

Manage Privacy and Data Requests

September 10, 2026

Manage Privacy and Data Requests

Use the Privacy area to review privacy-related information and respond consistently to organizational questions about data protection. This helps you provide approved, evidence-based answers without guessing or sharing unsupported details.

Overview

Privacy and data requests can include questions about how organizational information is protected, where security controls apply, and which data-protection topics are covered by your organization's published materials. In Atloria, you can begin from the **Security** area and select **Privacy** to access the privacy information available to your organization.

The Privacy experience is intended to support clear, grounded responses. Security and trust content distinguishes between **In-scope questions — grounded, cited (samples from the live run)** and **Out-of-scope questions — refused, not fabricated**. When you receive a request, use the available privacy and security information to answer only what is supported.

For broader data-protection questions, you may also need to review related security topics, such as  **Data Protection**, **Infrastructure Security Architecture**,  **Database Security**, or **Application Security & Access Control**. Use these areas to understand the context before responding to a requester.

 *Screenshot pending: The Security area showing the Privacy action used to open privacy information.*

Prerequisites

Before you begin, make sure you have:

- Access to the administrator security area.

- A clear copy of the privacy or data-related question you need to answer.
- Permission to view your organization's security and trust information.
- Any internal approval guidance required for responding to privacy requests.
- Enough context to determine whether the question is in scope for the available privacy and security materials.

Step-by-Step Instructions

1. Open the **Security** area in the administrator experience.
2. Select **Privacy** from the available security actions.
3. Review the privacy information presented on the Privacy screen.
4. Compare the requester's question with the available privacy information.
5. Check  **Data Protection** when the question concerns protection of organizational data.
6. Review **Infrastructure Security Architecture** when the question concerns the environment supporting organizational systems.
7. Select  **Database Security** when the request concerns database protections or database-related security.
8. Review **Application Security & Access Control** when the question concerns application access, permissions, or security controls.
9. Check  **Network Security** when the requester asks about network-level protections.
10. Review  **Kubernetes Security** when the question concerns container or Kubernetes security.
11. Use **In-scope questions — grounded, cited (samples from the live run)** as the standard for questions supported by the available materials.
12. Treat questions matching **Out-of-scope questions — refused, not fabricated** as unsupported by the available information.
13. Prepare a response using only information that is supported by the Privacy and Security & Trust content you reviewed.
14. Escalate the request through your organization's approved process when the requested information is not available or requires an authorized decision.

 *Screenshot pending: Privacy and security trust topics, including Data Protection, Database Security, and Application Security & Access Control.*

Tips and Best Practices

- **Answer only supported questions.** Follow the approach indicated by **In-scope questions** — **grounded, cited (samples from the live run)**. Use information that is available in the Privacy and Security areas rather than relying on assumptions.
- **Do not fabricate answers for unsupported requests.** If a request falls outside the available materials, follow the standard represented by **Out-of-scope questions** — **refused, not fabricated**. Explain that you cannot confirm the requested detail and use your organization's escalation process.
- **Match the topic to the right security area.** For example, use  **Data Protection** for data-protection questions,  **Database Security** for database questions, and **Application Security & Access Control** for questions about access controls.
- **Use the broad security context when needed.** A question may involve more than one topic. Review **Infrastructure Security Architecture**,  **Network Security**, and  **Kubernetes Security** when a requester needs a fuller explanation of the applicable security context.
- **Keep administrative settings separate from request responses.** Select **Manage in Settings** only when you need to manage settings. Do not change settings merely to answer a privacy question.
- **Use published information consistently.** Provide the same evidence-based answer for similar requests so that privacy communications remain reliable across your organization.

Related Pages

- [Review Security and Trust Findings](#)
- [Manage Data Protection Information](#)
- [Review Application Security and Access Control](#)
- [Review Database Security](#)
- [Manage Security Settings](#)
- [Manage Screenshots](#)

Troubleshooting

You cannot find the Privacy option

Return to the administrator **Security** area and look for the **Privacy** action. If it is not available, confirm that you have access to the security administration experience with your organization's administrator.

The request is not covered by the available privacy information

Do not create an answer from assumptions. Treat the request as out of scope, consistent with **Out-of-scope questions — refused, not fabricated**, and escalate it through your approved privacy, legal, security, or compliance process.

You are unsure which security topic applies

Start with  **Data Protection** for general data-related questions. Then review  **Database Security, Application Security & Access Control**,  **Network Security**, or **Infrastructure Security Architecture** based on the specific wording of the request.