ChatGPT

Amazon Q Developer (AWS)

Critique: The uploaded summary of Amazon Q Developer remains largely accurate, with minor updates. It correctly notes the difference between the Free and Pro tiers in data use and privacy. In fact, AWS Service Terms confirm that only the Free Tier of Amazon Q uses customer prompts for model improvement (with opt-outs available) [1] [2]. The summary's guidance about data residency is still valid – Pro tier data stays in the customer's region (including EU/UK options), while Free Tier requests may be processed in AWS's US regions [2]. One outdated detail is the summary's mention that ISO 27001 certification was pending. As of 2025, Amazon Q Developer is **in scope for ISO 27001** and related standards (listed on AWS's ISO certifications page) [3]. AWS has also fully integrated Q Developer into its compliance programs, achieving SOC 2 and inheriting FedRAMP controls via AWS's platform. No new features beyond those in the summary were found in official docs. Overall, the guidance is **valid**, with the update that Amazon Q Developer is now covered by AWS's ISO certifications and compliance framework (meaning the service meets those security standards, as expected).

Guidance Validity: Mostly valid. The summary's content remains up-to-date regarding features, privacy, and terms. Only minor compliance updates (ISO status achieved) were needed, and these do not change the recommended use of the Pro tier for sensitive government work.

AWS Bedrock

Critique: The summary of AWS Bedrock is accurate and remains valid. It correctly states that **user data is not used to train models by default** [4] and that Bedrock can be deployed with private connectivity (e.g. AWS PrivateLink) and even on-premises via EKS for certain models. (AWS's documentation confirms Bedrock's private connectivity and zero-training commitments [4].) One notable update since the summary was written is that **AWS Bedrock achieved FedRAMP High authorization in AWS GovCloud (US)** in 2024, making it approved for U.S. federal use [5]. The summary did not mention FedRAMP, which is a significant compliance milestone. Additionally, Bedrock now explicitly supports **HIPAA eligibility** for healthcare workloads [4], which aligns with the summary's note on health data settings. The summary's mention of a UK region (London) for data residency is still valid – Bedrock supports regional data control, including EU regions for EU/UK customers. All other guidance (data encryption, use of AWS CloudTrail/CloudWatch for audit logging, IAM-based access controls) remains unchanged per current AWS documentation.

Guidance Validity: Valid with minor updates. The core guidance is up-to-date (no training on customer content, strong encryption, AWS compliance inherited). An added point is that AWS Bedrock is now FedRAMP High authorized [5], bolstering its suitability for government. The summary's recommendations (use Bedrock's enterprise features for privacy, leverage AWS logging and access controls) require no changes.

Azure AI Foundry

Critique: The summary of Azure AI Foundry continues to reflect the current state of this service. Azure AI Foundry (launched in preview in 2024) indeed provides an end-to-end platform with model catalog, multi-agent orchestration, and governance features as described. The summary correctly notes that it operates

under Microsoft's standard terms (Product Terms, DPA for GDPR) and that **customer data is not used to retrain models** by default (this is confirmed by Microsoft's documentation for Azure OpenAI and Foundry) [6]. The described privacy controls – private networking (via Azure Private Link), customer-managed encryption keys, role-based access via Entra ID (Azure AD), and diagnostic telemetry opt-out – are all supported in current Foundry documentation. Since the summary was written, Azure AI Foundry has moved further toward general availability, with Microsoft unveiling additional features (e.g. a **general release of the Agent service and new model options**) at Build 2025 [7] [8]. These enhancements do not contradict the summary; they mainly expand on Foundry's capabilities (e.g. new model providers like xAI and Mistral, which the summary already anticipated under "model catalogue"). Azure's compliance stance remains the same: Foundry inherits **Azure's certifications (ISO/IEC 27001, SOC 2, etc.)** as noted in the summary [9], and it aligns with Azure's general compliance programs. No outdated details were found in the summary – it even anticipated the need for preview terms and noted that UK/EU data residency can be configured (Azure now confirms that Foundry data stays in chosen regions by leveraging Azure's regional resources).

Guidance Validity: Fully valid. The summary accurately captures Azure AI Foundry's privacy, data handling, and compliance posture. Recent product updates (feature GA announcements) add nuance but do not invalidate any guidance. The advice about using the enterprise (Workspace) mode for government, leveraging Azure's built-in security controls, and reviewing preview terms remains sound.

ChatGPT (OpenAI)

Critique: The guidance in the ChatGPT summary remains largely **accurate and current**. It correctly differentiates between Free/Plus accounts and the business-oriented **ChatGPT Team and Enterprise plans**, particularly regarding data usage. As the summary states, OpenAI **does not use data from ChatGPT Team/ Enterprise customers to train its models** [10], and this is confirmed in OpenAI's latest privacy commitments. The summary noted that Enterprise customers can opt for European data residency from February 2025 – indeed OpenAI launched an EU data residency option for new Enterprise and Education workspaces in early 2025 [11]. (OpenAI further expanded data residency in mid-2025 to include other regions like the US, Japan, Canada, etc., for API and enterprise users [12], though Europe remains the key region for UK/EU compliance needs.) The summary's description of privacy controls is up-to-date: the **chat history toggle** and 30-day retention when off, the ability to **export or delete data**, and the default exclusion of business data from model training are all unchanged in OpenAI's documentation [13] [10]. It also correctly lists **SOC 2 Type II and CSA STAR** Level 1 certification for ChatGPT's business services [13]. One addition since the summary is that OpenAI achieved **Privacy Shield successor compliance (the EU–US Data Privacy Framework)** in 2023, which the summary already anticipated by referencing that transfers rely on legal safeguards [14]. There have been no significant policy shifts – OpenAI's approach to user prompts and data review (e.g. limited human review for abuse, which the summary notes for free users) remains the same.

Guidance Validity: Valid with no significant changes. The summary's recommendations – use Enterprise for sensitive data, leverage the history-off mode, and note the new EU data residency option – are fully aligned with current official guidance. Recent expansions in data residency (additional regions beyond Europe) and ongoing compliance (OpenAI's SOC 2, STAR listings) reinforce the summary's points rather than contradict them.

Claude and Claude Code (Anthropic)

Critique: The summaries for Anthropic's Claude and Claude Code are still **up-to-date and accurate**. The key guidance was that Anthropic does *not* use customer conversations or code to train its models by default – this remains true. Anthropic explicitly states it will **not use your prompts or outputs to train Claude** unless you opt in or flag content for abuse review [15], and this policy covers both Claude's chatbot and the Claude Code tool. The summary highlighted Claude's **plan tiers** (including an Enterprise tier with added security) and noted that regular chats aren't reviewed by humans. That holds: Anthropic's privacy center confirms no human reviewing of normal Claude chats, except for safety violations. For **Claude Code**, the summary correctly describes that it runs locally and only sends snippets to the AI. In fact, Anthropic documentation for Claude Code reiterates that code and prompts sent to the Claude Code assistant are **not used to train models** [16], and processing occurs in-memory. The summary's mention of **custom retention periods and audit logs for Enterprise** is still valid – Anthropic's enterprise dashboard offers those controls. On compliance, the summary is very current: Anthropic has achieved **SOC 2 Type II and ISO 27001:2022**, and notably was an early adopter of **ISO 42001 (AI management)** and FedRAMP. In mid-2025, Claude became available in FedRAMP High environments (via AWS GovCloud and Google's IL2 platform) [17], exactly as the summary anticipated. No details in the summary appear outdated or incorrect. (Anthropic has introduced newer model versions like Claude 2 and Claude Instant, but these do not affect the privacy and compliance guidance given.)

Guidance Validity: Fully valid. The summary's guidance – especially using Claude's Enterprise settings to ensure no data leaves the organisation – remains the best practice and aligns with current official policy. No changes are needed to the advice; it already incorporates Anthropic's strong privacy stance and recent compliance credentials (ISO certifications, FedRAMP authorization, etc.), which have since been confirmed [18] [19].

Cursor

Critique: The summary for Cursor (the AI-powered code editor) is **accurate and up-to-date**, capturing its unique privacy modes and enterprise features. In late 2024, Cursor introduced the new **Privacy Mode vs. Privacy Mode (Legacy)** distinction, which the summary details. This aligns with Cursor's documentation: *Privacy Mode (new)* allows limited encrypted storage for advanced features, whereas *Legacy mode* stores nothing on servers [20]. The summary correctly warns that **"Standard" mode (privacy off) is not suitable for government use** due to broad telemetry. That guidance stands – Cursor's security page emphasizes zero-retention for enterprise and minimal data collection even in Privacy Mode [21] [22]. Since the summary, Cursor has integrated additional AI model providers, such as **Google's Gemini via Vertex AI and xAI's Grok**. These were not explicitly named in the summary but fall under its note of "multiple AI providers." Notably, Cursor has entered into zero-data-retention agreements with these providers (as it had with OpenAI and Anthropic) [21] [22], so this expansion doesn't change the privacy posture – it reinforces that even if Google's or xAI's models are used, user code snippets aren't retained by them. The summary's discussion of data locations is still current: Cursor's servers operate primarily in the US with some EU/Asia presence for latency [23] [24], and all requests from users (even with self-provided API keys) go through Cursor's backend. One new item is that Cursor obtained **SOC 2 Type II certification** (confirmed on their security page in mid-2025) – the summary already implied strong security but did not explicitly mention SOC 2. Still, this certification [25] [26] validates the summary's assurance of Cursor's enterprise readiness. No policies have changed: code remains private by default in enterprise, and admins can enforce org-wide privacy settings as described.

Guidance Validity: Valid. The summary's guidance about using Cursor's Privacy Mode (or Legacy mode) in government settings and leveraging its admin controls remains correct. Recent developments (support for more LLM providers, SOC 2 compliance) strengthen the product's enterprise suitability and were in line with the summary's points. No corrections to the guidance are necessary.

GitHub Copilot for Business

Critique: The summary's guidance on GitHub Copilot for Business is **still accurate** and has no significant outdated elements. It properly highlights Copilot for Business features like **public code filtering**, **organization-wide policy controls**, and that by default **no prompts or completions from Business users are retained or used for training** [27] [28]. Microsoft's documentation and GitHub's terms confirm this: Copilot for Business does not feed customer code into the training set of the AI models [29] [30]. The summary also notes that admins can choose which underlying AI model to use (or disable third-party models). Currently, GitHub primarily uses OpenAI's models hosted on Azure, and an admin can indeed enforce that only Microsoft's infrastructure is used (this effectively is the case by default – no calls go to external non-Microsoft APIs). No new privacy features have been introduced since the summary; rather, Microsoft has maintained the same approach. In 2023, GitHub aligned Copilot with the **EU-US Data Privacy Framework** and continues to rely on Standard Contractual Clauses for transfers [14], which the summary covers. The compliance certifications remain as stated: GitHub's platform is **SOC 2 Type II, ISO/IEC 27001, 27018, and CSA STAR** certified [31] (the summary mentioned these inherited certifications). One small update: GitHub has improved transparency by providing an opt-out for public code owners who don't want their code used in training, but this is an ecosystem change and does not affect Copilot for Business users (whose data was never used in training anyway). Additionally, GitHub has not yet made Copilot officially cleared for higher-classified data (it's still generally recommended only up to OFFICIAL, with caution at OFFICIAL-SENSITIVE). The summary's caution on that point remains apt.

Guidance Validity: Fully valid. The best practices – use Copilot for Business (not the free Copilot) for any government or sensitive projects, and leverage its admin controls like disabling suggestions that match public code – are unchanged. The summary needs no corrections; its privacy and compliance statements are confirmed by current GitHub documentation and have been reinforced by Microsoft's ongoing compliance updates (e.g. DPA coverage under the Microsoft Online Services terms).

Google Gemini

Critique: The summary of Google Gemini is **accurate and reflects the current product offerings**, with no major discrepancies. In late 2023 and 2024, Google rebranded its generative AI assistant across consumer and Workspace products to "Gemini," and the summary captures this evolution (describing free vs. enterprise versions, integration with Gmail/Drive, etc.). The summary correctly warns that the **free consumer Gemini (e.g. in Google's personal accounts)** logs user conversations and uses them for model improvement by default [32]. Google's documentation confirms that consumer AI services (like the Gemini/Bard consumer app or the Google One AI features) may retain history and use it unless the user opts out. Conversely, the summary highlights that **Gemini Enterprise (within Google Workspace)** does *not* use conversations for training, and no human reviewers assess those chats [33] [34]. This is explicitly stated by Google: with Gemini for Workspace, prompts are not used for advertising or model training, and Google provides strong privacy commitments [34]. The summary also notes **data residency and processing** – this remains a consideration. Google confirms that Gemini processing may occur globally and cannot guarantee UK/EU processing for all real-time interactions [35] [36], though saved Workspace data can reside in Europe

if an admin has set a data region for Google Drive, etc. Since the summary, Google achieved significant compliance milestones for Gemini: in March 2025, **Google's Gemini (Workspace and app) became FedRAMP High authorized** [37] – the first generative AI chat assistant to do so – and Google also touts that Gemini has comprehensive certifications (SOC 2, ISO 27001/27017/27018, **ISO 27701 for privacy**, and even **ISO 42001 for AI**) [19]. The summary did list those standards (including ISO 42001, calling out that Gemini was the first chat AI to get it). This indicates the summary was well-informed and nothing is missing on that front. One minor note: Google has since merged "Duet AI" branding into Gemini, and introduced a paid consumer tier (Google One AI Premium) for Gemini access, but those do not alter the privacy considerations the summary outlines. The summary's advice to **use the Workspace (Enterprise) Gemini for any government or sensitive use** is strongly reinforced by these developments – that edition now carries FedRAMP High and other assurances.

Guidance Validity: Valid and comprehensive. The summary's information is up-to-date. It correctly distinguishes the free vs. enterprise usage and highlights data sovereignty concerns which remain true (Gemini cannot guarantee UK-only processing for live queries [36]). The noted certifications and policies in the summary have been confirmed by Google's announcements. Therefore, the guidance stands as given: avoid the free version for official use and prefer the enterprise Gemini with its privacy safeguards.

Google NotebookLM

Critique: The summary of Google NotebookLM is **accurate** and requires no major changes. NotebookLM (an AI research assistant for notes/documents) was in public preview and is now part of Google Workspace (recently included for all Workspace users). The summary correctly states NotebookLM's core principle: it **does not use customer-provided content to train Google's models** [38]. Google's help center explicitly says personal data in NotebookLM is never used to train AI [39]. The summary highlights the distinction between **Personal NotebookLM** (under consumer Google terms) and **Workspace NotebookLM** (enterprise) – this remains applicable. In Workspace NotebookLM, data stays within the organisation's Google Cloud tenant and is subject to Google's DPA, which is true; NotebookLM is now a core Workspace service covered by the Workspace customer agreement and data processing amendment (GDPR compliant) [40]. The summary also notes that in the enterprise version, admins can control retention and sharing – indeed Google has added admin controls to enable/disable NotebookLM and (coming soon) set custom retention periods for notes [41]. One update is that Google now allows **regional data storage** for some Workspace data; the summary mentions that Workspace admins *can pin data to UK/EU/US regions if required* [42]. This is accurate: Workspace's data region setting can apply to NotebookLM notebooks (since they are stored in Google Drive as documents under the hood), so an organisation could ensure the stored content resides in a European data center. For in-flight processing, the summary correctly notes data may be processed globally for performance [42]. The audit logging and access control features described are also current – NotebookLM writes audit events to Google Cloud Logging and provides Access Transparency logs for any Google support access [43] [44]. The compliance section of the summary is up-to-date: NotebookLM inherits **ISO 27001, SOC 2, HIPAA, PCI, and FedRAMP Moderate** via Google Workspace [45]. (Since Workspace itself recently achieved FedRAMP High for certain services, NotebookLM may also benefit from that in the future, but as of now it's under FedRAMP Moderate as stated.) No content in the summary appears outdated – if anything, it was prescient in noting upcoming features like custom retention (now confirmed by Google's roadmap).

Guidance Validity: Fully valid. The summary's guidance that NotebookLM enterprise can be used for Official data (with proper policies) is still sound. It emphasizes that no model training occurs and that data

stays within the Workspace domain – both key points remain true. There have been no policy regressions or changes that contradict the summary. Government users should follow the summary's advice to use NotebookLM via Google Workspace (not personal accounts) and apply the available admin guardrails; this aligns with Google's latest privacy documentation for the tool.

Windsurf (Exafunction)

Critique: The summary of Windsurf is **very thorough and remains up-to-date**, capturing this tool's strong focus on enterprise privacy and deployment flexibility. Windsurf (formerly known as Codeium) indeed offers multiple deployment modes as the summary describes: **Standard cloud (US-based)**, an **EU cluster in Frankfurt** for European data residency, a **FedRAMP High GovCloud deployment**, hybrid on-prem/cloud, and even fully self-hosted options [46] [47]. These options are confirmed on Windsurf's official site, which highlights its FedRAMP High authorization and DoD IL5/ITAR compliance for government use [48]. The summary correctly notes Windsurf's **zero-data-retention mode** – by default, enterprise cloud users have no code persisted on Windsurf servers [49]. Current documentation reinforces that: enterprise requests are processed in memory with zero retention unless an organisation opts into features that require it [50]. The summary's mention that **administrators can disable specific external AI providers and features like web search** remains accurate; Windsurf provides granular feature toggles for orgs [51]. Another accurate point is audit logging: the summary notes that detailed audit logs (down to every AI suggestion and content matching) are available in hybrid/self-hosted deployments [52] [53]. Windsurf's security documentation confirms that full audit and attribution logs are kept on the customer-controlled side in those deployments, to support compliance needs. The terms and privacy notes in the summary (June 2025 update, DPA support, data controller/processor roles, etc.) align with Windsurf's policies; notably, Windsurf distinguishes enterprise customers' data ownership and offers DPAs, as the summary says. Since the summary, there have been no known policy changes – if anything, Windsurf's position has been strengthened by achieving formal **FedRAMP High authorization** (through the FedStart program) and listing its solution on the FedRAMP Marketplace. The summary already anticipated this compliance (it explicitly mentions FedRAMP High and IL5, which Windsurf has attained). The summary did not explicitly mention that Windsurf is **SOC 2 Type II certified**, but this is indeed the case as of early 2025 [54] – inclusion of that detail only bolsters the summary's message that Windsurf is serious about security. All features (like Cascade agentic AI, multi-model support) are described accurately.

Guidance Validity: Valid and very comprehensive. The summary's guidance requires no changes. It correctly advises on using Windsurf's zero-retention and secure deployment options for government scenarios. The multi-regional and even on-premises choices it documented are confirmed by official sources, and Windsurf's attainment of FedRAMP High/IL5 compliance underscores the reliability of the summary. Agencies can continue to follow the summary's recommendations (e.g. deploy in GovCloud or Frankfurt as needed, use hybrid mode for audit logging) with confidence that they reflect the current state of Windsurf.

Sources:

- AWS Service Terms – Amazon Q Developer data use [1] [2]; AWS ISO Certifications (service in scope) [3]
- AWS Bedrock Security & Compliance page – no training on customer data, compliance programs (ISO, HIPAA, FedRAMP High) [4] [5]

- Microsoft Azure Blog – Azure AI Foundry announcements (built-in security, model catalog) [7] [8] ; Azure compliance (ISO 27001, SOC 2 for platform) [9]
- OpenAI Security & Privacy page – SOC 2 Type II and CSA STAR for ChatGPT business [13] ; OpenAI blog – European data residency launch (Feb 2025) [11] and expansion (May 2025 update) [12] ; OpenAI privacy commitments (no training on Enterprise data) [10]
- Anthropic Trust Center – Claude FedRAMP High/DoD IL5 announcement [17] ; Anthropic Privacy Center – data not used for training by default [15] ; Anthropic FAQ – Claude Code data handling (no training on your code) [16]
- Cursor Security page – integration with multiple model APIs (OpenAI, Anthropic, Google Vertex, xAI) under zero-retention agreements [21] [22] ; Cursor Security page – global infrastructure (US/EU servers) [23] and SOC 2 certification [26]
- GitHub Copilot documentation – default no-training and enterprise data protection [27] [14]
- Google Workspace Blog – Gemini for Workspace launch (Enterprise data not used for training, privacy commitments) [33] ; Google Cloud Public Sector blog – FedRAMP High for Gemini (certifications ISO 27001, ISO 42001, etc.) [19] [37]
- Google NotebookLM product page – privacy and security (no model training on user data) [38] ; Google support doc – “NotebookLM protects your data” [39] ; NotebookLM Help Center – enterprise coverage under Workspace DPA [40] ; NotebookLM admin settings (retention control roadmap) [41]
- Windsurf Security page – FedRAMP High accreditation and IL5 compliance [48] , SOC 2 Type II certification [54] , deployment options (US, GovCloud, EU) [46] , zero-retention default [50] .

---

[1] [2] AWS Service Terms
https://aws.amazon.com/service-terms/

[3] ISO Certified
https://aws.amazon.com/compliance/iso-certified/

[4] [5] Secure Gen AI Apps - Amazon Bedrock Security and Privacy - AWS
https://aws.amazon.com/bedrock/security-compliance/

[6] Azure AI Foundry frequently asked questions - Azure AI Foundry | Microsoft Learn
https://learn.microsoft.com/en-us/azure/ai-foundry/faq

[7] [8] Azure AI Foundry: Your AI App and agent factory | Microsoft Azure Blog
https://azure.microsoft.com/en-us/blog/azure-ai-foundry-your-ai-app-and-agent-factory/

[9] azure-ai-foundry-summary.md
file://file-T4vUsVCipzor7WShxCC7LS

[10] [11] [12] Introducing data residency in Europe | OpenAI
https://openai.com/index/introducing-data-residency-in-europe/

[13] Security | OpenAI
https://openai.com/security-and-privacy/

[14] [27] [28] [31] github-copilot-summary.md
file://file-L7rEHY8JZaYwghNQSs8JSc

[15] Is my data used for model training? | Anthropic Privacy Center
https://privacy.anthropic.com/en/articles/10023580-is-my-data-used-for-model-training

16 Data usage - Anthropic API
https://docs.anthropic.com/en/docs/claude-code/data-usage

17 18 Claude in Amazon Bedrock: Approved for Use in FedRAMP High and DoD IL4/5 Workloads \ Anthropic
https://www.anthropic.com/news/claude-in-amazon-bedrock-fedramp-high

19 37 Gemini in Workspace and the Gemini app are first to achieve FedRAMP High | Google Cloud Blog
https://cloud.google.com/blog/topics/public-sector/gemini-in-workspace-apps-and-the-gemini-app-are-first-to-achieve-fedramp-high-authorization

20 Discussions - Cursor - Community Forum
https://forum.cursor.com/c/general/4/l/latest?page=23

21 22 23 24 Security | Cursor - The AI Code Editor
https://cursor.com/en/security

25 Guide to Cursor | Software.com
https://www.software.com/ai-index/tools/cursor

26 What is SOC 2? Principles, types & requirements - Cursor Insight
https://www.cursorinsight.com/post/1156/what-is-soc-2-principles-types-requirements

29 Does GitHub Copilot use any code from individual users to train ...
https://github.com/orgs/community/discussions/152229

30 Does Github Copliot save or use any code? #149873
https://github.com/orgs/community/discussions/149873

32 35 36 41 google-gemini-summary.md
file://file-VBcFq1AeuFfxQVRA8pkSt6

33 34 Announcing Gemini for Google Workspace | Google Workspace Blog
https://workspace.google.com/blog/product-announcements/gemini-for-google-workspace

38 NotebookLM: AI-Powered Research and Learning Assistant Tool | Google Workspace
https://workspace.google.com/products/notebooklm/

39 Learn how NotebookLM protects your data - Google Help
https://support.google.com/notebooklm/answer/15724963?hl=en

40 42 43 44 45 notebooklm-summary.md
file://file-Nued9XsB888c8oBu4gxJSa

46 50 54 Security | Windsurf
https://windsurf.com/security

47 49 51 52 53 windsurf-summary.md
file://file-5kjfEybmznABq1Hj8crzAj

48 Windsurf for Government | Windsurf
https://windsurf.com/enterprise/government