How VORTEX Facilitates GDPR Compliance

VORTEX BY VIVOTEK

Overview

The General Data Protection Regulation (GDPR), enacted by the European Union (EU) in 2018, is designed to safeguard privacy and personal data of EU citizens and residents. It places obligations on companies offering services in the EU or processing EU personal data in other countries. One of the key aspects of the GDPR is that it creates consistency across EU member states on how personal data can be processed, used, and transferred securely.

VORTEX delivers cloud video surveillance services across the globe and has implemented the necessary measures to fulfil our GDPR responsibilities.

VORTEX's product is built with privacy at its core, offering features specifically tailored to support GDPR compliance. Our commitment is to help our customers meet their GDPR requirements when using our products and services.

This document guides customers to information to help them honor rights and fulfil obligations under GDPR when using VORTEX services.

The Role of VORTEX under GDPR

Under GDPR, VORTEX acts as a data processor. A processor is a natural or legal person, public authority, agency, or other body, which processes personal data on behalf of the controller (end-customers).

For example, when customers use VORTEX to process personal data based on legitimate interests, VORTEX acts as a data processor to assist them in ensuring compliance for the protection of the rights of the data subject.

VORTEX's Preparation for GDPR

Processing Personal Data

The GDPR establishes key principles for the processing of personal data. Our VORTEX platform is engineered to align with these principles, providing robust features that enable both our customers and VORTEX to uphold the highest standards of data privacy and compliance.

GDPR Principles	How VORTEX supports GDPR
Lawfulness, fairness and transparency	Inform data subjects of the data collected in a lawful, fair and transparent manner. VORTEX's End User Agreement outlines the categories of personal data collected and processed by our platform on behalf of customers.
Purpose limitation	Collect data for specified, explicit and legitimate purposes, without further processing incompatible with those purposes. VORTEX collects, processes, and retains personal data from its customers and their VORTEX cameras to provide and operate our platform and services for customer use.
Data minimization	Collect relevant and necessary personal data for the processing purposes. VORTEX collects and processes data that is necessary to provide, develop and improve its products and services. Customers can use the 'privacy mask' feature to remove unnecessary and identifiable areas.
Accuracy	Provide resources to remove data that is inaccurate, or asked to be erased by a data subject. Customers can remove facial connections when using the 'profile search' feature, ensuring that all footage remains unidentified. They can also contact VORTEX for any removal requests.
Storage limitation	The video footage should not be kept longer than necessary to achieve the intended purpose. The recordings must be erased once this period ends. VORTEX offers various retention periods for edge storage on SD cards (30,60, 90 days) and cloud storage (30-365 days). All data is automatically deleted based on the selected retention period.
Integrity and confidentiality	Place appropriate security measures in place to protect personal data. VORTEX provides SSO, MFA and role-based management to ensure data security. Audit logs are trackable for privacy enhancement. For more details on role-based access control and audit logs, please refer to the information below.

Securing Data Privacy and Role Integrity

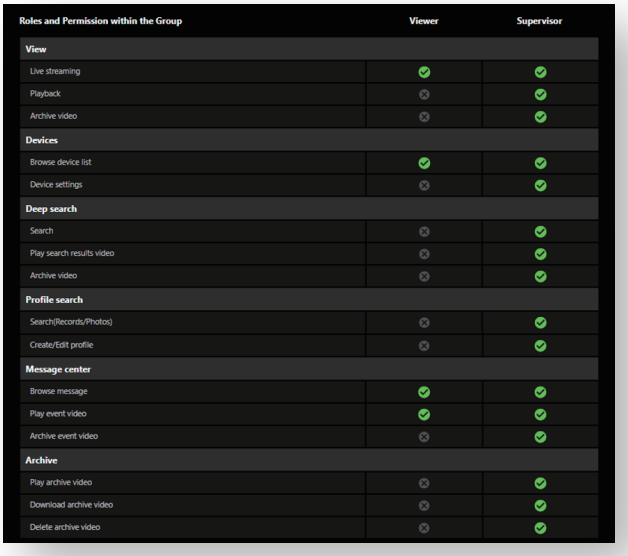
Role-based Access Control: Enhancing Security and Privacy

Role-based access control (RBAC) is a model for authorising end-user access to systems, applications and data based on a user's predefined role.

By restricting access to specific features such as live streaming, deep search, and downloading archived videos, RBAC enhances data privacy and minimises risks.

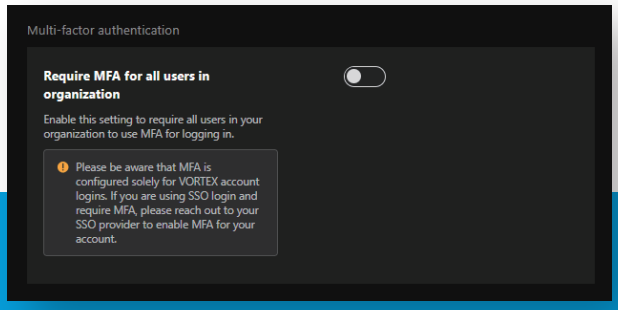
With VORTEX, RBAC is seamlessly integrated to provide robust user permissions to ensure they are aligned with each user's role, safeguarding data and maintaining operational security.

Operators have the flexibility to assign permissions to specific device groups and features based on individual roles. VORTEX supports three roles: 'Admin', 'Supervisor' and 'Viewer'.



Roles and Permission within the Group	Viewer	Supervisor
View		
Live streaming	✓	✓
Playback	✗	✓
Archive video	✗	✓
Devices		
Browse device list	✓	✓
Device settings	✗	✓
Deep search		
Search	✗	✓
Play search results video	✗	✓
Archive video	✗	✓
Profile search		
Search(Records/Photos)	✗	✓
Create/Edit profile	✗	✓
Message center		
Browse message	✓	✓
Play event video	✓	✓
Archive event video	✗	✓
Archive		
Play archive video	✗	✓
Download archive video	✗	✓
Delete archive video	✗	✓

- **Admin:** Complete access for configuration and management, with the exclusive authority to delete the entire organisational account. Each organisation can designate only one Admin, ensuring centralised and secure oversight.
- **Supervisor:** Advanced access tailored for monitoring and operational oversight.
- **Viewer:** Limited access designed for basic viewing needs.

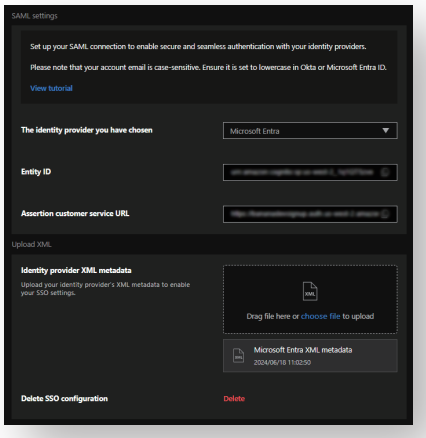


Multi-Factor Authentication (MFA): Strengthening Access Security

VORTEX incorporates Multi-Factor Authentication (MFA), such as Microsoft Authenticator, OKTA or Google Authenticator, to provide an additional layer of access security. By requiring two or more verification methods, MFA protects against unauthorised access and ensures only authorised users can access sensitive data and systems.

- **User Flexibility:** Support various authentication methods, such as SMS codes, authenticator apps, or hardware tokens, making it convenient for different organisational needs.
- **Risk Mitigation:** Prevent unauthorised access even if passwords are compromised, safeguarding sensitive data and systems.

Single Sign-On (SSO): Simplified and Secure Access



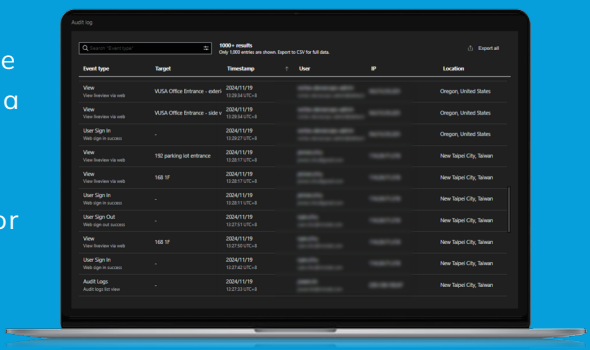
SSO allows users to access multiple systems and applications with a single set of credentials, reducing complexity and improving user experience. VORTEX supports SSO via Microsoft Entra ID to streamline user authentication and enhance security.

- **Improved Efficiency:** Eliminate the need for multiple logins, saving time and boosting productivity.
- **Centralised Access Control:** Integrate seamlessly with existing identity providers for consistent and secure user management.

Audit logs: Transparency and Accountability

Audit logs in VORTEX support GDPR compliance by providing a transparent record of user activities, ensuring accountability and security.

By tracking actions such as live viewing, user management, logins/logouts, and access to the message center for trigger events, VORTEX's audit logs serve as a powerful safeguard against unauthorised access. This not only helps detect and mitigate potential risks but also provides organisations with clear evidence trails for audits and incident investigations.



With VORTEX, businesses can enhance operational security, strengthen data protection, and confidently meet GDPR obligations—all while offering customers the peace of mind that their data is managed responsibly.

International Data Transfer

VORTEX ensures safe data transfers from the European Economic Area (EEA) to our data centre in the US, recognised as a safe country providing adequate protection by the European Commission.

Partnering with AWS, our infrastructure provider, we adhere to GDPR requirements by leveraging AWS's robust compliance framework and ISO certifications, including ISO 27001 (technical security), ISO 27017 (cloud security), and ISO 27018 (cloud privacy).

For EEA customers, they can choose to have their footage (image and videos) data hosted in VORTEX's Frankfurt, Germany AWS data centre, available in January 2025.

VORTEX
BY VIVOTEK

About VORTEX

VIVOTEK Inc., founded in February 2000, is a global leader in security surveillance, dedicated to fostering an ecosystem for the IP surveillance industry.

As part of this vision, VIVOTEK launched VORTEX, its VSaaS platform, in 2022 to expand the ecosystem into cloud surveillance. This enables long-term collaboration and growth with partners in creating a safe, more secure society.

At VORTEX, safeguarding customer data privacy and ensuring compliance are key priorities. Every product and feature we develop is built with data security in mind.

As a cloud solution provider of video surveillance, we understand the importance of managing personal data. We handle personal data responsibly and are committed to helping customers meet GDPR and other data protection standards, while continuously evolving our platform to support compliance and protecting data integrity.

Contact Us

Get in touch with us to discuss your needs, ask questions, or provide feedback.