vormats

Security White paper

Table of Contents

Introduction

Our mission is to make video accessible to everyone, so that everyone can make an impact with their story in a world that is more visual than ever. Here at Vormats, protecting your information is our highest priority. Our security strategy covers all aspects of our business, including:

- Physical and environmental security
- Operational security policies and processes
- Communications and data transfers
- Reliability and security of our architecture
- Data Centre Security

This whitepaper aims to provide an overview of the technical and organisational measures taken by Vormats to ensure security and legal compliance.

Physical and environmental security

Office security

Our office is secured and can only be entered with a dedicated keyset. The keys needed to enter the office can only be duplicated with a dedicated security code. Visitors are only allowed into the premises upon invitation from one of our staff members. We do not hold any form of personal data in our office.

Our office network router has been securely configured to remove the default network name and password as well as guest accounts, and its firmware is regularly patched.

Data centre security

The data you exchange with us via our website, email or other communication channels is stored on, and exchanged through, our Vormats Google Drive Environment. This data is hosted In Ireland, on Google's own data centres. These data centres secure your data through encryption, back-up and strict location tracking and access controls. The physical security measures taken to secure these data centres range from secure perimeter defense systems, comprehensive camera coverage to biometric authentication.

To read more about Google's data centre security, please visit: Data and Security – Data Centers – Google.

Operational security policies and processes

Compliance with GDPR

Vormats complies with GDPR through security policies and processes. Vormats has carried out a Data Protection Impact Assessment and physical risk assessment to identify risks and the necessary measures to remediate these. We further keep and regularly update the legally required policies and have strict retention periods for personal data in place.

Information Security Policy

Vormats requires all new staff to read and sign our extensive Information Security Policy, which details how staff are expected to keep your data safe and secure. This policy includes, but is not limited to, a secure remote working policy, requirements on passwords, multi-factor authentication, encryption of devices and stringent access controls.

Data Protection Officer and Information Security Officer

Vormats has appointed a Data Protection Officer, who is responsible for ensuring adherence to all Vormats policies and procedures, regularly updating policies and procedures and ensuring that all staff is adequately trained on handling personal data under the GDPR and other relevant legislation.

Vormats has also appointed an Information Security Officer, responsible for all technical security measures and responding to a security incident within a reasonable time frame in accordance with our Incident Response Policy.

Security training for all employees

All Vormats employees undergo security training during their orientation phase and receive annual security training throughout their Vormats careers. This training covers, amongst others, how to handle personal data under GDPR; how to deal with Data Access Requests and Data Breach obligations.

Confidentiality

All Vormats Employees are required to sign a confidentiality agreement upon hiring, which ensures that all personal data owned by Vormats will not be made public to an unauthorised recipient. This confidentiality agreement is enforceable by a penalty clause.

Supply chain security

All third parties in the Vormats supply chain are evaluated on their level of security. Through signing processing agreements, we ensure that these third-party suppliers uphold the highest standards of security and compliance possible. Vormats regularly audits third-party suppliers and has ensured it can end the relationship immediately if the audit reveals inadequate levels of security and compliance.

Hardware

All laptops and workstations are secured via full disk encryption. We update devices as soon as updates become available and monitor workstations for malware. Vormats has the ability to remote wipe a machine.

External audit & certifications

Vormats has successfully completed the ISO27001 and Information Assurance and Governance Certification (IASME Governance) for controls relevant to security, availability, and confidentiality.

Both ISO27001 and IASME Governance ensure that Vormats takes adequate steps to secure personal information in the following areas: Risk Assessment and Management; Monitoring; Change Management; Training and Managing People; Backup; Incident Response and Business Continuity.

We have hired an independent third party to validate our processes and practices with respect to these criteria and topics.

Communications and data transfers

Vormats uses different communication tools for communications between teams and with our customers. Vormats has data processing agreements in place with all of these communication tool providers to ensure appropriate technical and organizational measures to protect personal data against unauthorized or unlawful processing and against accidental loss, destruction, damage, theft, alteration or disclosure are in place. In line with the GDPR, Vormats does not transfer data to countries outside of the EU/EEA.

Security of our architecture

Application access and identity management

All Vormats users are required to set up an account with a combination of a unique username and strong and secure password (minimum 8 characters), complying with our access management policy and privacy by design requirements. To ensure confidentiality of user video data, passwords are never stored unencrypted in any cache, file, database or access log.

User accounts are validated through email verification. If a wrong password is entered 5 times, the account will be locked for one hour.

The Vormats app uses AWS Cognito to authenticate users and grant access to the app. Through AWS Cognito, Vormats has defined roles and mapped users to different roles so the Vormats app can access only the resources that are authorized for each user.

Amazon Cognito encrypts data at-rest and in-transit. Amazon Cognito is HIPAA eligible and PCI DSS, SOC, ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, and ISO 9001 compliant.

User authentication and data access controls

Access to the AWS development environment is strictly controlled via IAM roles. Separate IAM users are used for development and live environments. All access to the AWS platform is controlled by two-factor authentication.

Vormats follow the policy of ‘least privilege’ meaning that all users are given the minimum privileges required to perform their role. Any increase in privilege must be formally requested and is logged in an administrator tracking tool.

Video data is strictly controlled via Data Access Controls to ensure confidentiality. To this end, Vormats uses the strong segregation mechanisms in AWS to segregate each user’s data and encrypted and sandboxed S3 containers to store videos. The back end is developed to enforce strict data segregation by checking and enforcing permissions for each network request.

Back-up and security of user data

Vormats uses Amazon Web Services (RDS & S3) to manage user data. The database is replicated synchronously so that we can quickly recover from a database failure. As an extra precaution, we take regular snapshots of the database and securely move them to a separate data centre so that we can restore them elsewhere as needed, even in the event of a regional Amazon failure. Backups are periodically tested to ensure they can be loaded quickly in the case of any incident. All S3 buckets are private by default and access to particular files is strictly managed through time-sensitive links.

All data is encrypted at rest using AES-256 encryption. Vormats hosts data in regions exclusively within the European Union.

Monitoring

Vormats is built with the following AWS services: Computing, Networking, User Identity and Application Security Resources. These systems include built-in vulnerability scanning and uptime monitoring. All access to the AWS environment and products built by Vormats are restricted to the responsible and authorised entities and alerts of suspicious activity are reported in real time.

Secure development practices

All software created by Vormats must be designed following the principles of Privacy by Design. The core definition of Privacy by Design is that privacy, and security, must be a primary focus throughout the entire software development lifecycle, from initial inception, through to design, development, testing, deployment, support and end-of-life.

Source code management and review

Vormats uses the Bitbucket revision control system. Vormats uses a third-party source code analysis software to check for any vulnerabilities or issues prior to manual testing being performed. There is then a round of manual review. When the code changes pass these tests, the changes are first pushed to a staging server wherein Vormats employees are able to test changes before an eventual push to production servers and our customer base.

All source code is backed up to a physically separate data centre where it is encrypted using the AES-256 encryption algorithm.

Data centre security

All personal data sourced from our architecture is stored in Amazon data centres. Amazon employs a robust physical security program and is accredited against multiple security industry certifications, including SSAE 16, ISO 27001 and SOC type II. For more information on Amazon's physical security processes, please visit: Cloud Security – Amazon Web Services (AWS).

Environment separation

All development of the application is performed within a dedicated development environment with completely separate architecture prior. Once functional and security tests have been performed, any configuration or source code is transferred to a separate live environment.

Patching

All applications, frameworks, libraries and operating systems are regularly patched. These patches environments are tested within the testing environment to ensure no issues or conflicts arise due to patches being applied.

Encrypted transactions

Web connections to the Vormats service are via TLS 1.2 and above. We support forward secrecy and AES-GCM, and prohibit insecure connections using TLS 1.1 and below or RC4.

Compatibility

In order to comply with Apple and Google security standards and ensure security of the Vormats application, the app is always compatible with the latest Android and iOS versions. The Vormats application supports some earlier versions: Android from version 9 and iOS on iOS phones from iPhone 7.

Privacy Policy

Vormats' privacy policy, which describes how we handle data throughout all of our business process, can be found here.

Cookie Policy

Vormats' cookie policy, which describes how we handle cookies on our website, can be found here.

Want to report a security concern?

Email us at hello@vormats.com.