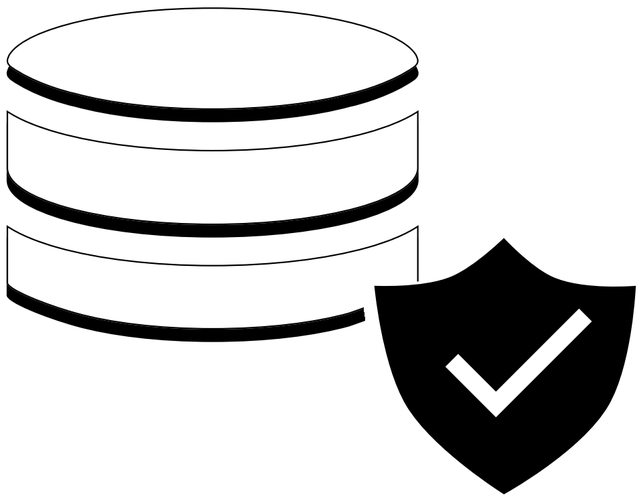
INFO PACK

AI and data security with Briink

Briink Intelligence GmbH / Max-Urich-Straße 3, 13355 Berlin / info@briink.com

We take data security seriously.



As an AI-first provider, we strongly believe that we have the moral and societal duty to treat our user data ethically and responsibly, and to uphold to the highest standards of model security and data privacy.

We additionally offer multiple options to ensure our customers can benefit from our AI tools, while keeping their data secure.

> “Data security is a top priority issue for Briink and an integral part of being a sustainable company in every sense”
>
> Samuel King
> CTO and Co-founder of Briink

Briink is **SOC2 Attested**, as verified by a third-party auditor, and as an EU-based company we are subject to compliance with the European privacy regulation such as the GDPR and the German Bundesdatenschutzgesetz.

You can **read our real-time monitored SOC2 report here.**

Briink Intelligence GmbH / Max-Urich-Straße 3, 13355 Berlin / info@briink.com

AI and data security: our approach

Continous security monitoring

We work with industry leading security partners like Drata to perform **continuous monitoring** of our data and system security. Learn more on our security page.

Data encryption

As part of the SOC2 we provide **full end-to-end encryption** in transit and encryption at rest as default of all client data within the Briink production system using TLS v1.2 or above. We also provide object-level permission, logically separate data and identify authentication to enforce that data can only be accessed by the correct user. We additionally use best practices for infrastructure security, and we leverage Google Cloud Platform's built in security features.

Identity verification

Briink uses Auth0 as our **identity provider** to further harden our protection of user management data, which includes best-in-class security features for authorization (such as SSO, MFA, attack-protection, enforced password policies, account access monitoring).

Vulnerability scanning and development practices

We ensure the code base deployed on our infrastructure minimizes security risks by following a robust process for software development and code review with enforced branch policies. **Automated vulnerability scans** are also run on our entire codebase as well as deployed containers to identify vulnerabilities and mitigate these before deployment. Full system vulnerability scanning is also conducted on a regular basis.

Team culture and employee training

Our data security posture **starts with our own team and culture.** We ensure employees local environments are secure (with antiviruses, hard drive encryption, password managers and security training etc.) and that we maintain high standards for physical (e.g. locked assets and workstations) and digital security (e.g. password policies).

Frequently Asked Questions (FAQs)

IS MY DATA USED FOR MODEL TRAINING?

Briink develops AI models optimised to recognize, interpret and identify a great variety of user-generated ESG and Sustainability KPIs with superior accuracy compared to baseline large language models. The main source of data for model fine-tuning is actually our own proprietary datasets that we have collected and curated to ensure high quality ground truth data that results in optimal model performance for ESG tasks. However we do have the ability to further fine-tune models using **free user tier data** to further boost performance where appropriate.

For paying customers (Growth and Enterprise) we do offer specific mechanisms to ensure that your data **is not included** in these model fine-tuning pipelines, unless explicitly agreed to.

HOW DO YOUR ENSURE THAT CLIENT DATA IS NOT USED FOR FINE-TUNING?

Clients document data is kept is a separate, isolated and fully encrypted object store buckets per user housed in our production environment. All buckets by default have permissions turned-off for fine-tuning and are encrypted so that they cannot be accessed even by Briink's own employees (outside of maintenance and assurance purposes). Any data used for fine-tuning our models must be explicitly white-listed first in accordance with the contractual agreement of the owner of such data.

Further, ESG queries can only be used for training if they can also be linked to a object store bucket which is also specifically white-listed for fine-tuning.

DO YOU SHARE DATA WITH THIRD-PARTY MODEL PROVIDERS (E.G. OPENAI)?

Briink uses both open source (self-hosted) and closed source foundational models from reputable 3rd party providers like OpenAI (GPT-3.5 and GPT-4) to ensure we can deliver the best results to our users. The OpenAI API system is SOC 2 compliant and our API contract with them guarantees they "**do not use API data, inputs or outputs for training our models**".

There are further guarantees that any data sent through the API is "**securely retained for a maximum of 30 days only to identify abuse [and then permanently deleted]**". Furthermore it is also possible for our enterprise clients to request zero data retention (ZDR) if necessary.

HAVE MORE QUESTIONS ABOUT DATA SECURITY?

Get in touch directly at security@briink.com, or ask your account manager! We are always happy to provide more information about our data security standards and policies.