

FAQ Privacy

Navigating the Privacy (GDPR) Landscape with Verkada

Disclaimer: This document is for informational purposes only and does not constitute legal advice. Organizations should consult with legal counsel to ensure their specific use of Verkada products complies with the laws and regulations that apply to them.





A Collaborative Approach to Privacy

The global privacy landscape is increasingly complex, making it difficult for organizations to distinguish between meaningful compliance and regulatory “noise.” At Verkada, we aim to simplify this process by providing the technical foundation and transparency you need to manage your data protection program effectively. Although this FAQ primarily addresses GDPR compliance, the principles discussed are broadly applicable to many other global compliance programs, as highlighted throughout this FAQ.

Shared Responsibility: Controllers and Processors

Compliance is a shared journey. Under the GDPR, our roles are distinct but complementary:

- **You are the Data Controller:**

As the customer, you maintain ultimate control over your data. You determine the purpose of the processing, the retention periods, the legal basis for collecting footage and sensor data. You determine which privacy features are appropriate for your specific environment and legal context.

- **Verkada is the Data Processor:**

We provide the infrastructure and tools to secure and manage your data. We act solely on your behalf and according to your documented instructions, as formalized in our Data Protection Addendum (DPA).

Verkada’s “Privacy by Design” features are built to facilitate your path to compliance by translating complex requirements into intuitive technical controls. These tools are designed to reduce administrative friction and surface the most relevant information, allowing your team to maintain a “human in the loop” for critical oversight and final decision-making.





GDPR Operational Mapping FAQ

GDPR Article & Requirement	How Verkada Helps	Documentation & Resources
Articles 12-22: Data Subject Rights	Verkada's Command platform is designed with on demand tools to streamline the Controller's ability to manage Data Subject Requests such as accessing, updating, exporting, and deleting personal data of individuals.	Verkada Help Center
Article 28: Processor Obligations	Our Data Protection Addendum (DPA) is a binding commitment ensuring we process data only on your instruction, subject to appropriate confidentiality and security terms.	Data Processing Agreement
Article 28(2): Subprocessors	We provide transparency through a public Subprocessor List and a dedicated Notification Portal for updates on our service providers.	Subprocessor List & Portal
Article 32: Security of Processing	We implement appropriate technical and organisational measures to safeguard your personal information. In addition, we adhere to and are audited against industry standard security and privacy compliance frameworks, such ISO 27001/27701/27017/27018; SOC 2, Type 2.	Verkada Security Controls Security & Incident Response
Article 33: Breach Notification	Our security team has in place technical safeguards to protect your data and monitors the environment 24/7/365. In the event of a verified breach affecting customer data, we notify you without undue delay.	Data Processing Agreement
Article 35: DPIA Support	We offer a detailed Data Privacy Impact Assessment (DPIA) Support and FAQ For Cameras to help provide information needed for you to conduct and document your impact assessments.	Available upon request



International Data Transfers (GDPR Chapter V)

For customers transferring personal data from the EU, UK, or Switzerland to the United States, Verkada employs a “belt and suspenders” legal framework to ensure an equivalent level of protection as required by **Articles 44–46 of the GDPR**.

1. Data Privacy Framework (DPF)

Verkada is self-certified with the U.S. Department of Commerce under the **EU-U.S. Data Privacy Framework (EU-U.S. DPF)**, the **UK Extension to the EU-U.S. DPF**, and the **Swiss-U.S. Data Privacy Framework**. This allows our customers to rely on the European Commission’s “adequacy decision” for transatlantic data flows.

- **Official Listing:**

You can verify our active status on the [Department of Commerce DPF Participant List](#).

2. Standard Contractual Clauses (SCCs)

As a secondary layer of protection, Verkada incorporates the latest **Standard Contractual Clauses (SCCs)** into our Data Protection Addendum. This ensures that even in the absence of an adequacy decision, your data transfers remain governed by an EU-approved legal contract applying the required EU-level of data protection.

Privacy Enhancing Technologies (PETs)

Verkada integrates specific technical measures designed to help you minimize data exposure and protect individual privacy. We summarize them here, but for more information, please visit our [Knowledge Center](#).

- **Public Privacy Disclosures (QR Functionality):**

Command allows you to generate site-specific **QR Codes** for physical signage. Visitors can scan these to view your privacy notice and see which features (e.g., People Analytics) are active.

- **Privacy Regions:**

Define “Block-out Zones” in a camera’s field of view to ensure sensitive areas are never recorded or viewable.

- **Face Blur (Live & Historic):**

Support data minimization by blurring faces in real-time. For investigations, authorized users can apply blurring to bystanders during video export.

- **Person of Interest (Faces Only):**

Our facial recognition technology can be configured to alert only on **specific** pre-determined profiles rather than identifying every person who enters the frame. “Faces Only” leverages Verkada’s hybrid cloud architecture to decentralize the search process, performing facial analysis directly on the camera instead of in the cloud. When a person is detected, the camera’s onboard processor creates a unique mathematical map of their facial features—a digital signature used solely for comparison. This signature is checked locally on the camera against the “Person of Interest” profiles you’ve designated; if there isn’t a match, the biometric signature is instantaneously wiped from the camera’s temporary memory and is never sent to the cloud. While the biometric signature is destroyed to protect privacy, the system still preserves a low-resolution thumbnail and basic attributes (like clothing color) in your “People History” logs. This allows you to still search for individuals based on their appearance without the system maintaining a permanent biometric record of their face.

- **Access Control & Immutable Logging:**

Every action taken within the platform—from logins to video exports—is recorded in an **immutable audit log**, providing an unalterable record for compliance audits.

- **Retention Settings:**

Verkada provides individually configurable retention settings at the device and platform level. You can select camera hardware with onboard storage ranging from 30 to 365 days for local, continuous recording. For added redundancy, the Command platform includes 30 days of cloud backup by default, which can be extended for long-term security needs.



Global Compliance & Biometric Requirements

- **Global Reach:**

Our platform supports your compliance with **CCPA/CPRA** (USA), **PIPEDA** (Canada), **APPs** (Australia and New Zealand) and other regional frameworks.

- **Biometric Data Management:**

We ship our products with “default off” settings where facial recognition is concerned, and offer granular controls for region-specific biometric law compliance (e.g., Quebec, EU).

- **Data Residency:**

Choose to store your data in specific regions per device or globally, including the US, Canada, Ireland, or Australia, to satisfy local data residency requirements.

