Public Security Declaration

Our Public Security Declaration

About our security

If you’ve come to Safe Online, it’s because you care about keeping your customers’ data safe and private. Would you like to know a little about how we keep data safe when you use our products?

We’ve prepared this public security statement as a companion to our privacy policy (https://bysafeonline.com/safe-online-cookie-and-privacy-policy/) to outline our security and data protection standards and practices.

Our secure data storage

Here are a few highlights about our data storage:

- We log all access to your files
- We frequently back up documents and data
- We use the latest encryption standards both when transferring and storing your documents, including backup
- Only 2 developers in Denmark have access to user data and their access is restricted with MFA and location access.
- We guarantee that your data will not leave the EU
- We monitor and keep all servers up to date with the latest OS and security patches
- Any access to user data requires the minimum consent of at least 2 people from your company before we can access your data.

Our ethical AI

As AI becomes more and more widely used, questions about its ethics arise. Indeed, anytime you use AI, you should ask if it is ethical and use it responsibly.

Ethical AI should adhere to well-defined ethical guidelines and protect fundamental values, including:

- Individual rights
- Privacy
- Non-discrimination
- Non-manipulation

DataMapper's AI does not create ethical concerns, for the following reasons:

- DataMapper uses AI to quickly detect and classify the personal data you already store in your systems. It does not collect additional data from your customers in any way.
- You decide who to invite to DataMapper, and what access they will have to the information gathered. You can give a user access to only their own data storage (regular user); or give them access to data and statistics for the whole company.
- Once DataMapper's AI finds sensitive data and shows it to you, it is up to you to decide what to do with it. DataMapper's AI cannot be used for automated decision making and it does not alter or manipulate the data in any way.

Access control

Our products were designed to help you manage your own company's personal data. Our developers can access your data if you need them to, but only with two written consents.

More security details

Here are some more details about our security:

Users control access

Each user chooses which files DataMapper can access and retains full control to manage data access over time.

Users are authenticated

The verified creator of an account is given admin status and is the only one who can invite users to that team and the only one who can view a complete dashboard of all results. Users are identified by an administrator's invite and a dedicated sign-up flow ensuring each user is verified.

Password and access tokens

Password and access tokens are signed with a shared secret signature key and the password is hashed with sha256_cryp.t. Every access to your data is securely logged.

Network and access

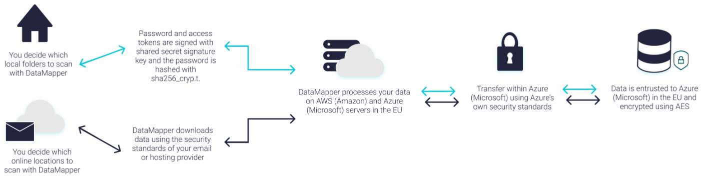
All communication between your computer and our servers is encrypted using 2048-bit RSA encryption. To prevent man-in-the-middle attacks, all our servers are certified with X.509 certificates provided by WebTrust certified certificate authorities. Finally, all your data is hosted on trusted third-party services (e.g., Azure) that use state-of-the-art access control and operate server facilities that are physically guarded.

Data encrypted in transit

HTTPS in transit, TLS 1.2, Shared access signature

Data encrypted at rest

Azure private blob storage encrypted at rest with Azure managed AES 256 bit keys


You decide which local folders to scan with DataMapper
Password and access tokens are signed with shared secret signature key and the password is hashed with sha256_cryp.t.
You decide which online locations to scan with DataMapper
DataMapper downloads data using the security standards of your email or hosting provider
DataMapper processes your data on AWS (Amazon) and Azure (Microsoft) servers in the EU
Transfer within Azure (Microsoft) using Azure's own security standards
Data is entrusted to Azure (Microsoft) in the EU and encrypted using AES

Key security questions, answered

The Danish Government's Agency on Digitization has set out a series of questions to determine if companies really keep data safe. These questions can be a good basis for you to decide if you trust a company with your data. Here are our answers:

1. Where is Safe Online's data storage physically located?

Microsoft Azure in Amsterdam, Holland. We and Microsoft guarantee that the data will not be moved to servers located outside of EU.

2. How and where are backups made?

We continuously do automatic backups of our database. A full backup is done weekly, another backup is done twice daily, and we do a backup of the transaction log every 5 minutes.

An automatic security copy of all users' data is done to guard against system errors. This copy is deleted together with the primary data if the customer relationship ends.

All backup data is encrypted with AES 256-bit encryption.

3. What is the process for updates and changes to IT systems and programs?

We update the system continuously as new features are added. We always try to update when user activity is at its lowest, so our customers experience the least possible downtime.

4. How does Safe Online control user access and privileges for IT systems?

There is, as a rule, no access to the production systems. However, for technical reasons or for troubleshooting, access may occur if the administrator gives access to the technical manager. All traffic and changes that may occur during this period will be logged.

When an end-user has purchased access to the system, the user gets a unique login that can only be used by that user. This data is saved so we are able to reset the user's login ID and password. Only our IT support team can access to this data and they will only access it at the request of the user.

5. How does Safe Online ensure the security of data networks?

Our network is segmented and protected by a firewall. All machines in the same segment only have access to each other through defined ports.

6. What is Safe Online's IT emergency plan?

In the event of a security breach and/or a third party's unauthorized access to our data we have the following in place:

1. Data Breach Procedures
2. Data Breach Notification Procedures
3. Data Breach Log

Firstly, all identified security breaches or unauthorized access to data are communicated to our data protection officer. He will make an initial assessment based on the severity of the breach and the data involved, to define which measures should be taken. He will make the assessment based on the likelihood of the breach resulting in a risk for the persons involved. Here are some examples:

1. If you lose your work computer but it is password protected, it is probably unlikely to pose a big risk. However, this depends of what kind of data you have how much, where you lost it etc.
2. If your organization is hacked and all your data is stolen, there is no doubt you must inform the competent supervisory authority as well as the people involved.
3. If you have a break-in at the office and your hard drives with sensitive data are stolen, there is no doubt you must inform the competent supervisory authority unless everything is thoroughly encrypted and doesn't pose a risk for the involved.

All breaches will be logged, no matter the severity, but it is up to the data protection officer to assess which measures should be taken after a breach has been identified.

7. Does Safe Online regularly test the IT security within the company?

Our servers are protected by Microsoft Azure's Integrated Security Solutions and other anti-fraud and-malware services.

To help ensure our solution detects the latest threats, we have enabled automatic updates.

8. How does Safe Online handle personal data and ensure the confidentiality of the personal data you process for us?

At Safe Online, we are dedicated to protecting all the personal data of our employees as well as our customers, business partners; and anyone else whose data we may be storing or processing.

We have in place policies and procedures on both internal processing of personal data for each specific area such as customer data, job applications, marketing tools, etc. along with an overall data protection policy that outlines how we are handling personal data in a secure and orderly manner.

Do you have more questions about our security?

Please read our privacy policy (https://bysafeonline.com/safe-online-cookie-and-privacy-policy/) for more information on exactly what data we collect and why, how long we keep it, and more.

If you still have questions about our privacy and security, feel free to get in touch with us using the information below.

22 Købmagergade

1150 Copenhagen K

Denmark

Phone: + 45 27772737

E-mail: sal@safeonline.dk (mailto:sal@safeonline.dk)

CVR no: DK38589962

✉ Still need help? Contact Us (#)

Last updated on December 8, 2022