiction Specific Terms, unless required otherwise by Data Protectio…"
*"For contracts with HubSpot, Inc., both parties consent to the exclusive jurisdiction and venue in the courts of Boston, Massachusetts, U.S.A. for all disputes arising out of or relating to this Agreement."*
— Customer Terms of Service

## Encryption in Transit

**AI Comment:** The playbook requires data encryption upon transmission at AES-256-bit or then-current industry standard. HubSpot addresses this across three documents, with the most specific and controlling commitment appearing in DPA Annex 2 (Security Measures), Section 3 — Transmission Control: "We require HTTPS encryption (also referred to as SSL or TLS) on all login interfaces and for free on every customer site hosted on the HubSpot products. Our HTTPS implementation uses industry standard algorithms and certificates." The Privacy Policy §4.1 independently corroborates this, explicitly referencing "commercial industry standard secure encryption methods to protect customer data at rest and in transit, TLS for HubSpot hosted sites." The General Terms §5.4 incorporates the DPA Security Measures by reference as a contractual anchor.

AES-256 is not named explicitly, triggering a functional-equivalence assessment. The playbook's acceptable position expressly permits "then-current industry standard" as an alternative. HTTPS/TLS with industry-standard algorithms is the then-current industry standard for in-transit encryption. Modern TLS 1.2 and 1.3 — the protocols employed under any current "industry standard algorithms and certificates" commitment — use AES-256-GCM cipher suites as the predominant standard, placing HubSpot's commitment functionally at or above the AES-256 threshold. The DPA's security commitments are legally binding and the DPA takes precedence over other Agreement documents in the event of conflict (DPA §intro: "In case of any conflict or inconsistency with other terms included in the Agreement, this DPA will take precedence").

Classification is therefore GREEN on a functional-equivalence basis: the protection is achieved through different language ("industry standard algorithms and certificates" / "TLS") but delivers the same legal protection and enforceability as an explicit AES-256 specification. Confidence is MODERATE rather than HIGH because the cipher strength is not enumerated; an interpretive step is required to equate "industry standard algorithms" with AES-256-level encryption, and the contractual commitment does not explicitly commit to a minimum cipher version (e.g., TLS 1.2+), leaving a theoretical gap if HubSpot were to revert to legacy cipher suites while still asserting "industry standard" compliance.

No preference was specified in the playbook item; aiPreferenceMet is false as there is no ideal preference against which to compare.

> *"In-transit: We require HTTPS encryption (also referred to as SSL or TLS) on all login interfaces and for free on every customer site hosted on the HubSpot products. Our HTTPS implementation uses industry standard algorithms and certificates."*
> — Data Processing Agreement
>
> *"We also have additional safeguards where appropriate (such as commercial industry standard secure encryption methods to protect customer data at rest and in transit, TLS for HubSpot hosted sites, web application firewall protection, and other appropriate contractual and organizational measures)"*
> — HubSpot Privacy Policy
>
> *"We will maintain commercially appropriate administrative, physical, and technical safeguards to protect Personal Data as described in the DPA, including our Security Measures in Annex 2 of our DPA."*
> — Customer Terms of Service

## Data Processing Security Policies

**AI Comment:** HubSpot's terms comprehensively address data processing security through a multi-layered framework spanning the General Terms and, most substantively, the Data Processing Agreement (DPA) and its detailed Annex 2 Security Measures.

The General Terms §5.4 establish the top-level customer-facing commitment to "commercially appropriate administrative, physical, and technical safeguards," explicitly cross-referencing DPA Annex 2 for implementation detail. The DPA §3.3 then formalizes this as a commitment to "appropriate technical and organizational measures" — language aligned with international data protection standards (GDPR Art. 32) and consistent with high-watermark industry practice.

DPA Annex 2 enumerates specific controls that directly satisfy each element of the playbook requirement:

**Adequate Policies:** A written Information Security Policy is confirmed (Annex 2 §1). A written Incident Response Plan with associated playbooks is also maintained (Annex 2 §4), addressing detection and response to security events.

**Preventing Unauthorized Access to Processing Systems:** Access controls are detailed at multiple layers — role-based authorization with permission validation, authentication requirements before accessing Customer Personal Data (Annex 2 §2.1), and "just-in-time access" (JITA) privilege management with privileged access controls and monitoring for internal access to production systems (Annex 2 §2.3). Transmission control includes mandatory TLS/HTTPS on all login interfaces and customer-hosted sites, and layered at-rest encryption (Annex 2 §3).

**Adequate Technical Measures:** Intrusion detection via a Web Application Firewall (WAF) (Annex 2 §2.2), daily vulnerability scanning, and at least annual third-party penetration testing of the web application and corporate infrastructure (Annex 2 §6) provide ongoing assurance of control effectiveness.

**External Validation:** The DPA §7 confirms that HubSpot's systems are audited annually under SOC 2 and the hosting infrastructure is certified under ISO 27001, with SOC 2 reports and penetration testing summaries available to customers upon request. This provides third-party assurance that the described controls are operating as documented.

One YELLOW-classified reference exists: DPA §3.3 reserves HubSpot's right to unilaterally modify security measures. This right is, however, bounded by a contractual floor requiring that no modification result in "a material degradation in the protection offered by the Security Measures." This constraint limits practical risk, as HubSpot remains contractually

obligated to maintain the same level of substantive protection. This is also standard SaaS market practice, as vendors require flexibility to update security controls to address emerging threats.

No ideal preference was specified for this item, so aiPreferenceMet is set to false as a matter of policy rather than a gap finding.

Overall, the breadth, specificity, and external validation of HubSpot's documented security policies and technical controls clearly meet the acceptable position for adequate security and policies to prevent unauthorized access to processing systems. Item-level classification: GREEN, confidence: HIGH.

— 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. "Authorization: Customer Data is stored in multi-tenant storage systems accessible to Customers via only application user interfaces and application programming interfaces. Customers are not allowed di…"
2. "Privileged Access Management: Privileged access in our product environment is controlled, monitored, and removed in a timely fashion through "just in time access" (or "JITA") controls. Non-personal ac…"

> *"We will maintain commercially appropriate administrative, physical, and technical safeguards to protect Personal Data as described in the DPA, including our Security Measures in Annex 2 of our DPA."*
> — Customer Terms of Service
> *"We will implement and maintain appropriate technical and organizational measures to protect Customer Personal Data from Customer Personal Data Breaches, as described under Annex 2 to this DPA ("Security Measures")."*
> — Data Processing Agreement
> *"Notwithstanding any provision to the contrary, we may modify or update the Security Measures at our discretion provided that such modification or update does not result in a material degradation in the protection offered by the Security Measures."*
> — Data Processing Agreement
> *"You acknowledge that the Subscription Service is hosted by our hosting Sub-Processors who maintain independently validated security programs (including SOC 2 and ISO 27001) and that our systems are audited annually as part of SOC 2 compliance and regularly tested by independent third party penetration testing firms."*
> — Data Processing Agreement
> *"We maintain and adhere to an internal, written Information Security Policy."*
> — Data Processing Agreement
> *"In-transit: We require HTTPS encryption (also referred to as SSL or TLS) on all login interfaces and for free on every customer site hosted on the HubSpot products. Our HTTPS implementation uses industry standard algorithms and certificates."*
> — Data Processing Agreement
> *"Incident Response Plan: We maintain a written Incident Response Plan, playbooks, and other necessary processes and procedures to fulfill the standards and obligations reflected therein."*
> — Data Processing Agreement
> *"Vulnerability scanning: We perform daily vulnerability scanning on our products using technology and detection standards aligned with industry standards.*
>
> *Penetration testing: We maintain relationships with industry-recognized penetration testing service providers for penetration testing of both the HubSpot web application and internal corporate network infrastructure at least annually."*
> — Data Processing Agreement

## Subprocessor Agreements

**AI Comment:** This High weight playbook item contains two substantive and distinct requirements: (A) written agreements with processors and sub-processors at least as strict as the DPA, and (B) prohibition on using sub-processors/ subcontractors for privileged access. The contract addresses one requirement partially and contradicts the other.

**Requirement A — Sub-processor data protection agreements at least as strict as the DPA:**
DPA §5 commits HubSpot to imposing "data protection terms on the Sub-Processors that provide at least the same level of protection for Customer Personal Data as those in this DPA." This closely tracks the playbook's "at least as strict as this DPA" language and is reinforced by HubSpot's retention of full flow-down responsibility for sub-processor compliance and acts/omissions (PIF 2). Two gaps prevent a GREEN classification: (i) the qualifier "to the extent applicable to the nature of the services provided by such Sub-Processors" permits calibration of protections to sub-processor service scope, potentially allowing HubSpot to argue that certain DPA obligations do not apply to narrowly-scoped sub-processors; and (ii) the commitment uses "impose data protection terms" rather than explicitly "written agreements," though contractual imposition is strongly implied. Classification for this component: YELLOW.

**Requirement B — Prohibition on sub-processor/subcontractor use for privileged access:**
The DPA contains no such prohibition. DPA §5 expressly permits sub-processor engagement for "hosting and infrastructure" (PIF 3), and Annex 2 §2.1 confirms the service is hosted with "outsourced cloud infrastructure providers" (referenced in PIF 3 comment). Infrastructure hosting inherently carries elevated/privileged-level access to production systems, data storage, and network resources. Annex 2 §2.3 does describe JITA-based privileged access controls (PIF 4), but those controls expressly apply to "a subset of our employees" — not to sub-processors. The playbook's prohibition requirement is not addressed anywhere in the document set, and the DPA's architecture actively contradicts it by permitting infrastructure sub-processors whose roles require privileged access. Classification for this component: RED — contract conflicts with the acceptable position.

**Composite classification: YELLOW.** Requirement A is substantially (if imperfectly) addressed, preventing a full RED item classification. However, Requirement B is absent and structurally contradicted. Reviewing counsel should treat the Requirement B gap as a material RED finding given the High weight of this item. Negotiated addenda specifying that infrastructure sub-processors with privileged access are subject to explicit contractual restrictions (e.g., access limited to minimum necessary scope, audit rights, contractual prohibition on retaining or processing customer data outside service delivery) may be warranted if this control is critical to the customer's risk posture.

— 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. "We will remain responsible for each Sub-Processor's compliance with the obligations of this DPA and for any acts or omissions of such Sub-Processor that cause us to breach any of its obligations under…"
2. "Privileged Access Management: Privileged access in our product environment is controlled, monitored, and removed in a timely fashion through "just in time access" (or "JITA") controls. Non-personal ac…"

> *"Where we engage Sub-Processors, we will impose data protection terms on the Sub-Processors that provide at least the same level of protection for Customer Personal Data as those in this DPA, to the extent applicable to the nature of the services provided by such Sub-Processors."*
> — Data Processing Agreement
> *"You agree we may engage Sub-Processors to Process Customer Personal Data on your behalf, and we do so in three ways. First, we may engage Sub-Processors to assist us with hosting and infrastructure."*
> — Data Processing Agreement

## Processing Location Restrictions

**AI Comment:** This playbook item contains two distinct requirements: (1) all Vendor processing must occur in the US, Canada, or the EU — or alternatively, all processing must be completed under Standard Contractual Clauses (SCCs); and (2) any K12 processor or sub-processor must be located in the US.

COMPONENT 1 — PROCESSING LOCATION / SCCs:

Positive findings: HubSpot, Inc. is identified in DPA Annex 1A as the US-based Data Importer and Processor — primary processing occurs in the United States, satisfying the US prong of the geographic restriction. SCCs are formally incorporated into the DPA (§11.2) for "Restricted Transfers," defined as transfers of European Data to countries without adequate protection under European Data Protection Laws, directly satisfying the "OR SCCs" arm of the requirement for European-originating data. HubSpot also participates in the EU-US Data Privacy Framework (DPA §11.1), providing an additional validated transfer mechanism for EU-originating data. Regional Hosting Locations are available in the US and EU (CToS §5.5), providing geographic storage specificity for primary data storage.

Negative findings: The requirement that ALL processing occurs in the permitted regions or under SCCs is not satisfied. DPA §6 expressly permits HubSpot to "access and Process Customer Personal Data on a global basis" in "other jurisdictions where HubSpot Affiliates and Sub-Processors have operations" — unambiguous language that processing is not constrained to US, Canada, or EU. The SCCs apply only to "Restricted Transfers" (a defined term limited to European-originating Data); they are not applied to all global processing of non-European customer data. The Regional Hosting Location has broad exclusions (§5.5.1): Add-Ons, Third-Party Products, Beta Services, Consulting Services, HubSpot Content, analytics, and any access by users outside the Hosting Location are all explicitly excluded. HubSpot further disclaims that the Hosting Location satisfies data residency requirements. The sub-processor list is maintained at an external URL not included in the provided document set, preventing geographic verification of all sub-processors. The Privacy Policy §4.1 corroborates global processing, confirming transfers to Affiliates "where we have operations" globally.

Note on Canada: The Jurisdiction Specific Terms Appendix identifies HubSpot Canada Inc. as the contracting entity for Canadian customers; however, DPA Annex 1A identifies HubSpot, Inc. (US) as the Data Importer/Processor for all customers. Evidence of Canadian-location processing was not found in the provided documents.

Document hierarchy note: For processing location matters, the DPA controls over the General Terms: the DPA's opening clause establishes DPA precedence in case of conflict with the Agreement, and DPA §6's global processing authorization is the operative governing provision (see Superseding Details).

COMPONENT 2 — K12 PROCESSOR IN US:

All five reviewed documents (Customer Terms of Service, Product Specific Terms, DPA, AUP, and Privacy Policy) are entirely silent on K12-specific restrictions, FERPA compliance, or any US-only sub-processor restriction for educational institution contexts. Under the silence-handling framework, this sub-requirement on a High weight item defaults to RED. The intake brief does not specify a K12 use case, but the requirement appears in the Review Specific Playbook and must be flagged. If this deployment serves a K12 institution, human review and direct vendor negotiation are required before relying on this vendor.

OVERALL CLASSIFICATION — YELLOW:

Classified YELLOW because the main requirement (US/Canada/EU OR SCCs) has meaningful partial coverage: US-based primary processing and SCCs/DPF for European Data provide substantial protection for EU-originating data flows, and HubSpot, Inc. as the primary processor is US-based. Classification should be escalated to RED if: (a) the customer is a K12 institution (K12 sub-requirement is completely silent); (b) non-European customer data processed in third-country sub-

processor jurisdictions is a material compliance concern; or (c) the Hosting Location exclusions (Add-Ons, Beta Services, Third-Party Products) are core to the deployment. Manual review of HubSpot's sub-processor list at https://legal.hubspot.com/sub-processors-page is strongly recommended to confirm geographic distribution of all engaged processors.

— Superseding reasoning —
The DPA takes precedence over the General Terms (Customer Terms of Service) for all data processing matters, pursuant to the DPA's explicit precedence clause: "In case of any conflict or inconsistency with other terms included in the Agreement, this DPA will take precedence to the extent of such conflict or inconsistency." For processing location analysis, DPA §6's global processing authorization (PIF[0]) governs over any reading of the CToS §5.5 Hosting Location (PIF[4]) as restricting all data processing to US/EU geographic regions. While the Hosting Location addresses primary storage location, the DPA makes clear that processing occurs globally; the DPA's explicit global authorization is controlling. Additionally, within the DPA hierarchy, §11.2(F) establishes that the Standard Contractual Clauses prevail over DPA provisions in the event of conflict — meaning for European Restricted Transfers specifically, the SCCs provide the highest-level contractual protection in the hierarchy.

— 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. "The Standard Contractual Clauses will be incorporated by reference and apply to the Restricted Transfer as follows:

(A) In relation to Customer Personal Data (i) the Module Two terms apply to the ext…"
2. "We will store your Customer Data in a specific location or geographical region (e.g., United States, European Union, etc.) as part of your subscription subject to the terms of this Agreement (each a "…"

> *"You acknowledge and agree that we may access and Process Customer Personal Data on a global basis as necessary to provide the Subscription Service in accordance with the Agreement, and in particular that Customer Personal Data may be transferred to and Processed by HubSpot, Inc. in the United States and to other jurisdictions where HubSpot Affiliates and Sub-Processors have operations. Wherever Customer Personal Data is transferred outside its country of origin, each party will ensure such transfers are made in compliance with the requirements of Data Protection Laws."*
> — Data Processing Agreement
> *"HubSpot will not transfer European Data to any country or recipient not recognized as providing an adequate level of protection for Customer Personal Data (within the meaning of applicable European Data Protection Laws), unless it first takes all such measures as are necessary to ensure the transfer is in compliance with applicable European Data Protection Laws. Such measures may include (without limitation) (i) transferring such data to a recipient that is covered by a suitable framework or other legally adequate transfer mechanism recognized by the relevant authorities or courts as providing an adequate level of protection for Customer Personal Data, including the Data Privacy Framework; (ii) to a recipient that has achieved binding corporate rules authorization in accordance with European Data Protection Laws; or (iii) to a recipient that has executed the Standard Contractual Clauses in each case as adopted or approved in accordance with applicable European Data Protection Laws."*
> — Data Processing Agreement
> *"HubSpot, Inc. participates in and certifies compliance with the Data Privacy Framework. Where and to the extent the Data Privacy Framework applies to the Restricted Transfer, HubSpot, Inc. will (i) provide at least the same level of protection to Customer Personal Data and Controller Personal Data required by the Data Privacy Framework Principles and (ii) inform you if we determine that we are unable to comply with this requirement."*
> — Data Processing Agreement
> *"The Hosting Location does not apply to or cover other services or types of data including (i) Add-Ons, Third-Party Products, or Beta Services (ii) Consulting Services; (iii) HubSpot Content; (iv) analytics generated in connection with the Subscription Service; (v) as indicated on the HubSpot Sub-Processors Page; or (vi) if Users or your end users access the Subscription Service outside of the Hosting Location. WE MAKE NO WARRANTY THAT A SPECIFIC HOSTING LOCATION WILL MEET YOUR DATA RESIDENCY REQUIREMENTS."*
> — Customer Terms of Service
> *"Annex 3 - Sub-Processors](https://legal.hubspot.com/dpa#annex-3)"*
> — Data Processing Agreement
> *"To facilitate our global operations, we may transfer information that may include Personal Data to other HubSpot Affiliates who act as subprocessors, where we have operations for the purposes described in this policy."*
> — HubSpot Privacy Policy

## Confidentiality

**AI Comment:** HubSpot's agreement contains a mutual confidentiality framework that substantially satisfies most elements of the acceptable position but has one primary structural deviation that prevents a GREEN classification: the "HubSpot Solutions Partners" carve-out in §7.1(iii).

**What Meets the Acceptable Position:**

The definition of Confidential Information (§1 of the General Terms) is broad, mutual, and includes all four standard carveouts required by the playbook: (i) becomes generally known to the public without breach, (ii) was known to Receiving Party prior to disclosure without breach, (iii) received from a third party without breach, and (iv) independently developed by the Receiving Party — §1.44. Customer Data is automatically treated as Confidential Information under §1.45 regardless of designation, providing meaningful protection for the customer's most sensitive material.

The mutual obligation structure uses "Receiving Party / Disclosing Party" language that applies symmetrically to both HubSpot and Customer. The customer's right to share its CI with its own employees, contractors, and agents who need

access — provided they are bound by confidentiality agreements with protections no less stringent than those in the Agreement (§7.1(iv)) — directly satisfies the acceptable position's requirement that we be able to share CI with our subcontractors on a need-to-know basis.

Legal process disclosures (§7.2) are appropriately constrained: prompt notice, minimum-necessary disclosure, referral to the disclosing party, and assistance in opposing disclosure unless prohibited. These are standard and well-structured.

The DPA §3.4 adds a further layer of confidentiality protection specific to Customer Personal Data: all personnel authorized to process it must be under contractual or statutory confidentiality obligations.

**Primary Deviation — "HubSpot Solutions Partners" Carve-Out (§7.1(iii)):**

The acceptable position requires that Vendor not disclose CI to third parties unless they have a need-to-know in order to perform the services. HubSpot's §7.1(iii) carves out disclosure to (a) third-party service providers used to provide the Subscription Service or Consulting Services — which is within the acceptable position — AND (b) "HubSpot Solutions Partners bound by confidentiality obligations." HubSpot Solutions Partners are resellers, implementation agencies, and certified partners in HubSpot's ecosystem. This category is not limited to parties engaged to perform HubSpot's services to this specific customer; it is a broad class of business partners. While they must be bound by confidentiality obligations, the carve-out's scope clearly exceeds the "need-to-know for performing the services" threshold required by the acceptable position. This is the controlling reason for the YELLOW classification.

**Secondary Concern — AI Training Default Opt-In (§5.3.1):**

Customer Data is Confidential Information per §1.45. §5.3.1 permits HubSpot to use Customer Data to train its AI models by default; the customer must affirmatively opt out. Because this use is explicitly authorized within the Agreement itself, it does not technically violate §7.1(ii)'s prohibition on using CI "outside the scope of this Agreement." However, it represents a use of CI beyond the core purpose of service delivery that the customer must actively prevent — a posture that warrants attention in the context of a confidentiality review.

**Preference Not Met:**

The preference requires a clean mutual obligation where Vendor shares none of Customer's CI with third parties. The Solutions Partners carve-out (§7.1(iii)) and the AI training default opt-in (§5.3.1) both prevent this threshold from being reached. The preference is not met.

**Governing Jurisdiction Note:** Under Massachusetts law (the default jurisdiction per §11.2 of the General Terms), confidentiality provisions are enforceable as-written in commercial contracts. No statutory provision fills the Solutions Partners gap.

— 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 if required to do so under any federal, state, or local law, statute, rule or regulation, subpoena or legal process; p…"

> *""Confidential Information" means all confidential information disclosed by a party and its Affiliates ("Disclosing Party") to the other party ("Receiving Party"), whether orally or in writing, that is designated as confidential or a reasonable person would consider confidential. Confidential Information includes all information concerning: the Disclosing Party's customers and potential customers, past, present or proposed products, marketing plans, engineering and other designs, technical data, business plans, business opportunities, finances, research, development, and the terms and conditions of this Agreement. Confidential Information does not include any information that (i) is or becomes generally known to the public without breach of any obligation owed to the Disclosing Party, (ii) was known to the Receiving Party prior to its disclosure by the Disclosing Party without breach of any obligation owed to the Disclosing Party, (iii) is received from a third party without breach of any obligation owed to the Disclosing Party, or (iv) was independently developed by the Receiving Party. Subject to the foregoing exclusions, Customer Data will be considered Confidential Information under this Agreement regardless of whether or not it is designated as confidential."*
> — Customer Terms of Service
> *"The Receiving Party will: (i) protect the confidentiality of the Confidential Information of the Disclosing Party using the same degree of care that it uses to protect the confidentiality of its own confidential information of like kind, but in no event less than reasonable care, (ii) not use any Confidential Information of the Disclosing Party for any purpose outside the scope of this Agreement, (iii) not disclose Confidential Information of the Disclosing Party to any third party (except those third party service providers used by us to provide some or all elements of the Subscription Service or Consulting Services and HubSpot Solutions Partners bound by confidentiality obligations), and (iv) limit access to Confidential Information of the Disclosing Party to those of its and its Affiliates' employees, contractors and agents who need such access for purposes consistent with this Agreement and who have signed confidentiality agreements with the Receiving Party containing protections no less stringent than those herein."*
> — Customer Terms of Service
> *"We may use Customer Data to develop, support, and improve HubSpot AI features and functionality. We may also use Customer Data to train our AI models in compliance with our obligations under the Agreement. You may opt out of having your Customer Data used for this purpose by updating your settings in your HubSpot account. If you opt out, we will no longer collect Customer Data to train our AI models, unless you later update your settings and opt in."*
> — Customer Terms of Service

*"We will ensure that any personnel whom we authorize to Process Customer Personal Data on our behalf is subject to appropriate confidentiality obligations (whether a contractual or statutory duty) with respect to that Customer Personal Data."*
— Data Processing Agreement

# Documents

| Title | URL | Type | Scraped At | Replaced |
|---|---|---|---|---|
| Customer Terms of Service | https://legal.hubspot.com/terms-of-service | text/markdown | 2026-06-28T18:08:22.475Z | No |
| Product Specific Terms | https://legal.hubspot.com/product-specific-terms | text/markdown | 2026-06-28T18:08:40.575Z | No |
| Data Processing Agreement | https://legal.hubspot.com/dpa | text/markdown | 2026-06-28T18:09:05.071Z | No |
| Acceptable Use Policy | https://legal.hubspot.com/acceptable-use | text/markdown | 2026-06-28T18:09:17.558Z | No |
| HubSpot Privacy Policy | https://legal.hubspot.com/privacy-policy | text/markdown | 2026-06-28T18:09:37.327Z | No |

# Beyond-Playbook Findings

### Broad Vendor Setoff Rights May Extinguish Customer Refunds and Credits [MEDIUM] — § 3.3.3 (Collection and Setoff Rights)

Section 3.3.3 grants HubSpot the right to set off and deduct any amounts the customer owes from any amounts HubSpot owes the customer, including refunds, credits, and other payments. This is structurally adverse because refunds and SLA credits are the customer's primary contractual remedies under this Agreement — warranty breach refunds (§ 10.1), termination-for-cause refunds (§ 4.5), and service uptime credits (§ 9.2 of PST) could all be unilaterally reduced or eliminated if HubSpot asserts an offsetting balance. Combined with the prepayment structure (§ 3.5: 'all fees are due and payable in advance throughout the Subscription Term'), customers may have substantial advance payments outstanding while simultaneously being owed remedial credits — and HubSpot can net those credits against any disputed charges without judicial process. Market standard: setoff rights are common in SaaS contracts but are typically limited to undisputed, liquidated amounts. Extending setoff rights to refunds and credits — which are themselves remedies for HubSpot's non-performance — creates circularity that undermines the remedy structure. Common remediation: limit setoff rights to undisputed amounts; exclude SLA credits and warranty refunds from setoff eligibility.

### AI Output Non-Uniqueness Acknowledgment Creates Commercial IP and Competitive Risk [MEDIUM] — § 7.4 (Ownership and Rights — HubSpot AI)

Section 7.4 of the Product Specific Terms requires the customer to affirmatively acknowledge that AI Output may not be unique and that HubSpot AI may generate the same or similar output for other users or third parties. This creates layered risks: (1) commercially sensitive AI-generated materials — marketing copy, sales scripts, strategic messaging, pricing proposals — may be functionally identical to output provided to direct competitors using the same platform; (2) under current U.S. Copyright Office guidance (February 2023 registration guidance and subsequent USCO decisions), AI-generated content that lacks human creative authorship may receive no copyright protection; identical AI output across customers means neither party may have a protectable IP interest in the content; (3) in regulated industries (e.g., financial services, healthcare), duplicated AI-generated compliance language or client communications could create regulatory exposure if the output is presented as customized advice. Emerging regulatory context: the EU AI Act's transparency obligations for general-purpose AI systems and several U.S. state AI disclosure bills are beginning to address output attribution and uniqueness disclosure requirements. This acknowledgment clause essentially pre-empts any IP warranty claim for AI Output. Common remediation approaches: limit high-stakes use cases (e.g., regulatory filings, client-facing legal documents) to non-AI-generated content; seek written commitment that AI Output will not be provided to identified direct competitors in identical form.

### Non-Exhaustive Restricted Industries List Enables Unilateral Service Discontinuation Outside Defined Breach Standards [MEDIUM] — § 6 (Restricted Industries)

The Acceptable Use Policy Section 6 reserves HubSpot's right to discontinue service if the customer operates in a 'Restricted Industry,' characterized by 'higher than average abuse complaints.' The listed industries (Cryptocurrency, NFTs, Pharmaceuticals, Multi-level Marketing, Gambling, List Brokers, etc.) are explicitly framed as 'some examples,' making the list non-exhaustive. Several concerns arise that fall outside the playbook's standard termination analysis: (1) HubSpot may apply this right to unlisted industries at its sole discretion based on its own complaint-monitoring assessment; (2) no objective threshold, industry classification standard, or appeal mechanism is defined; (3) the AUP is itself unilaterally updatable by HubSpot (AUP § 9.3), meaning new industries can be added to the restricted list without meaningful customer

consent or negotiation; (4) the Pharmaceutical category is particularly broad and could sweep in medical device companies, health technology providers, and life sciences firms that have no history of abusive marketing practices; (5) it is not specified whether industry-based discontinuation triggers any refund right (the General Terms § 4.5 refund provisions are anchored to 'termination for cause' under § 4.3, not AUP-based discontinuation). Common remediation: customers in or adjacent to listed industries should seek written confirmation that their specific use case falls outside the restriction; negotiate a defined cure period and refund entitlement if HubSpot exercises this right.

### SLA Credit Remedy Requires Two Consecutive Months of Failure and Is the Sole Exclusive Remedy for All Uptime Failures [MEDIUM] — § 9.2 (Service Uptime)

Section 9.2 of the Product Specific Terms conditions the customer's sole and exclusive uptime remedy on Service Uptime falling below 99.95% for two or more *consecutive* calendar months. This structure is materially adverse for several reasons: (1) a single calendar month of severe or complete outage — including outages lasting days — triggers zero compensable remedy; (2) alternating months of failure and recovery (e.g., February fails, March recovers, April fails) permanently reset the consecutive-month counter, allowing repeated failures to evade the credit trigger; (3) the credit request must be submitted within 20 days of the end of the relevant month — a very short administrative window with no grace provision; (4) credits apply to the *following* renewal term invoice, not the period of actual harm; (5) this section is explicitly the 'sole and exclusive remedy' for uptime failures, displacing all damages claims including claims for consequential losses from downtime; and (6) Section 7.6 of PST separately excludes HubSpot AI downtime caused by third-party AI providers from the SLA calculation entirely, meaning AI-dependent workflows have no SLA protection at all. Market norm: enterprise SaaS SLAs typically provide credit after a single month of failure, with automatic credit application and no 20-day claim window. The two-consecutive-month trigger is below market standard and, given the 'sole and exclusive remedy' designation, forecloses all alternative recovery paths. Common remediation: negotiate a single-month failure trigger; automatic credit application; removal of the 'sole and exclusive remedy' designation for outages exceeding a defined severity threshold.

# Reviewers

| Name | Current Step |
|---|---|
| Acme Tenant Admin | ANALYSIS |