Last review: 2018/07/11

- The Prezi Security Manifesto
- An overview of security at Prezi
    - Prezi's Security Program
        - Does Prezi have a dedicated security team?
        - Does Prezi have written Information Security Policies?
        - Does Prezi have an incident response program?
        - Are managers engaged in driving security within the business?
        - Does Prezi have an accredited third-party perform security audits of the security program?
        - Does Prezi have a vulnerability management program and perform vulnerability scans on a regular basis? Does the application undergo regular penetration tests?
        - Does Prezi have regular vulnerability assessments from independent third parties?
        - Can you share the results of your latest penetration test and the status & mitigation plan for the open issues?
        - Do you maintain a patch management process?
        - What networking security measures do you have in place?
        - Does the QA process also address common application vulnerabilities as defined by OWASP or SANS? Does Prezi perform internal security code reviews?
        - Does Prezi have security certification such as SSAE16, ISO27X, BASEL, or CoBIT?
    - Prezi's internal processes
        - Do employees undergo regular security awareness training appropriate to their role and function within the organisation?
        - Does Prezi conduct background checks and prescreening for new employees?
        - Does Prezi have controls in place ensuring timely removal of systems access when an individual leaves the organization?
        - Is there an actively maintained and updated inventory of all assets associated with information and information processing facilities?
        - Do you have controls in place to ensure that only authorized personnel have access to user data?
        - How do you ensure the "4-eyes principle"?
        - Is remote access permitted into Prezi’s environment? If yes, what controls do you have in place?
        - Do you have controls in place to detect malware on workstations and servers?
        - What physical security controls are in place at your facilities?
    - Third-party tools and services
        - Does any part of Prezi use the services of a third party, partner or entity other than your company? Do these services transmit, process or store user data?

The Prezi Security Manifesto

We believe that Prezi is an awesome tool to spread ideas and can reinvent how people share knowledge, tell stories, and inspire their audiences to act. We believe that trust is a key component for such a tool. We collected some of the principles we live by to earn this trust:

Security and privacy is not optional.

We don't make compromises on them and will do all the necessary steps to integrate them deeply into our daily life from the scratch board until implementation.

We believe in transparency.

We are honest about our mistakes both internally and externally to speed up our and others' learning process and to increase trust.

We are part of the security community and we value our peers.

We make our tools and knowledge public and we respect others pointing out risks in our systems.

Security is a mindset, not a team.

We believe that having security as organic part of the company's daily life is more healthy, effective and sustainable on the longer run.

We love to automate.

To reduce the risks caused by the human factor we support our internal processes and development with automation wherever we can.

We believe in selling instead of telling.

We believe in the power of security awareness more than pure policies, we keep all functions within the company up to date and share the relevant best practices / threats with them.

We trust data and nothing else.

We have detailed logging on every level (from the OS through the network layer to the application) to be able to automatically detect anomalies, manually spot suspicious events or have all the necessary information in case of an incident to figure out what happened & improve our reactions.

We follow best practices in cryptography.

We believe in battle tested cryptography, we fight against self-developed solutions - we propagate the usage of long tested, safe to use cryptographic algorithms within the company.

An overview of security at Prezi

Prezi's Security Program

Does Prezi have a dedicated security team?

Our dedicated Security Team is responsible for coordinating information security activities within the company and integrating security best practices and baselines to the tooling and default configurations used throughout the organization. All members of the Security Team are engineers with experience in security, development, and operations and hold security certifications like CEH, OSCP, and OSCE.

Does Prezi have written Information Security Policies?

Yes, we have documented the security requirements and obligations through a set of written policies available on our internal Wiki.

:

- Risk assessment methodology
- Infrastructure level security policies
- Data and application classification / handling policy
- Secure Development Best Practices
- Internal application handling & hardening policies
- Security incident response plan
- Change management policy
- Access management policy
- Physical and visitor access policy

We believe in awareness more than pure policies, the security team continuously keeps all functions within the company up to date and share the relevant best practices / threats.

Does Prezi have an incident response program?

Yes. We have a written Incident Response Policy which was created by the security team and was approved by management. It is being reviewed and tested continuously, but at least on an annual basis.

Are managers engaged in driving security within the business?

Management actively supports effective controls within the organization through clear direction, demonstrated commitment, explicit assignment, and the acknowledgment of information security responsibilities.

Does Prezi have an accredited third-party perform security audits of the security program?

We successfully went through an audit by an independent external third-party and obtained a SOC2 report on Security for Prezi Next.

Please also keep in mind that we also run a responsible disclosure program (https://bugbounty.prezi.com/) and third-party penetration tests are executed regularly. As a result, our infrastructure and application is scanned by vulnerability scanners and enthusiastic hackers twenty-four hours a day, seven days a week.

Does Prezi have a vulnerability management program and perform vulnerability scans on a regular basis? Does the application undergo regular penetration tests?

Yes. We run a responsible disclosure program (https://bugbounty.prezi.com/). As a result, our infrastructure and application is scanned by vulnerability scanners twenty-four hours a day, seven days a week.

In addition, we also run automated vulnerability assessments to ensure issues are detected and eliminated before they are detected by our responsible disclosure program.

Time to time larger changes also undergo penetration tests by our dedicated security team.

Does Prezi have regular vulnerability assessments from independent third parties?

On an annual basis, we engage with an independent third-party auditor company to execute an infrastructure and application level penetration test. Results are evaluated by the Security Team and the identified vulnerabilities are prioritized, logged, and sent to the appropriate engineering team according to our bug handling procedures.

Please keep in mind that we also run a responsible disclosure program (https://bugbounty.prezi.com/). As a result, our infrastructure and application is scanned by vulnerability scanners and enthusiastic hackers twenty-four hours a day, seven days a week.

Can you share the results of your latest penetration test and the status & mitigation plan for the open issues?

Sure thing, however we are only allowed to share the results of the penetration test executed by an independent third party auditor company if you have signed an NDA with Prezi.

Do you maintain a patch management process?

We don't have a formal patch management process however any outstanding, public facing critical security issue introduced by outdated / vulnerable software versions will be immediately patched. We have automated vulnerability scanning tools in place to be able to detect such risks as soon as possible.

We also have an internal SLA on fixing PRIO1, Critical and Medium severity security risks which SLA is continuously monitored, tracked and reported towards management. Prioritisation of fixing Low severity issues is the responsibility of the product owner & product manager responsible for the affected feature.

What networking security measures do you have in place?

We use Amazon EC2 Security Groups to restrict access to microservices on a networking level. Services by default are not accessible from anywhere; explicit inbound rules have to be added manually. To ensure that changes potentially affecting the security of the infrastructure are detected in a timely manner, an automated solution (reddalert) was developed by the Security Team which creates alerts in the ticketing system for review.

Network access to databases hosted at Amazon by default is restricted only to EC2 instances of the microservices using the data.

Administration of the infrastructure happens over SSH. SSH is accessible from the BP and SF offices or from behind Prezi's VPN and only allows key-based logins.

Does the QA process also address common application vulnerabilities as defined by OWASP or SANS? Does Prezi perform internal security code reviews?

Yes.

All initiatives impacting the infrastructure or code of Prezi are required to have a detailed architectural plan according to Prezi's software development life cycle. All architectural plans are reviewed by the Security Team in order to highlight potential security risks in the plan as early as possible.

We follow Secure Software Development Lifecycle best practices tailored down for our Agile methodologies to make sure that no risky code or infrastructure changes get into production.

We support our SSDLC with tools automatically detecting code or infrastructure changes against security best practices. We review all possibly risky code changes, keep track of open issues and communicate with engineers regularly to share security related knowledge and best practices.

We run a responsible disclosure program (https://bugbounty.prezi.com/) as a result, our infrastructure and application is scanned by vulnerability scanners twenty-four hours a day, seven days a week. We also run automated vulnerability assessments to ensure issues are detected and eliminated as soon as possible.

Does Prezi have security certification such as SSAE16, ISO27X, BASEL, or CoBIT?

We successfully went through an audit by an independent external third-party and obtained a SOC2 report on Security for Prezi Next.

Prezi's internal processes

Do employees undergo regular security awareness training appropriate to their role and function within the organisation?

Yes. We conduct new hire & annual security awareness training for personnel, which communicates information about employee security and confidentiality commitments, their roles and responsibilities for securing information, and reporting and escalating issues. The contents of the training are tested through a quiz about all security-related expectations relevant to employees. New employees are required to take the training & quiz. The Security Team, together with management, monitors compliance with the training requirements. We also regularly train developers and engineers on security issues as they are discovered during any phase of development.

Our dedicated security team continuously keeps all functions within the company up to date and share the relevant best practices / threats in our internal Blog and other communication channels like Slack.

Does Prezi conduct background checks and prescreening for new employees?

Personnel offered with employment in the US are subject to background checks and we have a detailed hiring process ending typically with a few days long on-site assessment after several other phases involving HR, the hiring manager and the team itself as well.

Does Prezi have controls in place ensuring timely removal of systems access when an individual leaves the organization?

Yes. All high risk systems are managed through a centralised identity and access management solution. We have clear processes related to account termination in our Access management policy. As a result when an individual leaves the organisation their access to the integrated systems is revoked on they last day.

Is there an actively maintained and updated inventory of all assets associated with information and information processing facilities?

We have hardware inventory for the laptops our employees use for their daily work. All these devices have an enterprise mobility management software installed which ensures that security requirements are met.

Do you have controls in place to ensure that only authorized personnel have access to user data?

We manage access to all high risk systems through a centralised identity and access management solution. We created our Access management policy and configured all defaults keeping the least privilege principle as our ultimate goal. The default access rights granted for everyone are configured based on their connection to Prezi (e.g. full time employees, contractors, people on assessment, students, ...), their department and their team. This way we believe by default we only give access to everyone to those systems which they need on a daily basis and any other access right is provided on a case by case basis.

Access rights and exceptions are handled by the IT and the Security team. All changes in the granted access rights are logged. Only a limited number of people have privileged access rights (e.g. be able to become root) to our systems.

2nd factor authentication is required to access any system integrated to the identity and access management solution or any internal administrative function. Disabling 2nd factor authentication can only happen on a per-user basis and temporarily by the Security team. For certain users 2nd factor authentication is not required from the Budapest and San Francisco offices.

How do you ensure the "4-eyes principle"?

Our Change management policy requires and enforces the 4-eyes principle for any code change affecting systems handling or accessing customer data. Changes in these codebases can be only introduced by opening pull requests and explicit approval from competent and responsible engineers (the owners of the microservice).

Since Prezi engineers are responsible for both code development and the operations of the underlying infrastructure (with the support of the dedicated Infrastructure Team), they have access to our AWS infrastructure to be able to implement changes effectively. Changes that happen directly in AWS or through the use of our infrastructure automation tool, the proposed changes are reviewed in a timely manner leading up to their introduction.

Only Prezi employees are allowed to "impersonate" Prezi customers upon incidents or in relation to a support request. Impersonation requires providing a business reason. The provided business reasons are reviewed periodically.

Is remote access permitted into Prezi’s environment? If yes, what controls do you have in place?

Administration of the infrastructure happens over SSH. SSH is accessible from the BP and SF offices or from behind Prezi’s VPN and only allows key-based logins. We also have the audit trails for every command executed through SSH and receive alerts on suspicious ones.

Do you have controls in place to detect malware on workstations and servers?

An enterprise grade endpoint security solution is installed on all employee Windows & Mac workstations (both laptops and desktops). It is configured to run “real-time file system protection” (antivirus) continuously and to receive updated virus signatures from the vendor at least daily. Any discovered issue is investigated and, if needed, resolved by the IT and Security Teams.

We maintain, develop, and use an internally-built Security Information and Event Management (SIEM) solution capable of processing, correlating, and alerting based on various security logs arriving from the servers within Prezi's infrastructure.

What physical security controls are in place at your facilities?

All production infrastructure responsible for processing and storing customer data is within a physically secure data center provided by Amazon. Amazon is responsible for the physical security of their environment. You can find Amazon's most recent security & compliance whitepapers at https://aws.amazon.com/whitepapers/#security.

Although there are no servers working with production data at the Prezi offices in San Francisco and Budapest, Prezi has implemented a physical and visitor access policy to protect company assets. Employees need to use badges, which are required to access the office area. Guests need to register themselves in the reception area. The office buildings are protected with security guards during the night, while certain areas are also equipped with closed-circuit cameras.

Third-party tools and services

Does any part of Prezi use the services of a third party, partner or entity other than your company? Do these services transmit, process or store user data?

Yes.

We heavily use Amazon as a cloud infrastructure provider, therefore most of the user data is transmitted, processed and stored on their infrastructure. You can find Amazon's most recent security & compliance whitepapers at https://aws.amazon.com/whitepapers/#security.

Selligent is used to send e-mails to our users (e.g. forgotten password emails, shared prezi notifications, ...).

Is the application provided within a multi-tenant environment?

Yes, we heavily use Amazon as a cloud infrastructure provider, therefore most of the user data is transmitted, processed and stored on their infrastructure. Amazon's PCI DSS compliance FAQ answers a few questions about multi-tenancy: https://aws.amazon.com/compliance/pci-dss-level-1-faqs/.

Are security requirements taken into account when using third-parties?

We have a lightweight process on evaluating any third-party which is planned to process or store high risk data. During the process the security team gets a deeper understanding of the planned integration / usage of the thid-party and together with the team implementing the change we execute threat modelling. The identified risks are evaluated and additional controls / contractual changes are requested if needed.

Does Prezi have any policies regarding the usage of external tools?

While we do not restrict developers in terms of third-party tools, we review, share and continue to monitor the security risks for each.

Product security

Does Prezi provide granular, role-based access control for all users?

Yes. With Shared Folders, role-based access control can be achieved.

What authentication options does Prezi support?

We support username / password based authentication along with third-party authentications like Facebook and Linkedin. The passwords are never stored in plaintext.

Does Prezi support 2-factor authentication?

No.

What kind of encryption does Prezi have for client-to-server and server-to-server communication?

TLS encryption is utilized between the Prezi client (either in the browser or in our Windows/macOS/iOS/Android applications) and the server at all times. TLS connection is also set up between servers in different regions within Amazon. Elastic Load Balancers are used to terminate TLS, where we rely on AWS Certificate Manager for the automatic issuance of certificates with strong security parameters (2048-bit RSA public keys with SHA256+RSA signature algorithm).

Communication between infrastructure components (ELBs, EC2 nodes and databases provided by Amazon) within the same availability zone happen within Amazon’s internal network.

Critical customer data (prezi XMLs and media assets) created after 2018 February is encrypted on the server side with AES-256 by utilising Amazon SSE-S3 (see https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingServerSideEncryption.html).

Logging, auditing and monitoring

Does Prezi perform audit logging of all user activity like adding, changing, deleting, and viewing of information at the application, OS, and database levels?

We have detailed user activity logging, including (but not limited to) security related events like login, password change, prezi creation/deletion/modification, privacy settings and access right changes at the application level. At the OS level we have detailed audit logging with the Linux Auditing Subsystem on our cloud infrastructure. We have detailed logs about the cloud infrastructure level changes with Amazon Cloud Trail. We don't have database level auditing enabled, however only a very limited number of prezi.com staff can access the databases directly.

Does Prezi conduct log data collection regarding host OS, guest OS, server, network equipment and web applications, and is the data you collect maintained in a secure storage place for more than half a year?

Yes. We collect OS level audit logs, web server logs, IDS logs, and detailed application level logs in a Hadoop cluster for more than half a year. These logs are also accessible for ad-hoc quick analysis from an elasticsearch cluster.

Is the log data collected by Prezi checked periodically to detect unauthorized access in a timely manner?

Yes. We have both physical dashboards and automated alerts to detect security or availability issues with our service.

Data at Prezi

What type of sensitive data does Prezi store?

We store & consider the following information as sensitive:

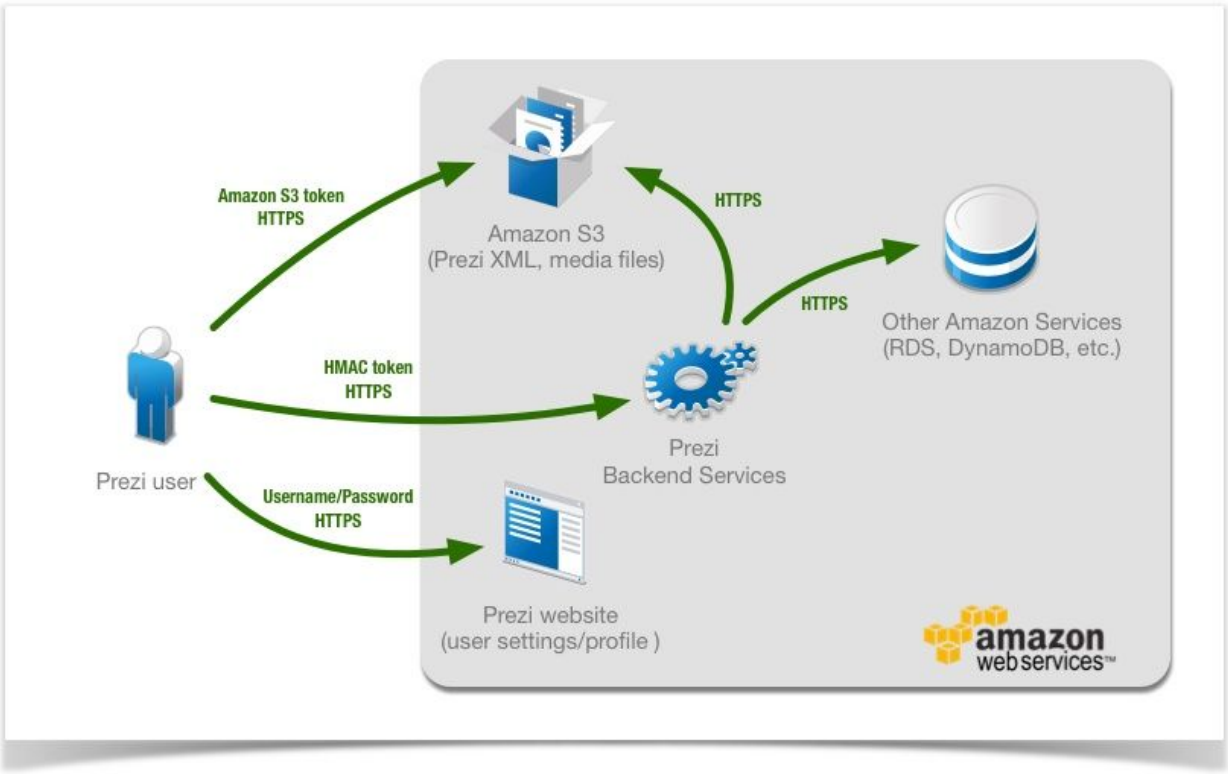
- authentication information
- the prezi document (represented in XML format)
- media content (images, videos) used in prezis

You can find more information about the information we collect in our Privacy policy.

Do you store any protected personal information (PPI) like home address, date of birth, Social Security Number, National Insurance Number, driver's license number, ID card number or bank account/credit card number?

We don't ask our customers to provide any of those.

Can you please provide an architecture diagram about the information flow of user data (password, prezi content) and the relevant authentication / authorization methods?



What are the access controls around the above mentioned sensitive data?

Logical access controls are in place for getting the contents of the prezi XMLs. Prezi XMLs contain references to every uploaded media asset.

Without having legitimate access to the prezi XML contents it is highly unlikely to gain access to the contents of a prezi since the uploaded media assets or the raw prezi XMLs themselves are stored in a location containing at least 40 random characters.

Does Prezi create backups of user content? Is the backup and recovery planned, implemented and tested? Does a disaster recovery plan exist?

Yes, we continuously backup all critical user content (e.g. media files and prezi XMLs) to a separate, strictly monitored and locked down account.

Disaster recovery was not tested yet.

In which countries will the data be stored and processed?

	Data processing	Data storage (live)	Data storage (backup)
Critical user content (prezi XMLs, media assets)	Amazon AWS US East and West region	Amazon S3 US East and West region	Amazon S3 US West region Amazon S3 Ireland region
Meta-data (registration information, prezi permissions, comments, ...)	Amazon AWS US East region	Amazon AWS US East region	Amazon S3 Ireland region

What encryption do you utilise for data in transit?

TLS encryption is utilized between the Prezi client (either in the browser or in our Windows/macOS/iOS/Android applications) and the server at all times. TLS connection is also set up between servers in different regions within Amazon. Elastic Load Balancers are used to terminate TLS, where we rely on AWS Certificate Manager for the automatic issuance of certificates with strong security parameters (2048-bit RSA public keys with SHA256+RSA signature algorithm).

Do you utilise encryption for storing data (encryption at rest)?

Critical customer data (prezi XMLs and media assets) created after 2018 February is encrypted on the server side with AES-256 by utilising Amazon SSE-S3 (see https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingServerSideEncryption.html).

Do you have a data protection policy?

Please read our privacy policy for more details at https://prezi.com/privacy-policy/.

From which geographic locations does staff access the data, either for business support or technical support?

Mainly US and Hungary.

Does Prezi support a method of enforcing users to use only SSO to log in?

Yes, currently Prezi supports Google SSO.