ChatGPT

Review of AI Tool Guidance Summaries

Below we examine each AI tool's current state compared to the provided guidance, highlighting any discrepancies or updates and assessing whether the guidance remains valid.

1. Aider

Discrepancies: The guidance for Aider remains accurate. Aider is an open-source, local AI coding assistant, and there have been no major changes to its privacy features or data handling. By default, Aider does **not** send your code to its servers, and analytics are strictly opt-in [1] [2]. The summary correctly notes that all source code stays on the user's machine and that Aider does not use code for model training. The privacy policy confirms data is only collected if explicitly opted in, and even then it's anonymized usage metrics (no code content) [3] [4]. Aider still has no formal security certifications (as expected for a local open-source tool), and this has not changed. No new subscription tiers or enterprise features have been introduced – Aider remains free and Apache 2.0 licensed, with an emphasis on using local models for maximum security.

Assessment: Guidance Valid. The existing guidance is up-to-date. Aider's privacy-first design (all code local by default, optional analytics) remains as described, and there are no new compliance concerns or features to add. Users should continue following the guidance: use local models and disable analytics for sensitive work, which aligns with current best practices.

2. Amazon Q Developer

Discrepancies: The guidance for Amazon Q Developer is largely correct, with a few updates on data handling and compliance. The summary accurately distinguishes between the **Free** tier and **Pro** tier privacy differences. Notably, **Free Tier** content **may be used for service improvements by default** (i.e. stored and used to refine models), whereas the **Pro (Enterprise)** tier ensures customer prompts/code are not used to train models [5]. This remains true. One update is that **Free tier data is stored in U.S. regions** only, while **Pro tier data stays in the customer's chosen AWS region**, such as EU or UK regions [6]. The summary mentioned this, and AWS's documentation confirms that at the Pro tier, data at rest remains in-region (e.g. EU for London) and free-tier requests default to US servers [6].

In terms of **compliance**, the guidance noted Amazon Q Developer was not yet listed under AWS's ISO 27001 scope. This has changed – as of early 2025, Amazon Q Developer *has been added* to AWS's ISO/IEC 27001:2022 certification scope and CSA STAR registry [7]. It also inherits AWS's broader compliance (SOC 1/2/3, ISO 27017/27018, etc.), so the expectation in the summary that ISO 27001 would be achieved is now fulfilled.

A significant event **not in the original guidance** is a **security incident** in July 2025 involving the VS Code extension for Amazon Q Developer. A malicious code injection in an extension update (version 1.84.0) was discovered and quickly fixed by AWS [8] [9]. Fortunately, the malicious code never executed due to a syntax error and no customer code was compromised [10]. AWS released a patched version 1.85.0 and removed the

bad update [11]. This incident underscores the importance of keeping Q Developer plugins up-to-date. The core service's privacy and data controls were unchanged, but this is a new consideration for tool security (the summary did not cover this, as it occurred afterward).

Assessment: Guidance Mostly Valid (minor updates needed). The existing guidance remains accurate about tiered privacy (Free vs. Pro), data residency, and enterprise controls. It would be beneficial to update the guidance with the following: (1) **Compliance:** Note that Amazon Q Developer is now ISO 27001 certified as part of AWS's audited services [7]. (2) **Security:** A brief mention of the July 2025 VS Code extension compromise and the importance of using the latest extension (v1.85.0 or later) could be added, though AWS handled it swiftly [9]. Overall, the privacy features (no training on Pro tier, regional data storage options) and access controls (IAM-based) remain as described and effective [5] [6].

3. Amazon Bedrock

Discrepancies: The guidance for AWS Bedrock remains **up-to-date and accurate**. The summary correctly states that Bedrock **does not use customer prompts or outputs to train models by default** – AWS confirmed that foundation models are not trained on your data [12]. It also emphasizes data residency options, noting a **UK (London) region is available** for Bedrock. This was aspirational at first, but as of June 2024 Amazon Bedrock became available in the **London region** (along with other EU regions) [13]. Bedrock now spans 13 regions including eu-west-2 (London), Frankfurt, etc., fulfilling the summary's promise of UK/EU region support. The summary's mention of **PrivateLink**, **dedicated capacity**, and even **on-premises via EKS Anywhere** is still current – AWS continues to offer those deployment options for enhanced privacy and performance. There have been no reported changes to Bedrock's default privacy stance: prompts are processed in memory and not stored permanently unless you intentionally use features like model fine-tuning or knowledge bases, which are stored with encryption (AES-256) [14]. The **compliance** notes in the summary hold true: Bedrock inherits AWS's certifications (SOC 2, ISO 27001/27018, CSA STAR) and supports HIPAA-eligible workloads, etc. One minor update is that AWS's overall compliance now includes the new EU–US Data Privacy Framework (as of 2023) for transfers – the summary references SCCs, which is fine and still applicable.

There is no indication of new **subscription tiers** or fundamental changes in access control since the guidance. Bedrock remains an AWS-managed service that integrates with AWS IAM, CloudTrail, and CloudWatch for audit and access control as described [15] [16]. Recent AWS announcements mostly expanded Bedrock's features (e.g. more model providers, **Bedrock Agents** for chaining tasks) but these don't conflict with the privacy guidance.

Assessment: Guidance Valid. The Bedrock guidance is comprehensive and still accurate. It could be lightly updated to celebrate that the **Europe (London) region is indeed live** for Bedrock [13], as well as other EU regions, which reinforces the data residency assurances. Otherwise, the default "no training on customer data" policy and encryption measures remain in place, and the guidance requires no substantive changes.

4. Azure AI Foundry

Discrepancies: The guidance for Azure AI Foundry remains largely valid, with minor contextual updates. Azure AI Foundry is a relatively new platform (still evolving through 2024–2025), and the summary correctly captures its essence: a unified environment in your Azure subscription with **model catalog, multi-agent**

orchestration, and governance. Notably, resources (hubs, projects) reside in the customer's Azure subscription, meaning data stays under your control – this is unchanged and remains a key design principle. The described **privacy settings** are accurate: support for **Private Link** (to keep traffic off internet), **customer-managed keys (CMK)** for encryption, and strict role-based access via Entra ID (Azure AD) all remain available and recommended.

One update is that Azure AI Foundry's **Agent Service** moved from preview to **general availability (GA)** in early 2025 (announced at Microsoft Build 2025) [17] [18]. This GA introduced new features (e.g. enhanced multi-agent workflows, observability tools), but these don't undermine the privacy or security controls noted in the summary. If anything, Microsoft has doubled down on governance features – for example, **Foundry Observability** (in preview) adds end-to-end monitoring of agent actions, which complements the "Diagnostic data opt-in" mention in the guidance [19]. The **terms of use and data handling** remain as described: Azure Foundry, as part of Azure, falls under Microsoft's standard Product Terms and Data Protection Addendum, with previews having supplemental terms. The summary's note that it's under preview might be slightly outdated now that portions are GA, but Microsoft still treats customer data carefully under contract even in preview.

No changes have been reported in **data residency**: Foundry still allows you to deploy hubs in a single region (e.g. UK South or other Azure regions) and will keep runtime data in that region unless you enable cross-region disaster recovery [20]. This aligns with Azure's approach; no new cross-region processing has been imposed. **Compliance** also remains inherited from Azure – the summary's table of certifications (ISO 27001, SOC 2, GDPR compliance, etc.) is up-to-date [21]. Foundry's recent GA means it's under Microsoft's full support and compliance umbrella now.

Assessment: Guidance Valid (with minor context updates). The existing guidance is accurate about Azure AI Foundry's privacy and data controls. It may be worth noting that some features have progressed from preview to GA (e.g. the Agent Service is now GA as of Build 2025) and that Microsoft continues to enhance governance (observability, policy enforcement) – all in line with the original guidance's direction [17] [18]. The core privacy posture (customer data in your Azure tenant, private networking, CMK encryption) and compliance stance (Azure's certifications, GDPR alignment) remain unchanged and correctly documented.

5. ChatGPT (OpenAI)

Discrepancies: The guidance for ChatGPT is very well-aligned with current OpenAI policies, with a couple of notable updates regarding data residency and enterprise features. The summary correctly outlines the **subscription tiers** – **Free**, **Plus**, **Team**, **Enterprise** – and their differing data protections. Since the guidance was written, OpenAI has indeed launched **ChatGPT Team** (also called ChatGPT Business in some contexts) as a paid plan for small organizations, and it operates as described: shared workspace, no training on data, etc. Pricing and features remain the same (Team is ~$25–30 per user/month, and it includes admin console features) [22].

A major update is the introduction of **data residency options for ChatGPT Enterprise**. OpenAI announced in February 2025 that new ChatGPT Enterprise (and Education) customers can elect to store their data **at rest in Europe** [23]. This means conversation content, uploaded files, etc., can be confined to EU data centers, which addresses EU and UK sovereignty requirements. The summary anticipated this ("from February 2025… data at rest in Europe for Enterprise") and it is now confirmed and live [23]. Additionally,

OpenAI has expanded residency to other regions (US, Japan, Canada, etc.) for enterprise/API, though Europe is the key option for UK government needs [24] [25]. Free/Plus/Team plans still do **not** have a data residency option – their data is stored in the U.S. by default [26], which matches the guidance.

The guidance's **privacy controls** are up-to-date. The **chat history toggle** and default behavior are as stated: Free and Plus users must manually turn off history to prevent retention/model training, whereas business tiers default to no data usage for training [27] [28]. OpenAI has maintained this policy – by default no customer content from **Enterprise/Team** is used to train models [29]. One minor clarification: OpenAI's terminology is that when history is "off," conversations are retained for 30 days for abuse monitoring then deleted, which the summary does mention [30] [31]. That remains accurate.

The **audit logging** and **access control** descriptions also remain accurate. ChatGPT Enterprise offers a Compliance API (or admin console tools) for audit logs of usage, without exposing conversation text unless explicitly pulled by the org – OpenAI continues to offer this for enterprise compliance monitoring [32]. Team plans still only provide basic metrics (no content logs), which is a current limitation. **SSO integration and SCIM** for Enterprise are available exactly as described [33]. No new tiers beyond these have been introduced (ChatGPT "Enterprise" and "Teams" are the business-focused plans).

On **compliance**, the guidance noted SOC 2 Type II and CSA STAR Level 1 – OpenAI *has* achieved those (SOC 2 Type II report in 2023, CSA STAR registry). There's no news yet of ISO 27001 for OpenAI; the guidance doesn't claim it, so no issue. It also mentions OpenAI signing BAAs for HIPAA on request – OpenAI has indicated willingness to do BAAs for enterprise API use, which presumably extends to ChatGPT Enterprise if needed, so that point remains fine.

Assessment: Guidance Valid (very minor additions). The guidance for ChatGPT is up-to-date. It correctly emphasizes not to input sensitive data in non-business tiers and to use Enterprise for maximum control. One positive update to note is the **availability of EU data residency for Enterprise customers from Feb 2025** [23], which the guidance already anticipated. It might be worth reinforcing that Free/Plus user data is stored in the US indefinitely unless history is disabled (which is unchanged) and that OpenAI's models still do not train on any data from business accounts by default [29]. All other privacy and security measures (encryption, DPA, SOC 2) remain as stated. In summary, the existing guidance stands and fully covers current ChatGPT usage considerations.

6. Claude (Anthropic)

Discrepancies: The guidance for Claude (Anthropic's AI assistant) remains largely accurate, with one notable change on data location. The summary correctly states that **Anthropic does not use normal conversation data to train its models** – this is a key part of Anthropic's policy and still true [34] [35]. Only safety-related data or user feedback may be used, which the guidance covers. It also lists Anthropic's **security certifications (ISO 27001:2022, SOC 2 Type II, etc.)** and compliance standards (HIPAA, GDPR) – those remain up-to-date and Anthropic has in fact achieved the new **ISO/IEC 42001:2023 AI management certification** as noted [36] (the summary already included ISO 42001). Additionally, Claude was approved for **FedRAMP High and DoD IL5 workloads via AWS GovCloud** in 2023 [37], which aligns with the guidance's FedRAMP mention.

The main update is regarding **data residency and processing**. The guidance assumes Claude's data is processed and stored in the United States by default [38]. This was true, but Anthropic recently announced

(effective **August 19, 2025**) an expansion to **multi-region processing** for Claude's services [39]. Specifically, while data **storage** remains in U.S. data centers, **processing** may occur in other regions (Europe, Asia, Australia) to improve latency and reliability [39] [40]. Customers can opt out to insist on US-only processing if needed [41]. For UK government users, this means that without a special arrangement, some data **may be processed outside the US (potentially in EU regions)**, although it will still be **stored** in the US by default [40]. The original guidance advised assuming U.S. jurisdiction unless otherwise negotiated – that advice still holds, but now Anthropic itself is offering limited in-region processing by default (with opt-out). It's a subtle change to note in the future.

Aside from that, **data retention policies** remain exactly as documented. The guidance's detailed breakdown (30-day deletion for user-deleted chats, 2-year retention for policy-violating prompts, 7-year for safety metadata, 10-year for feedback) matches Anthropic's published policy [42] [43]. **Audit logging** and **enterprise controls** (SSO, custom retention, admin console) are still as described – available to enterprise customers and functioning the same way [44] [45]. The summary's outline of **roles and SSO** is in line with Anthropic's offerings (Anthropic has since refined role definitions slightly, but the concept of Owner/Admin/User roles and SSO integration stands). Finally, Anthropic has not yet introduced any UK-specific government cloud or certifications beyond what is listed, which the guidance already flags as a consideration (data in US jurisdiction, need for DPIA, etc.) [46].

Assessment: Guidance Valid (with one update on data processing). The Claude guidance is up-to-date on privacy, data handling, and compliance. One new development to incorporate would be Anthropic's **expansion of processing to multiple regions** for Claude services [39]. Practically, UK users should still treat Claude as U.S.-hosted unless they have an enterprise agreement, but they should be aware that after Aug 2025 some processing might occur in EU/Asia unless they opt out [41]. This nuance aside, Anthropic's commitment not to use customer conversations for training, its encryption of data in transit and at rest, and its offering of enterprise controls all remain exactly as the guidance describes. The tool is still under review in Defra's context, but its security posture continues to strengthen in line with the original advice.

7. Claude Code (Anthropic)

Discrepancies: The guidance for Claude Code remains accurate, reflecting Anthropic's current approach to its AI coding assistant. Claude Code's key feature – running locally in the developer's terminal and only sending relevant snippets to the cloud – is unchanged. The summary's explanation that **"your full codebase stays on your computer and only snippets/questions are sent"** continues to hold true [47] [48]. Anthropic's documentation confirms that Claude Code does not upload entire repositories, and that all communication with the Claude model is via encrypted channels with minimal necessary context [49] [50].

A notable update since the guidance is Anthropic's clarification of **telemetry controls**. The summary already covers that with **environment variables**: `DISABLE_TELEMETRY`, `DISABLE_ERROR_REPORTING`, etc., and the master switch `CLAUDE_CODE_DISABLE_NONESSENTIAL_TRAFFIC=1` [51] [52]. This matches the current state – Anthropic provides exactly these toggles and, by default, **disables telemetry when Claude Code is used via third-party clouds (Bedrock/Vertex)** [52]. The guidance correctly advises enabling this full privacy mode for government use, and indeed Anthropic documentation encourages setting that variable to opt out of *all* non-essential traffic [52]. No new types of telemetry have been introduced beyond what's documented (Statsig metrics and Sentry errors, which can be turned off, and an optional `/bug` report command) [51] [53].

The **data storage and residency** section is still current. Claude Code still primarily operates with data stored in the US by default. The guidance notes that UK/EU hosting options are possible via **AWS Bedrock (UK regions) or Google Vertex AI (EU regions)** [54] – this remains true. In fact, Anthropic highlights that enterprise users can route Claude through Bedrock or Vertex in European regions for data residency needs [39] [40]. Additionally, as mentioned above for Claude, Anthropic is enabling some multi-region processing on their side, but **Claude Code usage by enterprises could also leverage those regional infrastructures**. The summary's recommendation to contact Anthropic for UK/EU hosting is still the right approach for now [55].

One minor discrepancy is in **role terminology**: The summary mentions roles like *Primary Owner, Admin, Developer, Member* for Claude Code users [56]. Anthropic's console now defines roles a bit differently (e.g. "Claude Code User" vs "Developer" roles) [57] [58], but this is a nuance in naming – the idea that enterprise admins can control who has Claude Code access remains correct. The overall access control (SSO integration, SCIM user provisioning) is implemented just as described [59] [60].

Assessment: Guidance Valid. The Claude Code guidance remains up-to-date regarding data handling and privacy. It properly stresses **Privacy Mode** and the importance of disabling any non-essential data sharing, which aligns perfectly with Anthropic's best practices for secure use [52]. No new features have undermined these controls – if anything, Anthropic has reinforced them. The guidance could be slightly refined to use Anthropic's latest role labels, but functionally nothing has changed (enterprise admins still enforce privacy and no code is retained). All compliance notes (Anthropic's SOC2, ISO27001, etc.) still apply equally to Claude Code usage, and the recommendation to run in the strictest privacy mode (which Anthropic's enterprise offering enforces by default) is still the gold standard.

8. Cursor

Discrepancies: The guidance for Cursor is very current, as it already includes the significant update Cursor made in late 2024 regarding **privacy modes**. In November 2024, Cursor introduced a new graduated privacy model, and the summary captures this by listing the three modes: **Legacy Privacy Mode (no code ever stored)**, **Privacy Mode (some encrypted storage for advanced features)**, and **Standard mode (telemetry enabled)** [61]. This is exactly how Cursor operates today. The guidance correctly advises that government users stick to **Legacy** or at most the new **Privacy Mode**, and *avoid Standard mode*, due to the broader data collection in standard mode [62]. That advice is still sound – Cursor itself notes that Business/Enterprise accounts default to the privacy mode (not standard) [63]. Indeed, **Business and Enterprise plans automatically enforce Privacy Mode** so that individual users cannot downgrade the privacy setting [63]. Free/Pro users still must manually opt in to privacy modes, as stated.

No notable changes in Cursor's policies have occurred since that update. Cursor remains **SOC 2 Type II certified** for security (the guidance mentions this and it's still the only major certification they cite) [64] [65]. There is no UK-specific hosting – the summary correctly notes that processing is primarily on U.S. servers (AWS in the US, with some Azure/GCP services) and even if using your own API keys, all requests route through Cursor's backend [66]. That remains true: Cursor acts as a proxy to model providers. The guidance also points out that **vector embeddings/metadata, not raw code, may be stored** to enable code search features [67]. This aligns with Cursor's descriptions that any stored data is in the form of non-reversible embeddings or short-term encrypted cache, not your actual source code text [67] [68].

One small development: Cursor's platform and company continue to evolve but no changes have been made public that affect user privacy. For instance, there's no evidence of new data residency options or regional data centers beyond the latency edge caching mentioned (the summary already notes requests might hit a London data center for latency but are processed in the US) [69]. This is still the case – no EU storage option is offered. Cursor's third-party model providers (OpenAI, Anthropic, etc.) still operate under **zero-retention agreements**, as the summary notes [70]. Cursor's updated privacy policy (Nov 8, 2024) is accurately reflected: code is never used for training, and in Privacy Mode any temporary server storage is encrypted and narrowly scoped [71] [72].

Assessment: Guidance Valid. The Cursor guidance is up-to-date and already includes the new privacy features that distinguish it from earlier AI coding tools. No corrections are needed. It might be worth reinforcing that **Business/Enterprise users automatically get the Privacy Mode** by default [63] – which the guidance does state – meaning the tool can be configured to meet government requirements. Also, since nothing significant has changed, the recommendation to use *Legacy Privacy Mode* for the highest security or the new *Privacy Mode* if features like "Background Agents" are needed (with a risk assessment) is still the best practice. In summary, Cursor's current operation matches the guidance, and the advice given remains fully applicable.

9. GitHub Copilot (for Business)

Discrepancies: The guidance for GitHub Copilot for Business is accurate and remains consistent with Microsoft's current offering. Copilot's privacy and security features for the Business tier (now the recommended tier for organizations) have not changed since the summary. The key points in the guidance are: **No prompts or code from Business users are retained or used for training** by default [73] [74], **public code filtering** to avoid suggesting licensed code [75], and **admin controls** like path exclusions and organization-wide policy enforcement. All of these are still in effect. In fact, GitHub emphasizes that Copilot for Business comes with **"no training on your code"** and enhanced privacy, exactly as the summary says [74].

The summary also notes the **choice of AI model** – specifically, organizations can disable "third-party" models and use only the GitHub-managed model. This refers to the setting where Copilot can be restricted to the older Codex model running on Microsoft Azure, rather than newer OpenAI models. GitHub still offers that option to customers concerned about data leaving Microsoft infrastructure [76].

On **data residency**: The guidance mentions that processing happens in EU and US Azure regions, and that you **cannot yet force UK-only processing** [77]. This is still true in 2025 – GitHub has EU and US datacenters for Copilot, but no dedicated UK region for Copilot's service. International data transfers are handled via the EU-US Data Privacy Framework and SCCs [78], which remains the legal mechanism in place.

The **telemetry and logging** behavior remains as described. The summary explains that Copilot Business only stores minimal telemetry (hashed identifiers, etc.) and discards source code and suggestions immediately after use [79]. Microsoft has not indicated any change here; this aligns with their SOC 2 report and privacy statement. The **operational logs** (7–30 day retention, never raw code) and the availability of usage stats via the API still hold [80]. No new auditing capabilities have been introduced publicly – detailed prompt logging is still not provided (by design, to avoid storing code). So the "no raw code in logs" and reliance on aggregated metrics remain accurate [80].

In terms of **compliance**, the guidance cites that Copilot (via GitHub platform) is covered by SOC 2, ISO 27001/27018, and CSA STAR certifications [81]. This is still the case – GitHub's platform compliance hasn't changed. It also correctly notes Copilot isn't yet approved for highly sensitive ("OFFICIAL-SENSITIVE") without further risk assessment [82], which is the same recommendation today given the service's cloud-based nature.

One small change: Microsoft rebranded the paid plan simply as "Copilot for Business" (removing the preview notion). The guidance already uses that name. Additionally, GitHub has been improving Copilot's **features** (e.g. adding a chat mode, Copilot voice, etc.), but these do not affect the privacy model or data handling. They all operate under the same safeguards described.

Assessment: Guidance Valid. The existing guidance for Copilot for Business is up-to-date. It accurately reflects the product's privacy features and enterprise controls. There are no new privacy concerns or data handling changes to incorporate. Organizations should continue to use Copilot for Business (not the free-tier Copilot) and leverage its settings like public-code filtering and **no training on prompts** [74]. The guidance's caution that it's *"not yet suitable for OFFICIAL-SENSITIVE without a risk assessment"* remains wise. In conclusion, the guidance remains valid – it may be worth emphasizing that these policies have been backed by Microsoft's SOC 2 audit and the new EU-US framework [78], but otherwise no changes are needed.

10. Google Gemini (and Bard/Workspace AI)

Discrepancies: The guidance provided for "Google Gemini" was forward-looking, and as of now (mid-2025) it still largely reflects Google's approach to AI in Workspace (which includes Bard and the upcoming Gemini models). The summary correctly differentiates between the **Free consumer AI (e.g. public Bard)** and the **Enterprise/Workspace AI**. Key points that remain true: **Free versions** of Google's AI (Bard) do log conversations for 18 months by default, can be used for model training, and may be reviewed by humans [83]. The guidance warns government users *not* to use the consumer/free version – this is still Google's own advice, as the free Bard is not suitable for sensitive data (it indeed uses conversations to improve the model unless you opt-out). Meanwhile, the **Enterprise version (part of Google Workspace)** does not use chats for training and provides stronger privacy with no human reviewers [84]. Google has confirmed this approach: enterprise Workspace AI interactions are kept private within the organization and not used to train Google's models [84].

The guidance notes that **Gemini** (Google's next-gen model) can be accessed via Workspace and that **client-side encryption isn't yet available** for it [85]. As of 2025, Google's generative AI in Workspace (often referred to as Duet AI rather than the model name "Gemini") still does **not support client-side encryption** – which is important for government data. The summary is accurate that while stored documents in Drive can be client-encrypted, the AI interactions cannot be, meaning data is decrypted on Google's servers to be processed [85]. This limitation remains.

One major update: Google's **data residency and region** options have expanded. The guidance says Google *"cannot guarantee data stays in UK/EU during processing"* [86] – this is still true for the generative AI processing, which uses Google's global infrastructure. However, Google has introduced **new admin controls** in Workspace: admins can now choose **Data Region** settings for some Workspace data at rest (EU or US). For generative AI specifically, Google announced it will *initially process queries in the United States*, but for Workspace customers in Europe, they are working on EU processing. This is a nuanced area; the summary's stance that data **"may leave UK jurisdiction during conversations"** remains valid [87].

The guidance about **audit logs** is slightly outdated only in the sense that Google is *expanding* what is logged. The summary mentions that currently only when Gemini (or Bard) accesses Drive files is it logged, and that future improvements will log Gmail interactions, etc. [88]. In 2025, Google announced more **Duet AI** log types (e.g. for Gmail assist), but these are indeed *in progress* just as the guidance anticipated [88]. Admins still rely on the Workspace audit log (Investigation Tool) to see AI file access events [89], which is unchanged. So no contradiction – just an ongoing development as noted.

Finally, compliance: The summary emphasizes **GDPR compliance** and the need to not input personal or sensitive data. Google has committed that Workspace's AI features are covered by the Workspace DPA (Data Processing Addendum) and meet GDPR obligations, which aligns with the guidance. It also highlights that **Enterprise use is approved with restrictions** (don't enter non-public data), which is exactly the current UK government stance. No new certifications specific to "Gemini" are to note, beyond Google Cloud's existing ISO27001, etc., which were already in place.

Assessment: Guidance Valid. The guidance remains on target. It effectively tells users to **avoid the free Bard/Gemini for any official data** and to use the **Enterprise/Workspace** edition with caution, which is precisely what Google and government policies advise. One minor enhancement when updating could be to mention that Google has introduced **data residency for some Workspace AI data** (for example, an EU data region setting for Workspace content at rest), though generative AI queries may still be processed globally [87]. Additionally, as Google's "Gemini" model rolls out (likely via the Duet AI in Workspace), the same rules apply as described. In summary, the guidance does not require changes – it already covers the necessary restrictions (no sensitive data, use Enterprise only, monitor audit logs) which remain the correct approach in 2025.

11. JetBrains AI Assistant (IntelliJ IDEs)

Discrepancies: The guidance for JetBrains AI Assistant is accurate and reflects JetBrains' current policies and the assistant's behavior. JetBrains has been very transparent about data collection: as the summary states, by default **all data sharing is opt-in** – meaning no code or prompt data is sent to JetBrains unless the user explicitly enables it [90] [91]. This remains true. JetBrains' own documentation confirms that if you do not opt in to "Detailed Data Collection," none of your code or chat content is kept by JetBrains or used to improve their models [91]. Only high-level usage metrics (feature usage counts, etc.) are collected by default, and even those exclude any source code and can be turned off in settings [92]. The guidance covers this, noting usage data (no code) and detailed data (with code/conversation) as two separate opt-ins [93]. This is unchanged.

The summary correctly points out that when using AI features, your code/questions **do get sent to third-party model providers** (OpenAI, Anthropic, etc.) for processing [94]. That is still how JetBrains AI works – it acts as a client that calls external APIs (OpenAI's GPT-4, etc.) on your behalf. Importantly, the guidance notes those providers have **zero-retention** policies for this data. OpenAI and Anthropic both offer zero-data-retention options for enterprise/API use, and JetBrains has configured its integration accordingly [95] [96]. As of 2025, OpenAI confirms that data via its API (which JetBrains uses) is not retained for training, and Anthropic offers a similar no-retention mode for partners [97] [98]. So the assurance that neither JetBrains nor the model providers will use your code to train models remains valid [99].

One update: JetBrains has introduced an **Enterprise plan** for AI Assistant, as the summary mentions, which allows things like custom model hosting and enterprise user management. This includes options like using

on-premises AI (via Ollama or LM Studio) or specifying model endpoints – the summary hints at that by mentioning "AI Enterprise… custom AI models" [100]. This is indeed a feature now: enterprises can connect the JetBrains assistant to models running under their control. The guidance already implies this and no contradiction exists.

The **data residency** portion of the summary is still relevant. JetBrains is EU-based (Czech Republic), and they route requests through EU servers when possible, but ultimately data goes to whichever cloud the AI provider is on [101]. For instance, an OpenAI request will reach the U.S., Anthropic's Claude is in the U.S., etc. The summary correctly notes **"data will often leave the UK/EU"** and that **Enterprise plan** could address this (e.g. by allowing self-hosted models or choosing providers with EU options) [102]. This remains the case – if a UK government wanted to avoid data leaving EU, they'd likely need the enterprise setup with a European model endpoint. The summary also mentions Google's Gemini might use EU datacenters – as of now, Gemini (Duet AI) isn't integrated into JetBrains yet, but if it is, Google's EU infrastructure could be leveraged. This point is speculative but not misleading.

Audit logging remains minimal, as stated: JetBrains AI does not provide detailed org-level logs of prompts/responses by default [103] [104]. The summary highlights that limitation and notes Enterprise might add logging features in future. This is still a limitation – currently, only ephemeral session history and basic usage metrics exist, which matches the guidance. JetBrains has acknowledged that for strict compliance, customers might require more logging, but those features are not yet productized (hence the guidance suggests Enterprise plan "may offer" enhanced logging) [105] [106].

Finally, **compliance**: The summary correctly notes JetBrains, being EU-based, adheres to GDPR and offers DPAs. JetBrains operates in ISO 27001-certified data centers and follows industry security practices [107]. These points hold true – JetBrains has a strong security reputation and their cloud services (like JetBrains Account) are ISO certified. Nothing contrary has surfaced.

Assessment: Guidance Valid. The JetBrains AI Assistant guidance is up-to-date and accurately describes the privacy controls (nearly all data collection is opt-in) and data flow (code goes to third-party LLMs under no-retention guarantees) [91] [96]. No changes are needed. Government users should continue to use the default "zero-retention mode" (i.e. not opt in to detailed logging) which ensures no code is stored on JetBrains servers [91]. They should also be aware that using the assistant will send code to external providers (OpenAI, etc.), and the guidance already advises reviewing that aspect. In summary, the guidance remains valid and is a good representation of JetBrains' current AI assistant policies.

12. Windsurf

Discrepancies: The guidance on Windsurf (an AI-powered IDE by Exafunction) is very detailed and mostly remains accurate, with one significant development: **corporate ownership changes**. In July 2025, Windsurf was acquired by another AI company (Cognition AI Inc.) [108] [109]. This does not immediately change the tool's features or policies – the interim CEO stated the Windsurf team will continue operating as before in the near term [110]. However, it's a notable update not in the original summary. Windsurf also signed a major partnership with Google in 2025 prior to the acquisition [111], which might bolster its European infrastructure and model access (the summary already notes a Frankfurt EU cluster and that Windsurf uses Anthropic Claude models – Anthropic had temporarily cut off Windsurf due to a rumored OpenAI bid, but post-acquisition, Claude access is restored) [112].

In terms of **privacy and data handling**, the guidance is up-to-date and extremely comprehensive. Windsurf's **zero-data-retention mode** is indeed the default for enterprise and is available to individuals as well [113]. The summary accurately says that in this mode, no code is stored on Windsurf servers at all – that remains true and is a core selling point of Windsurf (all processing in memory, no logging) [114]. It also notes that code will not be used to train models, which the company has promised and continues to uphold. The **feature controls** listed (disabling external model providers, controlling web access, etc.) reflect Windsurf's enterprise settings, which remain available [115].

The **deployment options** section in the guidance is a standout: it lists Standard cloud (US GCP), EU cluster (Frankfurt), FedRAMP High (AWS GovCloud IL5), Hybrid, and Self-hosted deployments [116] [117] [118]. All these options indeed exist. The summary is essentially current documentation – Windsurf offers EU hosting for Europe clients (and this Frankfurt cluster was in fact highlighted in early 2025 and remains in use) [119]. The FedRAMP environment for US government is also real (IL5 authorized, as noted) [117]. Hybrid and self-hosted modes are cutting-edge features Windsurf offered to let customers keep data on-premises; these are still part of their offering and nothing indicates otherwise. If anything, post-acquisition, these options will likely continue or fold into Cognition's product, but as of now they remain in effect.

Data protection measures are accurately described: TLS 1.2+ for all transit, end-to-end encryption for hybrid tunnels, etc. [120]. At rest, the summary notes that by default no code data is stored for enterprise (zero retention), and for individual users some logging could be enabled for those who opt in to service improvement (which is off by default) [121]. This still holds; Windsurf hasn't changed those defaults. The retention policies (prompt caches only for minutes, analytics metadata without code, abuse logs limited) are all still applicable [122].

For **auditing**, the summary rightly points out that **full audit logs (every AI suggestion, etc.) are only available in the hybrid/self-hosted scenarios**, not in the pure SaaS cloud deployment [123] [124]. This remains a limitation – cloud users get convenience but not on-prem audit trails, whereas self-hosted users can log everything internally. That trade-off is unchanged and is important for government considerations, as the guidance highlights. Windsurf's attribution logging (to detect open-source code matches) is also mentioned and is still a unique feature, stored locally when in self-hosted mode [125].

Access controls: The guidance covers SSO integration (SAML, OIDC), SCIM provisioning, and role-based team management [126] [127]. Windsurf does support SSO (Okta, Entra ID, etc.) and SCIM for enterprise, so that's correct. The hierarchical roles (team admins, group admins, etc.) are also as described in their enterprise offerings. No changes known there.

Compliance: The summary notes Windsurf aligns to GDPR, uses SCCs for transfers, and has FedRAMP IL5 for its GovCloud instance [128] [117]. It also mentions no UK-sovereign cloud (true, the UK users would likely use the EU cluster). These points remain valid. Windsurf as a private company wasn't separately certified on ISO, but it leverages compliance of its cloud providers (e.g. GCP's ISO 27001 data centers). The guidance doesn't list certifications except FedRAMP, which is fine.

Assessment: Guidance Valid (with note on acquisition). The Windsurf guidance is very up-to-date on technical and privacy aspects. The only external change is that Windsurf is now under new ownership (Cognition AI as of July 2025) [108]. So far this has not altered any privacy features or commitments – the new CEO explicitly reaffirmed continuity [110]. It might be worth monitoring in future if Windsurf's offerings merge with Cognition's, but as of now all the privacy controls (zero-retention mode, on-prem deploy, EU

hosting, etc.) remain available as described. Therefore, the guidance remains valid and thorough. Government users should continue to follow it: prefer **EU or self-hosted deployments** for data residency, use **zero-retention mode**, and leverage the hybrid/self-hosted options if audit logs are required. All these recommendations are exactly in line with Windsurf's current capabilities.

---

[1] [2] [3] [4] Analytics | aider
https://aider.chat/docs/more/analytics.html

[5] [6] AI for Software Development – Amazon Q Developer FAQs – AWS
https://aws.amazon.com/q/developer/faqs/

[7] 2025 ISO and CSA STAR certificates now available with four additional services | AWS Security Blog
https://aws.amazon.com/blogs/security/2025-iso-and-csa-star-certificates-now-available-with-four-additional-services/

[8] [9] [10] [11] Security Update for Amazon Q Developer Extension for Visual Studio Code (Version #1.84)
https://aws.amazon.com/security/security-bulletins/AWS-2025-015/

[12] The Wild West of AI Innovation | AI Consulting from Top-Tier Experts
https://neuronn.ai/the-wild-west-of-ai-innovation/

[13] Amazon Bedrock now available in the (London), (São Paulo), and Canada (Central) regions - AWS
https://aws.amazon.com/about-aws/whats-new/2024/06/amazon-bedrock-london-sao-paulo-canada-central-regions/

[14] [15] [16] aws-bedrock-summary.md
file://file-5YssVVT2Fv2Cx1Zh1E16VG

[17] [18] 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/

[19] [20] [21] azure-ai-foundry-summary.md
file://file-Wg9RuANQ3eC7giYiTdJZNY

[22] What is ChatGPT Team? - OpenAI Help Center
https://help.openai.com/en/articles/8792828-what-is-chatgpt-team

[23] [24] [25] [29] Introducing data residency in Europe | OpenAI
https://openai.com/index/introducing-data-residency-in-europe/

[26] [27] [28] [30] [31] [32] [33] chat-gpt-summary.md
file://file-LQ1RWRpUqJgaLCe8uevus9

[34] [35] [38] [44] [45] [46] claude-summary.md
file://file-K4FyUkw8AEJL5xJ8ACzSpu

[36] What Certifications has Anthropic obtained?
https://privacy.anthropic.com/en/articles/10015870-what-certifications-has-anthropic-obtained

[37] Approved for Use in FedRAMP High and DoD IL4/5 Workloads
https://www.anthropic.com/news/claude-in-amazon-bedrock-fedramp-high

[39] [40] [41] Where are your servers located? Do you host your models on EU servers? | Anthropic Privacy Center
https://privacy.anthropic.com/en/articles/7996890-where-are-your-servers-located-do-you-host-your-models-on-eu-servers

42 43 How long do you store my organization’s data? | Anthropic Privacy Center
https://privacy.anthropic.com/en/articles/7996866-how-long-do-you-store-my-organization-s-data

47 48 54 55 56 59 60 claude-code-summary.md
file://file-WpLLWxxeBohS8JHJ1UgFym

49 50 Security - Anthropic
https://docs.anthropic.com/en/docs/claude-code/security

51 52 53 Data usage - Anthropic
https://docs.anthropic.com/en/docs/claude-code/data-usage

57 58 API Console Roles and Permissions | Anthropic Help Center
https://support.anthropic.com/en/articles/10186004-api-console-roles-and-permissions

61 62 63 65 66 67 68 69 70 71 72 cursor-summary.md
file://file-V7FVb1HRSmoBNAZRwCyDKg

64 Cursor AI: Your 2024 Installation & Review Guide - HackerNoon
https://hackernoon.com/cursor-ai-your-2024-installation-and-review-guide

73 74 75 76 77 78 79 80 81 82 github-copilot-summary.md
file://file-Q3fT77SmLKn3htCeDvG3fC

83 84 85 86 87 88 89 google-gemini-summary.md
file://file-FwApFKSS2PxC6hX1UZUXzD

90 92 93 94 99 100 101 102 103 104 105 106 107 jetbrains-ai-assistant-intellij-summary.md
file://file-DCfRHKKraNi8g65xdi9GD9

91 95 96 97 98 Data retention | JetBrains AI Documentation
https://www.jetbrains.com/help/ai/data-retention.html

108 109 110 111 112 AI coding assistant startup Cognition acquires rival Windsurf - SiliconANGLE
https://siliconangle.com/2025/07/14/ai-coding-assistant-startup-cognition-acquires-rival-windsurf/

113 114 115 116 117 118 119 120 121 122 123 124 125 126 127 128 windsurf-summary.md
file://file-5QybJ6FhrK7T9A8fKxSPCs