Vendor Report

Vendor Report for Grammarly, Inc.

This report is based on publicly available information and does not consider artefacts such as external assurance reports or contract terms that may only be provided to clients. Refer to the References slide for a list of resources used to generate this report.

June 2024

Grammarly, Inc. – Vendor Summary

Launched in 2009, Grammarly is a digital writing assistant that utilises advanced AI techniques to help users improve their written communication across various platforms and applications. It assists users in identifying grammatical errors, improving sentence structure, and suggesting style improvements. Key features include grammar checking, spell checking, plagiarism detection, and suggestions for vocabulary enhancements, making it a helpful tool for writers, students, and professionals.

Grammarly offers a free version with basic writing corrections, while Premium, Business, and Enterprise subscriptions provide advanced features, enhanced security options, and premium customer support. Subscription plans are designed to cater to individual users, educational institutions, and businesses, offering flexible options that fit various needs and budgets.

Grammarly provides Terms of Service for all users and requires Business/Enterprise Plan subscribers to sign a Customer Business Agreement.

The Trust section of Grammarly's website details:

- Security measures and data protection practices to safeguard user data.
- Compliance with globally recognised security standards, privacy laws and regulations.
- Privacy practices to ensure user data remains private and secure across all platforms.
- Artificial Intelligence (AI) developed and deployed principles.

Grammarly Inc. – Key Risk Drivers

- Although Grammarly promises not to process sensitive information and its applications are designed not to run in sensitive fields (like credit card forms, passwords, and URLs), there are still some risks. If users enter personal information or other sensitive data in non-sensitive fields, this data may still be processed by Grammarly, potentially leading to privacy breaches.
- The Grammarly Office add-in and browser extensions have comprehensive access to view and process everything users write in their documents and on the web. This access raises concerns about inadvertently processing or exposing sensitive information. The 2018 security breach involving Grammarly's authentication tokens for browser extensions is a perfect example. Though it was resolved quickly, it highlighted the vulnerability of such tools to unauthorised access.
- Grammarly's privacy policy allows the sharing of user data with third-party service providers to maintain its product. This practice raises potential privacy and security concerns, as it depends on the third parties' adherence to data protection laws and their security measures, which directly affect the safety of user data.
- Grammarly's algorithms might unintentionally create or modify content that infringes on copyright laws or misappropriates intellectual property, leading to serious legal consequences for users, including potential lawsuits and damage to their professional reputation.
- Grammarly's AI algorithms may occasionally produce inaccuracies in suggestions, potentially leading to user dissatisfaction if the context is misunderstood or incorrect corrections are made.

Grammarly Inc. – Key Risk Drivers

- Grammarly utilises user-generated content to train its AI, posing potential privacy and compliance risks despite anonymisation efforts. While business account administrators can opt out of data usage for AI training and product improvement, individual users lack this option, intensifying concerns over involuntary data use and potential privacy breaches.
- Users heavily integrated into Grammarly's ecosystem might find it challenging to switch to other tools, which could create a dependency and reduce flexibility in their operations.
- Information submitted to Grammarly will be stored in the United States but due to Grammarly's global operations, will be also be accessed from other countries around the world. Hence, information will be subject to varying levels of data protection regulations and jurisdictions. Data breaches, unauthorised access, or data loss are risks, along with the dependence on internet connectivity.
- The global operations of Grammarly require compliance with numerous international data protection laws, such as the EU's GDPR and California's CCPA. This complexity may increase users' legal compliance, data security, and privacy protection challenges, including assessing complex regulations in various jurisdictions.

Vendor Due Diligence Review – Security & Privacy Facts

Security and Compliance

- Grammarly Inc. has the following external assurance artefacts: ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018 (2019), SOC 2 Type II and SOC 3, PCI DSS.
- Grammarly's GRC team maintains essential business and security-related documents through the Policy Central platform, including security risk assessments, information classification, vendor, access and change management.
- Policies require approval from the Information Security System Manager (ISMS Manager) and relevant functional heads. These policies are reviewed annually or whenever significant changes occur.
- Policies become effective upon publication on the Policy Central portal and are announced in the relevant corporate Slack channel. These policies are accessible to all employees starting from their onboarding.
- Grammarly has a company-wide Security Champions program, where specialists are integrated within each engineering team to scale security measures across product offerings, overseeing security decisions and communicating potential concerns.

Vendor Due Diligence Review – Security & Privacy Facts

Infrastructure and Risk Management

- All Grammarly server infrastructure is hosted in Amazon Web Services (“AWS”) data centres located in the United States in the US East region (North Virginia).
- The Trust Leadership team reviews security objectives, risk assessments, audit outcomes, vulnerabilities, and incidents quarterly.
- Grammarly has a public bug bounty program on HackerOne.
- Grammarly uses a vulnerability management program to identify and resolve vulnerabilities and undergoes third-party network penetration tests.
- Grammarly also conducts periodic independent audits as part of a formal program to evaluate the effectiveness of security in its processes, infrastructure, and products, with the Trust Leadership team overseeing audit results and corrective actions to enhance security.
- Sub-processors are listed on the website. They are required to process personal data following the provisions of the Grammarly Data Privacy Addendum (DPA) and Data Privacy Laws.
- Grammarly established a vendor management program that includes onboarding new vendors, regularly reviewing existing ones, and managing their offboarding to handle risks associated with third-party services.

Vendor Due Diligence Review – Security & Privacy Facts

Data Management and Privacy

- Grammarly hosts data in Amazon Web Services data centres in United States and notes to ensure continual product availability using native backup tools.
- The Privacy Policy outlines how Grammarly collects, uses, protects, and shares personal data as a data controller. It also notes that the company acts as a data processor under organisational instructions when serving business or educational team accounts.
- Grammarly may use personal data to improve its products, personalise user experience, offer customer support, troubleshoot and debug issues, enhance security, and comply with legal obligations, as per the Privacy Policy. Users are in control of whether their text data is used to train and improve Grammarly's models.
- The Data Privacy Addendum (DPA) details how Grammarly protects and processes personal data on behalf of its customers, specifically when acting as a data processor.
- Grammarly may share user information with certain third parties to provide, build, protect, improve, and promote their products or as required by law.
- Users retain all rights to user's content, including copyrights and duplication privileges.

Vendor Due Diligence Review – Security & Privacy Facts

Data Management and Privacy

- Users have several ways to interact with their personal information processed by Grammarly, including requesting a record of their information, updating or correcting it, and deleting it.
- Grammarly will return or securely destroy all personal data at the user's written request upon termination or expiration of the agreement, unless required to retain it by law or if the data is stored in backup systems, in which case Grammarly will securely isolate and ultimately delete the data following its deletion policies.
- Grammarly must adhere to GDPR, CCPA, HIPAA, Data Privacy Framework (DFS) and other privacy regulations.

Data Encryption

- Encryption in transit uses TLS 1.2, and encryption at rest in AWS uses AES-256 server-side encryption.
- Passwords are stored in an encrypted databases with applied bcrypt hashing.
- AWS Key Management Services ("KMS") is used for database encryption and key management. Access to the cryptographic keys is restricted to authorised personnel.

Vendor Due Diligence Review – Security & Privacy Facts

Operational and Network Security

- All components that process user data operate in Grammarly's private network inside Grammarly's secure cloud platform, and each user's data is isolated from other users' data.
- Grammarly's servers and network ports are behind load balancers and a web application firewall.
- Grammarly authenticates internal and external users of Grammarly by login/password, single sign-on ("SSO") via SAML or social sign-on with Google or Facebook.
- The Security page notes that Grammarly adheres to the principle of least privilege and that employees' data access rights are regularly reviewed to ensure only minimum required privileges are granted.
- Workstations run on centrally controlled endpoint-management software that enforces security configurations and protection solutions.

Artificial Intelligence (AI) and Ethical Guidelines

- Users are solely responsible for using Grammarly's generative AI features and the content that is generated.
- Grammarly's AI methods utilise user content to provide writing suggestions. For business accounts, administrators can opt out of allowing their data to be used for AI training and product improvement.
- Grammarly notes that they filter generative AI and natural language suggestions to address issues, such as hate speech, should they arise.

References

https://www.grammarly.com/trust

https://www.grammarly.com/privacy-policy

https://www.grammarly.com/terms

https://www.grammarly.com/security

https://www.grammarly.com/terms/Grammarly-DPA.pdf

https://www.grammarly.com/terms/customer-business-agreement

https://www.grammarly.com/blog/security-champions/

https://support.grammarly.com/hc/en-us/articles/360036884632-Does-Grammarly-use-subprocessors

https://assets.ctfassets.net/1e6ajr2k4140/6aciUJi2rkM8d64mUChpoR/a74a36043e4e305e3f0aa30455e89e2f/Grammarly_SOC_3_Report_FY23.pdf

NEED A DETAILED RISK ASSESSMENT OR VENDOR REVIEW?

GET IN TOUCH

Katja Feldtmann

0800 029 237

katja@cybershore.co.nz

www.cybershore.co.nz

Cybershore provides information for general purposes only. We are not liable for any potential risks associated with the use of this information, as the risks mentioned are presented as examples out of context.