VERKADA

VERKADA AND GDPR

Becoming GDPR Compliant With Verkada Video Security

How Verkada Supports GDPR Compliance

The General Data Protection Regulation (GDPR) is a comprehensive piece of legislation designed to protect citizens of the European Union and their personal data. Established in May of 2018, the GDPR replaces the Data Protection Directive

In order to ensure the proper protection is in place, the EU has provided guidelines that are necessary for businesses operating in these regions to follow.

Failing to meet the requirements of GDPR can result in significant penalties and fines for both those providing and using a service.

At Verkada, we've taken the steps to provide customers with the necessary protections, tools, and resources to use our service with confidence in these regions.

Fortunately, Verkada's platform is designed in such a way as to enable our customers to comply with the requirements of the GDPR in their use of our products.

International Data Transfers

Verkada establishes an adequate basis for the transfer of personal data from the European Economic Area (EEA) to our data centers in the U.S. by implementing the EU Model Clauses in a Data Protection Agreement with our customers based in the EEA.

Verkada's hosted infrastructure provider, AWS, maintains ISO 27001, SOC 2, and SAS 70 certifications and has implemented its own robust GDPR compliance regime. And EEA-based customers can elect to have their data hosted in Verkada's Dublin, Ireland AWS data center.

For more on Verkada's certification visit privacyshield.gov.

> At Verkada, we take customer security and privacy as our primary responsibility.

Verkada Takes a Security-First Approach to Data Protection

At Verkada, we take customer security and privacy as our primary responsibility. In everything we build, from our hardware to our cloud-based software, we've ensured that protecting our customers' data is at the forefront of what we do.

As a video security solution, Verkada is designed to capture continuous footage of objects that may appear in frame. This can include various forms of Personally Identifiable Information (PII), including an individual's face, property, and other materials or characteristics that may associate captured footage to a person.

Our commitment is to protect the privacy of businesses and individuals alike, and continue to make it our mission to protect the security and integrity of personal data.

Keys to Secure Video Surveillance

End-to-End Encryption

All connections to Verkada devices are securely encrypted, and cameras only make outbound connections to our cloud services. By default, all Verkada systems encrypt data in transit using TLS, and all communication is over Port 443.

Automatic Firmware Upgrades

Verkada's cloud-based management interface runs exclusively on Amazon Web Services (AWS), which meets the highest industry-standards for ensuring the security and protection of its customers' data. Verkada also provides integration with Single Sign-On providers for secure authentication and role-based access control for fine-grained permissions management and has implemented full audit logs of video access and configuration changes.

Secure Backend Infrastructure

We provide automatic updates to the firmware running on the cameras which include security patches, as well as new features and enhancements for device performance. These updates are delivered securely from our cloud service to the cameras and require no additional external downloads or configurations.

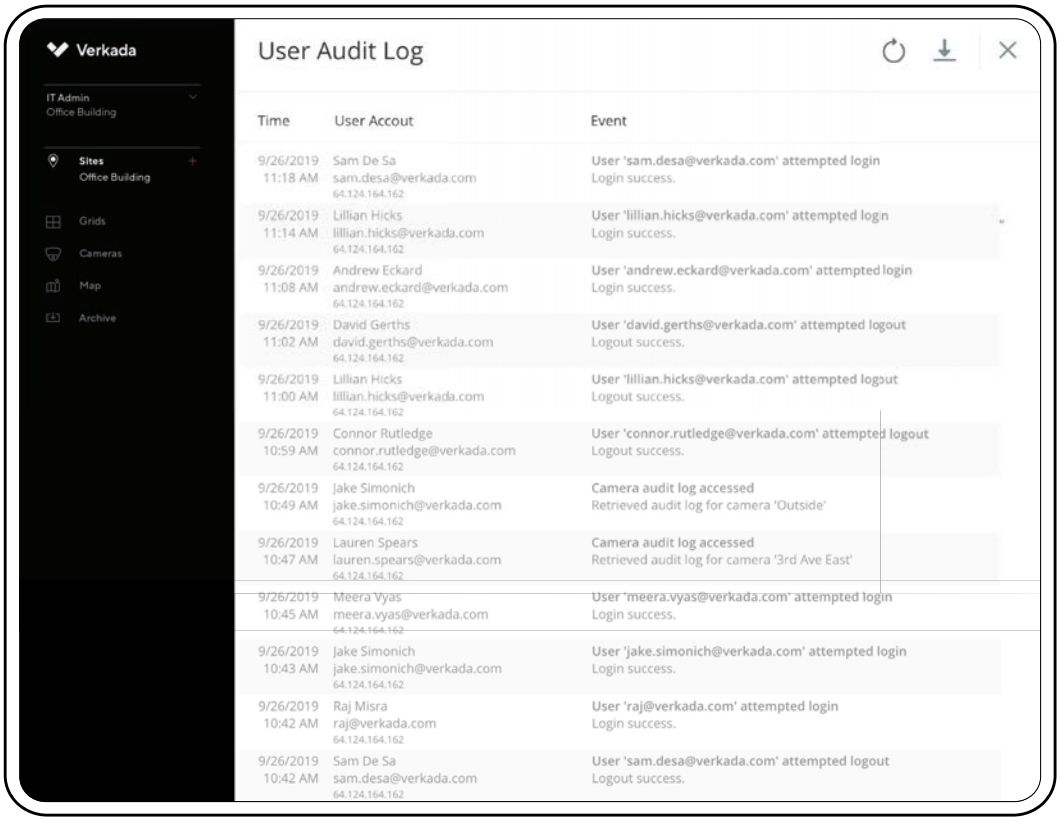
GDPR Privacy Principles

What's more, the Verkada platform enables our customers, as data controllers, and Verkada, as a data processor, to uphold the GDPR's privacy principles.

PRINCIPLE ONE **Lawfulness, Fairness, and Transparency**	Inform users of the types of data collected while using our products and services. Verkada's End User Agreement and Privacy Policy both make clear the types of personal data collected and processed by our platform on behalf of customers, and we recommend that our customers provide prominent notice in their locations of the use of video surveillance equipment.
PRINCIPLE TWO **Limitations on Purposes of Collection, Processing, and Storage**	Only collect, process, and maintain personal data for the explicit purpose of why it was collected and do not disclose it to a third party or used for materially different purposes. Verkada only collects, processes, and maintains personal data received from its customers and their Verkada cameras for the express purpose of making our platform and services available to each of our customers.
PRINCIPLE THREE **Data Minimization**	Only collect limited data that is relevant to the purposes of the product or service. Verkada won't collect or process data that is unrelated to the necessary actions of the product or service. We use the information we collect to provide, develop and improve Verkada products and services, including to make assessments and recommendations about products, safety, or security enhancements. We may use your contact details to send you this information or to ask you to participate in surveys about your Verkada use and to send you other communications from Verkada.
PRINCIPLE FOUR **Accuracy**	Provide resources to remove data that is inaccurate, incomplete, or requested (Right to be Forgotten). Through Verkada's management system, customers have the ability to delete footage, as well as contact Verkada support for any help with removal requests.
PRINCIPLE FIVE **Storage Limitation**	Provide the ability to delete any personal data once it is no longer needed. Verkada offers a range of camera options with different retention periods (ranging from 30-120 days), giving operators the ability to ensure specific cameras meet compliance needs. Local storage of footage on the camera also means that the bulk of the personal data captured stays on the customer's premises, with only a minimal amount of data transmitted to Verkada's cloud for processing.
PRINCIPLE SIX **Integrity and Confidentiality**	All personal data collected using Verkada services must be kept safe and protected against unauthorized or unlawful processing to avoid loss, destruction, or damage. Verkada's approach and offerings are designed to ensure the highest confidence and trust.

Data and Role Protection

USER MANAGEMENT **Role-Based Access Control**	Operators may use Verkada's role-based system to limit access to cameras that are placed in secure areas, reducing visibility for employees who may only need limited access.
USER ACTIVITY **Audit Logs**	For any activity — including adjustments to settings, accessing cameras, and archiving and sharing footage — Verkada keeps detailed logs including time, date, and the use who took any action within the platform.
SECURE ACCESS **User Authentication**	To ensure greater access security, Verkada includes options for integration with single-sign-on (SSO) and two-factor authentication (2FA) providers.
SECURE END-TO-END **Cyber Security Built-In**	Verkada provides all the necessary tools to ensure the security of video security systems. All hardware is also designed with end-to-end encryption for protection against threats, and can never accept third-party software.



Looking Ahead

Verkada is committed to protecting its customers' data and helping to ensure their use of our products complies with the requirements of the GDPR and data protection principles more generally. And as privacy and data protection laws continue to evolve, we will continue providing our customers with the necessary improvements and resources needed to meet the latest compliance standards.

About Verkada

Verkada makes enterprise physical security systems for the modern world Verkada's platform combines plug-and-play security cameras with intelligent, cloud-based software — all in a scalable, user-friendly system. Hundreds of organizations use Verkada to enhance physical security and gain new insights that improve the efficiency of their operations. Verkada is headquartered in San Mateo, California with offices in London, England.

Security Resources

For more information on the General Data Protection Regulation (GDPR)
eugdpr.org

For more information on Verkada's Privacy Policy
verkada.com/privacy

VERKADA

SF Bay Area - USA HQ
405 E. 4th Avenue
San Mateo, California 94401

London - UK HQ
91-93 Great Eastern St Suite 3
Hackney, London EC2A 3HZ, UK

Email
sales@verkada.com