



Data safety at UXprobe

Table of contents



Executive summary	3
1. Google App Engine	4
2. Security at Google	4
2.1. Data Access and identity	4
2.2. Storage	4
Highly protected data centres	4
Custom machines	4
Security of data	4
2.3. Security	5
High availability	5
Secure connection	5
Data ownership	5
3. Compliance	5
3.1. Standards Compliance of the App Engine Platform	5
3.2. European Compliance of the App Engine platform	6
Conclusion	6



Executive summary

At UXprobe, the security and integrity of your data, your customers' experience data, is critically important to us. It is because of this that we have built and operate UXprobe in a highly secure environment with industry's best practices to secure and guard data privacy and integrity.

UXprobe operates its service in world leading secure data centers, which are managed and operated under highly secure and audited processes. The security of the UXprobe platform begins with highly secure physical premises and continues up through it's security of the base hardware, operating systems, system software, and application software including best practices such as two factor authentication for access to UXprobe reporting.



Pic 1. Google App Engine

the **highest** industry standards and **support leading** practices

1. Google App Engine

The UXprobe service (SaaS) runs on the Google App engine platform which is hosted and managed by Google.

SEE PIC 1.

All customer data is stored and secured on this platform. This allows UXprobe to take advantage of all physical and logical security elements enjoyed by Google.

The data we collect are physically stored within Google's own data centres and enjoy the high level of security Google applies to all of its operations.

2. Security at Google

2.1. Data Access and identity

Access to UXprobe reports are through Google accounts which are guarded by the highest industry standards and support leading practices such as two factor authentication.

2.2. Storage

All data is stored within the Google infrastructure and so the same levels of security that apply to all of Google's data also applies to UXprobe.

Highly protected data centres

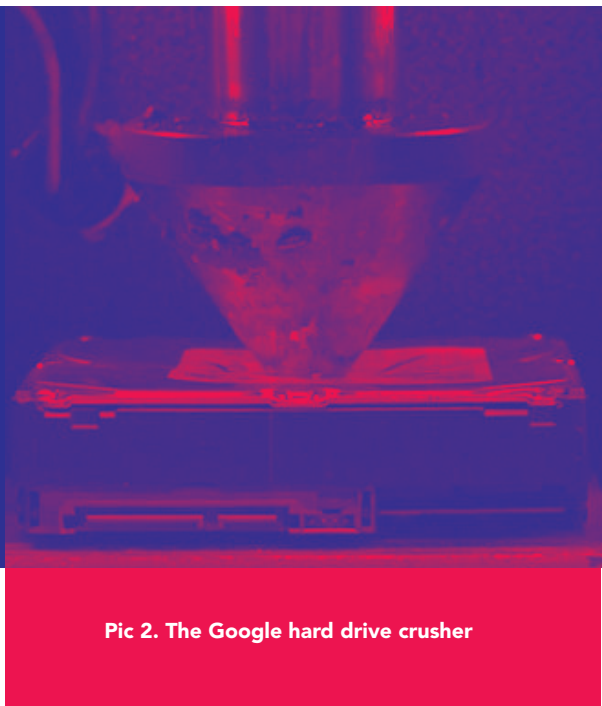
Restricted physical access, escalating level of security when approaching the core of the data centre, different types of security technologies used for each level (badges, secure chamber, biometric identification, etc.), security guards on site 24/7, video cameras with threat detection, etc

Custom machines

Hardware and Operating system are designed and built by and for Google, making the computing environment less prone to vulnerability and zero day threats.

Security of data

- **Data randomization.**
Data of the same company is stored in multiple locations to help ensure reliability. The files which store the data are given random file names and are not stored in clear text, so they're not humanly readable.
- **Strict process around hard drive life cycle management.**
Hard drives are constantly tracked for location and status. When one fails or begins to show performance problems, it's brought to a specific area where it's reformatted.



Pic 2. The Google hard drive crusher

Data collected by UXprobe on behalf of clients remains the property of our clients

If it's not proven 100% working, it's removed and overwritten, then destroyed. First with the crusher, then through a shredder. **SEE PIC 2.**

- **All data is backed up** to tape archives

2.3. Security

High availability

UXprobe runs on the Google App Engine and utilises High replication Datastores (HDR). This provides high availability for all reads and writes by storing data synchronously in multiple data centres.

Secure connection

UXprobe uses HTTPS to provide secure connection between the UXprobe system and the customer application system. Data transmitted to UXprobe is protected end to end by TLS encryption.

Data ownership

Data collected by UXprobe on behalf of clients remains the property of our clients - we never use our clients data for any other purposes, than feeding our clients own reports. It is and remains your property.

3. Compliance

3.1. Standards Compliance of the App Engine Platform

The Google App Engine platform and environment is subject to independent verification of security, privacy and compliance controls. Google undergoes several independent third party audits on a regular basis to provide this assurance. This means that an independent auditor has examined the controls present in our data centers, infrastructure and operations. Google solutions have regular audits for the following standards:

- **(SOC1) (SSAE-16/ISAE-3402):** Google Apps , Google Compute Engine, Google Cloud Storage, Google App Engine
- **(SOC2):** Google Apps , Google Compute Engine, Google Cloud Storage, Google App Engine
- **(SOC3):** Google Apps , Google Compute Engine, Google Cloud Storage, Google App Engine
- **ISO27001:** Google Apps , Google Compute Engine, Google Cloud Storage, Google Application Engine, Google DataStore, Google Big Query, Google CCloud SQL
- **HIPAA:** Google Apps , Google Compute Engine, Google Cloud Storage, Google Big Query, Google Cloud SQL



security and integrity of your customers' experience data

- FISMA: Google App Engine, Google Apps for Government

3.2. European Compliance of the App Engine platform

Google provides capabilities and contractual commitments created to meet data protection recommendations provided by the Article 29 Working Party. Google offers to sign EU Model Contract Clauses and a Data Processing Amendment. It is a participant in the U.S.-EU Safe Harbor Framework. Along with independent third-party audits of our data protection practices and our ISO 27001 certification, these provide our customers with several compliance options to address EU data protection regulations

Conclusion

At UXprobe, the security and integrity of your customers' experience data, is critically important to us. It is because of this that we have built and operate UXprobe in a highly secure environment with industry's best practices to secure and guard data privacy and integrity.

We welcome feedback and input of how to improve the security and integrity of UXprobe. Please do not hesitate to share your requirements with us at happy@uxpro.be

Call us +32 (0)485 71 48 36 or +32 (0)485 69 78 35 **Send us an email** happy@uxpro.be
Check our Website www.uxpro.be **Watch our video** <http://youtu.be/xRYuRvhlWVQ>
Follow us on Twitter @uxprobe **Facebook** Look for UXprobe **Google+** Look for UXprobe