

Replo's Commitment to Data Privacy and Security

We understand that the privacy and security of your data are of utmost importance, especially when it comes to sensitive information such as investor update documents. At Replo, we are committed to maintaining the highest standards of data protection and transparency. This document outlines our measures to ensure your data's safety and privacy.

Terminology:

1. **User:** In the context of Replo, a user refers to a company member responsible for drafting an update document or the individual reading it. Users have personal accounts on our platform, where they can create, store, and share their update documents securely.
2. **Update Document:** An update document is a report, typically in a "newsletter" format, used to inform a company's investors about the current state of the company. It may contain information about recent achievements, financial performance, upcoming projects, and other relevant news.
3. **Update Document Summary:** The update document summary is a condensed version of the update document, usually consisting of short bullet points that capture the document's most important takeaways. This summary is generated by an AI, allowing investors to quickly grasp the main points of the document without having to read it in its entirety.

Data handling:

1. **Data Storage and Hosting:** Our platform is hosted on Google Cloud Platform (GCP) servers located in Europe.
2. **Document Creation and Storage:** When you draft an investor update document using our platform, it is stored securely in our SQL database. We implement strict security measures to ensure the protection of your data.
3. **Document Summarization:** To provide a summarized version of your documents to investors, we utilize LLM based solution for summarization. The European-based AI solution that Replo is utilizing, is compliant with basic data protection regulations, ensuring a secure summarization process. The summarized version is then stored securely in our database.
4. **Access Control:** The owner of the update document maintains complete control over who can view the complete update document. We have robust access control

measures in place to ensure that your data is accessible only to authorized individuals.

5. **Data Deletion:** You can delete your document at any time. Once deleted, the data is permanently removed from our systems.
6. **Authentication:** We use Clerk as our authentication provider, which is GDPR compliant. This ensures that your personal data is handled in accordance with the highest privacy standards.
7. **Personal Data:** The personal information we store is limited to your email, name, and profile picture. This data is used exclusively within our platform to provide our services.
8. **Data Analysis:** At Replo, we **ONLY** analyze data quantitatively. This means we do not perform any content analysis on your documents. While we may use data to enhance our services, we respect your privacy and do not scrutinize the specifics of your document content.

At Replo, we strive to collaborate with European-based services to ensure the highest standards of data protection and privacy for our users.

We hope this information provides you with peace of mind regarding the safety and privacy of your data on Replo. If you have any further questions or concerns, please do not hesitate to contact us via email hey@replo.io.

// Replo team