vormats

FAQ

For Security, Privacy & Compliance

Table of contents

General

Data processing

As part of the contract between Vormats and its customers, Vormats processes data (both business information as well as personal information) for both our own business purposes and on behalf of the customer. By using the Vormats application (either mobile or web-app), our customers and their employees provide Vormats with data to process. We store that information for our customers, ensure that it is kept confidential and secure and share it with third parties that provide parts of our services on our behalf.

Data categories processed by Vormats

The Vormats' applications require our customers and their employees to provide us with identification information. This category of personal data consists of names, email addresses and telephone numbers. The applications further collect and store IP addresses, device information and information about the use of the applications. This information is anonymised where possible and serves to help Vormats to improve our service to our customers. Finally, Vormats processes special category personal data, namely portraits contained in the videos recorded by our customers and their employees.

Location of operations

Vormats carries out its operations from its headquarters located in Amsterdam, the Netherlands. These operations include the development, maintenance and security of our mobile and web applications. Moreover, our finance, sales and HR departments are also operating out of our Amsterdam office.

Registry with the relevant data protection authorities

Vormats' customers are located both within and outside of the EEA. Where required under the relevant legislation, Vormats has registered with the national data protection authority of the countries where our customers are located.

GDPR representatives

As an organisation which processes personal data on behalf of our customers (making us the 'processor' where our customers are 'controllers'), we are sometimes required to appoint a GDPR representative in the geographical area where our customers are located, when Vormats itself is not registered in that geographical area. For instance, we have appointed a UK representative to ensure that our data processing of British data subjects is in line with the UK GDPR. Our appointed representatives are listed in our privacy policy.

Vormats staff at customer premises

None of Vormats staff will need to go on site at any of the customer premises for technical or operational execution of the contract, technical maintenance or for security reasons. The execution of the contract is fully cloud-based, enabling Vormats to carry out necessary work fully remotely.

Customer data at Vormats data centres
Customer data is not held on Vormats' premises, but hosted on external data centres in the Frankfurt region in Germany (EEA).

Information sharing with third party vendors
Customer information is shared with third party vendors (subprocessors) in order to fulfil our service.

Moreover, we use a number of third party suppliers for operational processes, like accountants and legal support. These third party suppliers do not have access to information hosted in the Vormats application. They only have access to our Customer's company name and incidentally, to names of certain employees such as the Chief Executive, the Chief Information Security Officer (CISO) or the Data Privacy Officer (DPO).

Access to customer network
Vormats will never need or request access to any customer internal network.

Access to Personal Data
As part of its services, Vormats has access to the customer's data, including personal data (PII) of its employees. The business information Vormats has access to: Business name, address and registration number. The personal information of customer employees Vormats has access to: Contact information (name, email address, phone number), device information, location information and special category personal information in the form of portraits contained in the videos recorded with the Vormats app.

Certifications
Vormats works according to the international information security standards IASME Governance and ISO 27001. Vormats is audited annually by an external auditor and audit reports are shared with customers upon request.

Access Controls

Access control management
Vormats has access control policies which stipulate which Vormats' internal staff and third party vendors have access to systems that contain customer information. These policies ensure that access is only ever provided after a specific request subject to the authorisation of the chief information security officer of Vormats. According to the access control policy, the requested access will only be granted if there is a clear and defined business need.

Separation of roles
Vormats applies job role separation to staff that can grant access to users and those that need to request access to systems that contain customer information. This enables Vormats to quickly revoke access and delete user profiles or accounts for staff that leave the organisation or when there is no longer a business need for access.

Password policy
Vormats has a password policy that requires the use of strong and unique passwords for each account which are centrally and securely managed in a password manager. Where possible, Vormats systems enforce this policy by permitting only passwords that fulfil the criteria provided in the policy. The policy disallows users to share login credentials for systems and accounts that contain sensitive business information or personal data.

The password policy further requires all Vormats systems and accounts to enforce two-factor authentication. Where possible, all systems and platforms used by Vormats are configured to enforce the password complexity requirements and enforce two-factor authentication.

Access registry and logging
All access rights and account-level permissions are registered using our central security system. Activity logs of systems containing customer data are regularly reviewed.

Application specific

Standard builds
Upon procurement of a new laptop, the laptop is configured by the system administrator against our standard build including the removal of all unwanted software, the creation of user accounts and the creation of an administrator account. Users are not permitted administrative access to any computer.

Change Management
Vormats has change management processes in place to ensure that changes to operating systems, code and hardware are approved and recorded. Change management is also applied to maintenance and operational processes.

Anti-malware
All devices used to access customer information by Vormats staff or third party vendors are equipped with anti-malware software.

Security monitoring
The Vormats mobile application and web application are monitored for security events with third party vulnerability scanning software and with architecture specific monitoring tools. Vormats receives real-time alerts when a potential security event occurs and events are treated according to the incident response plans that are key to Vormats' operations.

Logging
Vormats maintains, stores and monitors audit logs of all user activities, including details of successful and unsuccessful login attempts.

User authentication
The Vormats platform uses external services to authenticate users and grant access to the app. Which uses industry best practice mechanisms (e.g. salted hashes of passwords) for credential storage. The service is compliant with stringent regulations such as HIPPA.

Vormats has defined roles and mapped users to different roles so the Vormats app can access only the resources that are authorised for each user.

Password requirements for Vormats users
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. Password input boxes hide text when it is input by users.

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

Override prevention
Access to the development environment is strictly controlled via IAM roles. Separate IAM users are used for development and live environments. All access to the platform is controlled by two-factor authentication. This prevents the use of unauthorised programs that can override system and application controls.

Dedicated environments
All development of the Vormats 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.

1-way salted hash
Vormats uses a 1-way salted hash to protect Linux or Unix passwords.

Periodic password update
Users are not forced to periodically change passwords as this is no longer best practice.

Encryption login page
All elements of the login page are encrypted.

Single Sign On (SSO)
SSO is possible for providers who adhere to the SAML standard. Our Identity Provider feature allows setting SSO with third-party providers. Vormats has been optimised for Azure Active Directory.

Two-factor Authentication (2FA)
Our user authentication can be expanded with 2FA via the authenticators of Microsoft and Google.

SSO security
When SSO is activated, other login methods become unavailable. When logging in with SSO, users are verified on their domain.

Pentesting
Our mobile and web applications are regularly penetration tested by an independent professional. The results of these pentests are discussed during the management meetings and entered into the change management registry to ensure Vormats' information security management system is continuously improved.

Development practises
Our application is developed in house. Our development team is regularly trained on security best practices, secure software development and the implementation of OWASP in software development.

Third-party access to infrastructure
The Vormats applications are not accessed by any third party for maintenance, backups, etc. Access to the back-end infrastructure is limited to Vormats staff which have signed a confidentiality agreement and are contractually bound to acting in accordance with Vormats' information security processes as described in the Information Security Policy.

Third-party data sharing
Information contained in the Vormats applications is shared with third-party vendors to provide the services to our customers. These services include hosting, providing subtitles, providing customer support and providing analytics and crashlytics.

IP Restriction for admin access
Access to administrative areas of the hosting environment and application is restricted by IP address.

Secure administration access
The Vormats web application uses SSL as a secure web admin authentication method.

Administration credentials
Administration credentials are forced to use strong authentication for access to the administration portal of the Vormats web app.

IP allow-listing
Access to login pages can be locked down to named IP addresses if required using an IP allow-list.

Information hosting
Information in the Vormats applications is hosted on data centres in the Frankfurt region in Germany.

International data transfers
Information in the Vormats applications is shared with third party vendors, for the Crashlytics and Analytics Services the vendor is located in the USA. For this third party vendor, a Data Transfer Impact Assessment has been carried out, showing a limited risk for data subjects or Vormats customers. International Data Transfers are based on Standard Contractual Clauses and additional security measures, such as encryption and anonymisation.

Asset management

Data classification

As part of Vormats' asset management, we maintain data classification according to our asset handling policy. All information assets, both in digital and hardcopy format, are reviewed at least once per year to ensure the assets are properly labelled and sharing rules correspond to the data handling and security guidelines from our asset management and information security policies.

Vormats maintains two levels of classification:

- Public: Information which can be made publicly available.
- Commercial in Confidence: Information which must remain within the organisation and not shared externally without permission from the CISO.

Vormats further subdivides the Commercial in Confidence classification into specific categories:

- Management: Document must only be shared with company directors or named individuals (signed off by company director).
- HR: Document contains HR related information and should only be shared with individuals which have a requirement to access such data. If released, this could cause embarrassment to the individual as well as potentially result in legal action.
- Financial: Document contains financial information about the company which, if released, could result in a breach of legal obligations and cause adversary consequences.
- Technical: Document contains technical information which contains company intellectual property. If released, this could have an impact on the protection of IP within the company.

Data retention

Vormats maintains a data retention policy which is not technically enforced but rather incorporated into internal processes which are subject to regular review. The Vormats CISO and Data Protection Officer are responsible for ensuring that data is purged on a regular basis and that customer personal information contained in the Vormats application is stored in a format that allows the customer (the Controller) to request the return, deletion or destruction of the personal data upon its request or upon termination of the contract.

Asset management registry

Vormats maintains an asset registry in its centralised security system that names the owner, its location and the data contained therein. This registry is regularly reviewed and updated and consulted upon termination of a member of staff to ensure that the assets in question are returned or destroyed according to the asset management policy.

Communications security and data leakage

Customer data segregation

Our application back end is developed to enforce strict data segregation by checking and enforcing permissions for each network request. Within our environment, data is stored in logically separate containers. This is separate from our internal network.

Secure data transmission

Vormats ensures that controls are in place for secure data transmission across internal and external networks. Data is never sent in an unencrypted format (e.g. via email) to any external party and only shared using links to our secure hosting environment. Internal access is only permitted via accessing any content within Google Drive. Storage on devices such as laptops is not permitted.

Monitoring data leakage

Vormats has monitoring controls in place to detect and prevent data leakage through corporate email, file sharing websites and other information systems. We also monitor for any breaches of Vormats email accounts.

Removable media

In principle removable media are not used within Vormats. If a business need arises and there are no viable alternatives, where removable media are used they are encrypted and always scanned for viruses upon insertion. Auto-run is turned off on all Vormats-owned and personally-owned devices.

Compliance

Compliance with the GDPR and the DPA

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.

Independent audit

Vormats has hired a third-party independent auditor who periodically reviews processes and systems for compliance with the Information Security policy and other requirements.

Audit issues are accurately tracked and opportunities for improvement and missing security controls are registered in the change management registry. They are remediated according to our Change Management Policy, which sets time limits for remediation according to severity of opportunities for compliance or non-compliance.

Processing Agreements

Vormats ensures that it has signed processing agreements with customers (controller-processor) and with its third party suppliers (processor-subprocessor). Vormats has hired a third-party consultant to ensure organisational and technical measures necessary for compliance are taken in a timely manner.

Data protection Officer

Vormats has appointed a data protection officer who is responsible for data protection compliance in the whole organisation. The Data protection officer works closely with the security officer to ensure that privacy and security are maintained throughout the entire organisation.

Processing Registry

Vormats keeps a record of all processing activities carried out on behalf of its customers or in its capacity as a Controller. This processing registry describes what data is processed, where and with whom it is shared and the security measures that are taken to maintain the Confidentiality, Availability and Integrity of personal data and business information.

Assistance with data subject requests

Where Vormats is a processor for its customers, we assist our customers with any data subject requests they receive from data subjects. We will never respond to these requests ourselves, unless the Controller has explicitly requested us to do so and only after explicit acceptance of this request on our part.

When thus advised by our customers, we are able to modify an individual’s data where it is inaccurate or incomplete.

Controller instructions
Vormats only processes data through the Vormats applications on the instructions of our customers, the Controller. These instructions are documented in the processing agreements we sign with our customers. The instructions cover, amongst others, our responsibilities under the GDPR, international data transfers, security measures and instructions in case of an information security breach.

Deletion of data
Vormats does not delete customer information contained in the Vormats mobile or web application in the normal course of business. Vormats only deletes this information after the contract with the customer has ended, or when the customer or a data subject requests us to do so.

Cryptography

Encryption policy

Vormats has an encryption policy. This encryption policy requires all data to be encrypted with high levels of encryption whilst at rest and in transit using SSL/HTTPS or AES 256 where appropriate.

Encryption on mobile devices

The encryption policy covers portables and smart devices. Full disk encryption is enabled on all devices, e.g. laptops and mobile phones. The full disk encryption is managed by the system administrator and only the system administrator is able to disable full disk encryption.

Key management

Encryption keys are maintained across all clients. Only the system administrator has access to the keys. We have established key management processes in place to protect the Confidentiality, Availability and Integrity of the encryption keys at all times.

Human Resource Security

Background checks
Vormats carries out background checks for personnel that have access to personal information. These checks include reference checks and a criminal record check.

Confidentiality agreements
All staff and contracted staff are required to sign a confidentiality agreement prior to employment.

Enforcement of information security policies
All members of staff and contractors are contractually required to abide by our information security policies. Vormats is able to enforce this through disciplinary action or termination of employment contracts.

Security training of personnel
All members of staff and contractors are required to follow our cybersecurity and GDPR training upon induction or as soon as possible afterwards and re-take the training once per year. Our staff and contractors are required to complete these online training courses and the exams that they include. All personnel receive regular phishing tests to ensure they are able to recognise malicious emails and are equipped to protect Vormats and customers data.

Information Security Aspects of Business Continuity Management

Business Continuity Management

Vormats has a formal Business Continuity Management policy in place which requires the Business Continuity Plan to be updated at least once per annum and business continuity testing to take place at least annually. Executive Management is responsible for approving and reviewing the Business Continuity Plan.

The business continuity plan and business continuity testing cover the following areas:
- Environmental
- Deliberate Disruptions
- Loss of Utilities and Services
- Equipment and/or System Failure
- Serious Information Security Incidents
- Supply Chain
- Loss of Facilities
- Other Emergency situations

Disaster Recovery Plans

Vormats has Disaster Recovery plans in place to respond to disruption of the IT/Technology that provides services for our customers. All staff are empowered to work remotely in the case of the loss of any office location. We also have full backups of all external environments and source code enabling us to get back to a full operational capability within an acceptable time frame. Our Disaster Recovery plan is reviewed and tested annually by our Security Incident Response Team.

Information Security Incident Management

Security incidents
Vormats has not experienced any security incidents that resulted in loss of sensitive data, financial, operational or reputational losses or regulatory action.

Information security incident management
Vormats has defined an information security incident management policy which all members of staff are required to familiarise themselves with and sign. This policy is reviewed and updated at least once per year.

Information security incident practise
At least once per year, a security incident or data breach is practised on the basis of a previously defined realistic scenario (e.g. ransomware, hack, phishing attack, or physical disaster event). The security incident response team as defined in our information security policies carries out this practise on the basis of a tabletop exercise. They are trained to enable them to identify action or potential security incidents and to understand their obligations to report and escalate such incidents as appropriate.

Data breach notification
Possible security incidents that could lead to a data breach are reported to Vormats customers in accordance with our formal data breach notification policy and the processing agreements that are in place with each individual customer. Vormats always notifies our customers of a potential breach as soon as possible, allowing our customers to fulfil their data breach notification obligations under the GDPR.

Information Security Policies

Vormats has information security policies which are issued, approved and supported by executive management. All Vormats staff and contracted staff are required to read and sign these policies, and disciplinary action is available to Vormats to enforce compliance with our information security policies. All information security policies are reviewed at least every 12 months.

Operational security

Change Management Process

Vormats maintains a formal change management process for systems processing and storing customer information, which includes the Vormats mobile and web applications. Changes need to be officially approved by our Chief Information Security Officer and are registered in a central depository.

Data segregation

Our environments, including operational and application-specific environments, are developed to ensure strict data segregation of customer information. Our environments check and enforce permissions for each network request. All assets in our environments are stored in logically separate containers to avoid contamination.

Separation of environments

Vormats uses three separate accounts for development, testing and production. These separate environments do not communicate with each other. All members of the Vormats development team have completely separate credentials to access the three environments.

Malicious code protection

We use third-party source code analysis software to check for any vulnerabilities or issues prior to manual testing being performed. Furthermore, we run authenticated scans against our web application using leading vulnerability analysis software.

Device security

All devices that are used to access or approach customer information are configured securely and equipped with state-of-the-art security controls.

- All devices are equipped with anti-virus software, ransomware protection, a firewall and hard-drive encryption.
- All software or operating system updates are carried out automatically, but at maximum within 14 days of deployment.
- It has been ensured that devices do not contain out of date software or applications.
- All devices have a separate administrator account to which only our Chief Information Security Officer has the credentials. The administrator account does not run day to day, and its password is required to make any security configuration changes or download new software.

Back-ups

All systems containing customer information are backed-up to a physically separate location. These backups are encrypted and tested regularly in accordance with our backup policy.

Operational risk management
In order to ensure Vormats identifies and mitigates all risks and vulnerabilities in a timely manner, we perform regular risk assessments. These assessments identify our assets and determine the likelihood and severity of impacted confidentiality, availability and integrity of these assets. Vulnerabilities are identified by pentesting, vulnerability scanning, source code analysis and other automated and manual processes. Vormats has produced a risk register that is maintained by our Chief Information Security Officer. Management has the ultimate responsibility for the acceptance of any residual risk.

Penetration testing
The Vormats mobile and web applications are regularly penetration tested by an independent third-party provider.

Secure destruction
Vormats has mandatory secure destruction processes in place for media such as hard drives, portable media, tapes, printers, and other devices with internal data storage which may contain customer information.

Logging and monitoring
All infrastructure services are monitored. Alarms are reviewed at least daily and retained in the case of any incident response process.

Organisation of information security

Dedicated Information Security Officer
Vormats has appointed a Chief Information Security Officer who is responsible for security initiatives within the organisation.

Information security team
We have an information security team whose responsibility is to maintain information security in the organisation, adequately react to security incidents and reply to customer and data subject requests. This team consists of a Data Privacy Officer, an Information Security Officer, a Legal officer, and a Communications officer who together form the SIRT along with our CEO and CTO.

Physical and Environmental security

Physical Security

The Vormats premises where its development and operations activities are carried out are secured to prevent unauthorised physical access, damage or interference to its offices.

All windows and entrance doors are secured with motion sensors when the alarm is turned on. The alarm system is connected to a 24x7 security guard who will be on premise within minutes in the event of a security event.

There is 24x7 camera surveillance around the property, the recordings of which are saved to a centralised platform. All windows and doors are fitted with locks and all points of ingress are secured at all times.

Access restriction to servers

Vormats's hosting provider has controls in place to restrict access and protect server rooms. Vormats's hosting provider provides physical data centre access only to approved employees. All employees who need data centre access must first apply for access and provide a valid business justification. These requests are granted based on the principle of least privilege, where requests must specify to which layer of the data centre the individual needs access, and are time-bound. Requests are reviewed and approved by authorised personnel, and access is revoked after the requested time expires. Once granted admittance, individuals are restricted to areas specified in their permissions.

Environmental security

Vormats and its hosting provider have fire and flood detection and prevention systems in place. Environmental conditioning and monitoring systems are in place to ensure the servers are protected from environmental impact or hazards.

Power failure

Vormats' hosting provider has several controls in place to mitigate the risk associated with power failures. Vormats' hosting provide has UPS devices on all network devices as well as redundant fuel powered generators. All Vormats employees are provided with laptops so in the case of power failure at the Vormats, all employees will relocate to a new facility (e.g. home).

Access logs server rooms or information systems

Vormats maintains access logs of access into sensitive information systems that contain customer information. Vormats' hosting provider keeps access logs of access into server rooms and reviews these logs periodically to prevent unauthorised access to sensitive information.

System Acquisition, Development and Maintenance

System security and hardening

Vormats follows recognised industry security and hardening standards CIS, CIS Apple macOS Benchmark, CIS Google Workspace Benchmark and OWASP top 10) for the development of its mobile and web applications.

System restrictions

Vormats applies system restrictions to software developers on the basis of least privilege. Privileged developer access is prevented in the production environment to ensure privacy and security of customer data.

Application security

Vormats' development process follows the OWASP top-10 standards and the Secure Software Development Lifecycle for building secure applications. This includes internal security reviews as well as external security verification through vulnerability scanning and penetration testing. This ensures our developers are provided with statistics on the most common vulnerabilities found in our applications along with prevention and remediation measures.

Secure development training

All software engineers at Vormats must attend a course on secure software development within the first three months of their employment. All developers must re-complete this training course at least once a year.

Customer data in other environments

The Vormats mobile and web applications are not the only information systems on which customer information is stored. Vormats has access to other customer information, such as business information or personal data of our customer's employees. Where necessary for business operations, Vormats stores this information in Google Drive and our CRM system. These databases of customer information are kept up-to-date and are secured through encryption, technical controls to prevent downloading or insecure sending, and organisational measures such as training staff on secure data handling. Vormats ensures that the same security controls are in place on these databases as in our application architecture.

Third Party Supplier Relationships

Relationships with third party suppliers
Vormats has standard terms and conditions with third parties including limitation of the right to access Vormats customer information and the right to audit and inspect supplier security and information handling practices. These terms form part of our data processing agreements with processors.

External access
No external party has access to any internal Vormats systems.

Security requirements in contracts
All contracts with any third parties include detailed security requirements. We also perform due diligence of each supplier to ensure they meet our security requirements. If they do not meet our requirements, we reserve the right to cancel the contract with that supplier.

Security vetting of suppliers
We send security questionnaires to all third-party suppliers to verify their security. If they do not conform to any requirements, we reserve the right to cease working with that supplier.

What actions are taken if these are deemed to be deficient?
Third parties are given 2 chances of remediation within a given time period. If remediation is unsatisfactory after these 2 tries, we have a contractual ability to cancel the contract with immediate effect.

Supplier review
All supplies are audited at least annually to ensure their security posture conforms with our requirements.

End of contract
At the end of any contractual relationship, each client has the opportunity to request any data we hold on them. If they do not respond within 30 days of the end of the contract, all data is purged permanently from all systems and notification of this purge given to the client.