BLOG POST

mimecast

Slack and GDPR: The Complete Guide

Everything you need to know to ensure compliance with GDPR regulations for Slack

AUGUST 13, 2026

Key Points

- While there are some exceptions for organizations with less than 250 employees, most organizations that communicate with customers in the EU are subject to GDPR regulations.
- Even for large organizations, retrieving the data necessary to meet GDPR compliance can be painstaking and costly, though automated tools like Mimecast Aware can help.
- Today's businesses are under constant pressure to ensure that their communication and collaboration tools comply with various data security regulations. One such crucial regulation is the General Data Protection Regulation (GDPR).
- In this comprehensive guide, we'll delve into the intricacies of Slack and GDPR compliance, answer whether Slack is GDPR compliant, and explore how you can support regulatory compliance in Slack.

Is Slack GDPR compliant?

Yes, Slack supports GDPR compliance. Slack has taken significant steps to align with GDPR requirements for data privacy and security, enabling GDPR-covered organizations to use Slack while meeting their obligations to handle personal data in a compliant manner.

What is GDPR?

The General Data Protection Regulation is a comprehensive data privacy regulation enacted by the European Union (EU) to provide individuals with more control over their personal data. GDPR was established to address the growing concerns about data breaches and the misuse of personal data, giving individuals the right to know, access, and delete their data. It also lays out strict rules for organizations handling personal data and enforces severe penalties for non-compliance.

Some of the world's biggest companies have fallen foul of GDPR and have been penalized for failing to secure user data. These include:

- Meta was fined $1.3 billion in 2023 for transferring EU users' data to the US.
- Amazon was fined $781 million for tracking user data without consent.
- WhatsApp was fined $193 million for failing to clearly inform users how their data was handled.
- Google was fined a combined $165 million for not giving users an easy way to refuse cookies.

Who does GDPR apply to?

GDPR is an EU law that safeguards the data of individuals residing in the European Union. However, it can be enforced against companies headquartered elsewhere in the world if they collect and manage that personal data or process it on behalf of others. Any company that offers goods and services within the EU, or monitors people's behavior within that area, must be GDPR compliant.

This is true even for small businesses, as GDPR applies regardless of company size. However, companies with fewer than 250 employees are exempt from some obligations, such as requiring a Data Protection Officer. GDPR does not apply to individuals engaged in "personal or domestic" activity, such as creating an email newsletter for friends and family. However, GDPR does apply to individuals engaged in more professional activities, even as a hobby, for example, running an email newsletter for fans of a popular TV show.

GDPR controllers vs. processors

In the context of GDPR, data controllers determine the purposes and means of data processing, while data processors act on behalf of controllers. Slack, for example, acts as a data processor when your organization uses its platform. Some companies may control their own data at all times and never use a processor, for example if your business builds and hosts its own internal communications tool. A processor always handles data on behalf of another organization.

Both controllers and processors have the same obligations under GDPR when it comes to handling data, but processors by definition also work under obligation to controllers. That makes it crucial to establish clear responsibilities and agreements between controllers and processors to ensure compliance. Often, these responsibilities are outlined using a data processing agreement. Slack offers a Data Processing Addendum (DPA) as a supplement to their Customer ToS. To be valid, the DPA must be executed by an individual authorized to sign on behalf of the controller organization.

Does GDPR apply to collaboration tools like Slack?

You might not think of collaboration tools as receptacles of personal data, but our research shows that many workplace communication platforms are packed with sensitive and confidential information. On average, PII can be found in 37% of all messages, and one in 17 contain at least three pieces of sensitive information. This risk proliferation makes it essential to consider tools like Slack when it comes to fulfilling GDPR obligations.

In addition to the PII risks Slack contains, the ability to exercise a customer or employee's right to be forgotten also applies to Slack data. Businesses need to proactively consider how they would identify, isolate, and purge Slack data from a single custodian within the timescales outlined by the GDPR.

Are employees covered by GDPR?

GDPR covers all data, including both customer and employee data. Employee data is subject to the same data protection standards as customer data. That means organizations must ensure they process their employees' data in a lawful and transparent manner. At any moment, an employee can file a subject data access request under Article 15 and have the same rights as any customer or client to view all the data the company holds on them within the one-month timescale outlined by Article 12.

Examples of GDPR risks in Slack

The GDPR gives individuals the right to access, review, correct, and remove data held about them by controllers or

processors. Businesses are required to comply with GDPR requests within specific timescales, which can be problematic for large organizations holding data in massive, unstructured datasets.

The average enterprise Slack user sends 28 messages per day, and over 90% of them are sent in private channels and DMs where even administrators may struggle to retain full visibility. The challenge of extracting this data in a timely fashion cannot be overstated, and this opens the organization to the risk of regulatory action.

- **Right of access (data subject access request):** An individual can request a copy of the personal data that an organization holds about them by filing a request known as a DSAR. This includes information about how the data is being processed, the purposes of processing, and who it is shared with. Time limit to comply: 1 month.
- **Right to rectification:** If an individual believes that the personal data held by an organization is inaccurate or incomplete, they can request the data controller to rectify or correct the data. Time limit to comply: 1 month.
- **Right to erasure (right to be forgotten):** Individuals have the right to request the deletion of their personal data if there are no legitimate reasons for the data controller to continue processing it. This right is not absolute and can be subject to certain exceptions. Time limit to comply: 1 month.
- **Right to data portability:** Individuals can request their personal data in a structured, commonly used, machine-readable format. They can also request that the data be transmitted directly to another data controller when technically feasible. This right allows individuals to move their data between different service providers easily. Time limit to comply: 1 month.

Five steps to make Slack is GDPR compliant

Slack supports GDPR compliance in its role as a data processor, but full compliance is a shared responsibility between Slack and its users (the controllers of the data Slack contains). Slack provides functionality and features that help users meet GDPR requirements, such as data export and deletion capabilities. However, organizations must also implement their policies and procedures to ensure GDPR compliance within their Slack workspace.

To make Slack GDPR compliant, organizations and compliance leaders should follow these five steps:

1. Review data usage: Understand what data employees share on Slack and ensure it aligns with GDPR principles.
2. Set data retention policies: Define how long to retain data on Slack and regularly review and delete data you no longer need. Consider using a data governance and compliance solution like Mimecast Aware to automate data retention and purging from Slack.
3. Educate users: Train your team on GDPR regulations and best practices for using Slack compliantly. All Slack users should be aware that their communications can be surfaced by subject access requests and be mindful of remaining professional despite Slack's informal communication style.
4. Use Slack's compliance features: Take advantage of Slack's built-in management tools for data export and profile deletion. These tools support searching Slack data and removing messages created by a single user (custodian) in compliance with GDPR. However, know that this tool will delete all user-generated content, and may include data the company may consider ownership of and wish to retain. Mimecast Aware's granular, bi-directional retention capabilities enable users to review custodian-generated content and assign value to it before deletion, preserving critical data.
5. Accelerate GDPR compliance with Mimecast Aware: Mimecast Aware supports GDPR compliance for Slack using purpose-built AI and natural language processing to enforce acceptable use policies within Slack. It can detect and remove unauthorized information — including PII, PHI, and company-sensitive data — using smart automated workflows, and implement granular, bi-directional retention policies to automatically purge

or preserve valuable data.

Other Slack compliance considerations

In addition to GDPR, organizations in highly regulated industries such as healthcare (HIPAA) or finance (FINRA) must adhere to specific compliance requirements when using Slack. And all organizations, whatever their industry, have a responsibility to protect personally identifiable information (PII) and payment card industry (PCI) data within Slack and comply with ISO 27001 and/or SOC 2 as best practice. Our research shows that when companies deploy collaboration platforms like Slack, employees use them as repositories for all company-related data unless they are given better alternatives.

How Mimecast Aware supports GDPR and compliance in Slack

Mimecast Aware supports GDPR-compliant data management with solutions designed to address organizations' obligations under:

- Article 5 — Principles relating to how organizations process personal data
- Article 12 — Transparent communication of the rights of the data subjects
- Article 15 — Right of access
- Article 17 — Right to erasure

Mimecast Aware connects to Slack via API to seamlessly ingest a complete record of all messages in Slack channels in real time with no IT lift and no impact on end users. Slack messages are then analyzed using Aware's proprietary, purpose-built natural language processing (NLP) and AI/ML models to automatically detect and mitigate unauthorized information sharing within Slack, including PII, PHI, PCI, and other sensitive data. Using Aware, compliance teams can mitigate risks across all collaboration tools — including Slack, Microsoft Teams, and Zoom — from a single, centralized platform that streamlines workflows, automates notifications, and effortlessly supports employee coaching and policy enforcement.

In addition to compliance functionality, the Aware data platform offers a suite of capabilities — including Signal for complete visibility and always-on protection, Search & Discover for fast and accurate investigations, Data Management for secure data lifecycle management, and Spotlight for emerging-risk detection — that support the holistic management of employee communications across the enterprise.

Recognized as a Leader in the 2025 Gartner® Magic Quadrant™ for Digital Communications Governance and Archiving, Mimecast helps more than 42,000 organizations keep ahead of the ever-evolving threat landscape.