grammarly business

Learn more about Grammarly's Information Security

Introduction

At Grammarly, we take our responsibility to protect your information seriously, because we know security is of the utmost importance to you, your business, and your customers. To this end, Grammarly uses a variety of measures to ensure that data is safe and secure. This document will explain what Grammarly does, what data we collect, and how we ensure security and privacy.

What is Grammarly?

Grammarly's mission is to improve lives by improving communication. Our AI-powered writing assistant helps 30 million people and 50,000 teams write more clearly and effectively every day by providing feedback on correctness, clarity, engagement, and delivery.

Grammarly makes money by offering best-in-class real-time writing suggestions to consumers and businesses, with both free and paid products. We do not—and will not—sell any users' data. We never provide information to third parties to help them advertise to end-users.

We comply with the EU's General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and the Health Insurance Portability and Accountability Act (HIPAA), by providing appropriate international data transfer mechanisms, as stated in our Privacy Policy.

What data is sent to and processed by Grammarly?

When users use Grammarly, Grammarly processes the following types of data:

User Text: Raw text that is written by a user and checked by Grammarly's writing assistant service.

Grammarly Account Information: Information provided by a user during the registration process, such as their username, email address, contact, and language preferences.

Log Data: Technical information about service use, such as server logs, browser type, and version, device information, and accept/ignore data on writing suggestions.

User Customization Data: Optional user and administrator inputs that customize the suggestions provided by the service, which operate at different levels. These inputs include additions to the personal dictionary at the individual user level and style guide entries at the team administration level.

Please refer to our Privacy Policy for more information.

How is data collected?

Data is collected through Grammarly's software clients, which include our browser extensions, desktop applications (Grammarly for Windows and Grammarly for Mac), a Microsoft Office add-in, a web-based editor, mobile keyboards, an iPad application and the Grammarly for Developers API. Grammarly products do not collect any data from sensitive fields, such as those requesting passwords or credit card information. Users can determine whether Grammarly is running on a particular text field on a site or application by looking for the Grammarly logo, a minimized Grammarly status dot or an icon showing the number of suggestions for their attention.

How is this data sent, processed, and stored?

All data is transferred to the United States for processing and storage using Amazon Web Services, one of the world's leading data center providers.

- Data in transit is protected by up-to-date encryption protocols (including SSL/TLS 1.2).
- Data at rest is encrypted using the industry-standard AES-256 algorithm.
- Passwords are encoded using the bcrypt algorithm.

What data does Grammarly store?

We will store documents created in the Grammarly Editor until they are deleted by the user, or upon request after contract termination or expiration.

For all other User Text processed by Grammarly (i.e., anything not saved in the Grammarly Editor): After Grammarly processes User Text, the text is disassociated from the account and deleted. Sampled, de-identified, and anonymized text may be retained to help us improve the algorithms underlying our software and services.

We may also keep some data for as long as reasonably necessary for our legitimate business interests, including fraud detection and prevention, and to comply with our legal obligations including tax, legal reporting, and auditing obligations.

What security certifications does Grammarly have?

Grammarly has completed and maintains a SOC 2 (Type 2) attestation. This examination, conducted by Ernst & Young, validates that Grammarly meets the strict SOC 2 standards for security, availability, confidentiality, and privacy of our customers' data.

Grammarly obtained a SOC 2 (Type 2) report in June 2021, which validates the strength of our security controls.

Grammarly has obtained ISO 27001, 27017 and 27018 Certifications. Read Grammarly's ISO 27001, 27017 and 27018 certificates.

Grammarly is HIPAA compliant and can sign a Business Associate Agreement. t

Grammarly is compliant with the Payment Card Industry's Data Security Standard, which validates that payments are handled with industry-standard security. Read Grammarly's attestation of PCI compliance.

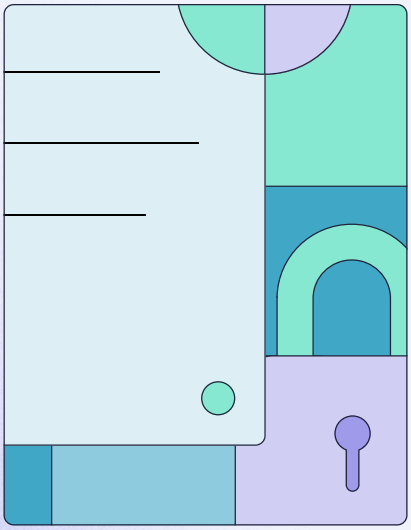
In addition, Grammarly is a member of the Cloud Security Alliance (CSA), a nonprofit dedicated to promoting secure cloud computing. Grammarly has completed CSA's Consensus Assessments Initiative Questionnaire (CAIQ), which details our security practices. Read Grammarly's CAIQ.

What does Grammarly do to protect against unauthorized developer and user access?

Grammarly supports multi-factor authentication (MFA) via SMS for access to our end-user products and developer console. End-users who are members of a Grammarly Business account are able to login to Grammarly through their identity provider if single sign-on (SSO) has been set up for their account. Any role-based access controls (owner/contributor/user) that have been set up by the administrators of their Grammarly Business account will also apply.

What does Grammarly do to control access to data?

Grammarly manages internal systems with single sign-on (SSO) and mandatory multi-factor authentication (MFA). Only company-managed devices can connect to the Grammarly corporate network. Grammarly adheres to the principle of least privilege—giving our employees only the access necessary to perform their work. Requests to access internal systems are documented and approved by the respective service owners and the Security team. Comprehensive access management is in place to ensure that access rights are provided based on business needs only and given the minimal privileges required. These access rights are subject to periodic review.



What does Grammarly do to train employees to follow security best practices?

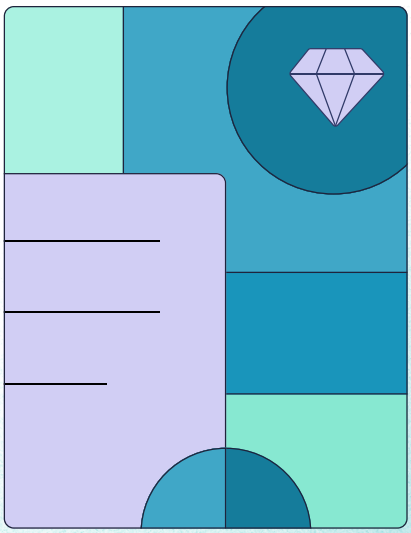
All new employees are required to complete online data security and privacy training. Any employees with access to user data need to complete additional training.

Our engineers need to follow our established Secure Development guidelines, and all changes undergo design and peer review before going to production.

What third-party audits and tests does Grammarly undergo?

In addition to the previously mentioned associations required for the above security attestations and certifications, Grammarly engages with a number of third-party reviews:

- We undergo annual internal audits of our services, penetration testing, and security reviews of our AWS environment.
- We use BitSight's vendor assessment system as part of a broader program to evaluate our security maturity as well as the security of our suppliers.
- Our technical security posture is assessed on the HackerOne platform on an ongoing basis.



What is Grammarly's incident management procedure?

Should we have a security incident, our documented incident management procedure establishes channels for the identification and communication of the incident to Grammarly's Security team. The Security team defines the type of event and its severity and then responds to it according to approved service-level agreements (SLAs) based on industry best practices. Grammarly's Legal team is consulted on all incidents to assess the necessity and manner of reporting and remediation. Security events that impact privacy are subject to additional analysis and response by Grammarly's Legal team.

We plan required mitigation actions for security incidents within the following timeframes, according to the defined level of severity:

- High: must be mitigated as soon as possible, within twelve hours
- Medium: must be mitigated within seven days
- Low: must be mitigated within fourteen days

Grammarly's incident management procedure can be found on Grammarly's Security Portal. You can obtain access to the portal through your Grammarly representative.

What is Grammarly's breach notification policy?

We will notify customers promptly upon becoming aware of a breach—where feasible, within 48 hours.

What subprocessors does Grammarly use and for what purposes?

Grammarly relies on a number of third-party vendors for specific services and functions. As part of our vendor approval process, we conduct multi-step security and privacy assessments, a detailed review of their compliance posture, and an in-depth legal review of their data practices. Grammarly repeats this due diligence regularly.

Where can I obtain further documentation about Grammarly Information Security?

More information can be found on Grammarly's security page.

You can access Grammarly's Information Security Documentation through the online Grammarly Security Portal. Please contact your Grammarly Representative to obtain access.