Verkada

Privacy

How we treat the data we collect & provide transparency and control around our data-handling practices.



SIX PRINCIPLES · PRIVACY CONTROLS · RESOURCES

OUR MISSION AND VISION

Protecting people and places in a privacy-sensitive way.

At Verkada, our mission is to protect people and places in a privacy-sensitive way. Embedded directly into our product design, our six foundational principles help keep customer data isolated—avoiding cross-customer data pooling—while providing robust privacy controls that help secure data, align usage with internal policies, and ensure organizations maintain the ownership and transparency needed to meet their unique compliance needs.



Table of contents

01	Purpose limitation and data boundaries	04
02	Transparency	05
03	Human-in-the-loop and agency	06
04	Integrity and model quality	08
05	Data minimization and privacy controls	09
06	Robustness, security, and accountability	11

PRINCIPLE ONE

Purpose limitation and data boundaries

01

Physical security data should remain focused on its intended safety purpose. We design technical controls directly into our platform architecture—such as enabling organizations to restrict facial processing strictly to designated Person of Interest (POI) profiles—to keep features targeted. Our global infrastructure features localized cloud shards that support data residency requirements by keeping data stored, and in some regions processed, locally. This is backed by robust data processing terms in our Customer Data Processing Addendum, Standard Contractual Clauses (SCCs), and certification to the EU-U.S., UK Extension, and Swiss-U.S. Data Privacy Frameworks (DPF) as a legal basis for transfers of personal information from the EU, the UK, and Switzerland to the U.S.

DATA HANDLING

Strict data siloing

Your video and data are logically separated in dedicated, tenant-isolated cloud environments. Your organization's data is never pooled with other customers or placed into a shared, searchable network.

DATA HANDLING

Local data residency

You choose exactly where your cloud data is stored to meet local compliance requirements.

United States | Canada | Australia | Germany | Japan | Singapore | South Korea



PRINCIPLE TWO

Transparency

02

We design our systems to help our customers explain the technology in clear, visible, and easy-to-understand ways for the people who interact with it. By integrating features like on-site signage with QR codes, our platform enables organizations to provide immediate, accessible privacy disclosures directly to building occupants—offering clear visibility into what technologies are active, how data is processed, and who to contact with questions.

PUBLIC TRANSPARENCY

Public privacy disclosures

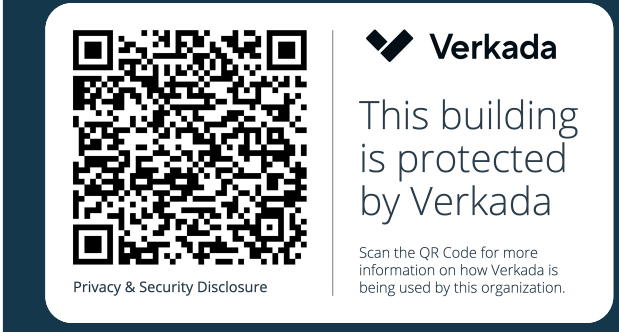
Allows on-site notices to be displayed physically so visitors can scan a QR code to easily review privacy policies and contact details.

THIRD-PARTY ACCOUNTABILITY

Public subprocessors list

We maintain a public list of third-party subprocessors with an active notification portal so legal teams can opt to receive alerts whenever we update our service providers.

verkada.com/privacy/subprocessors



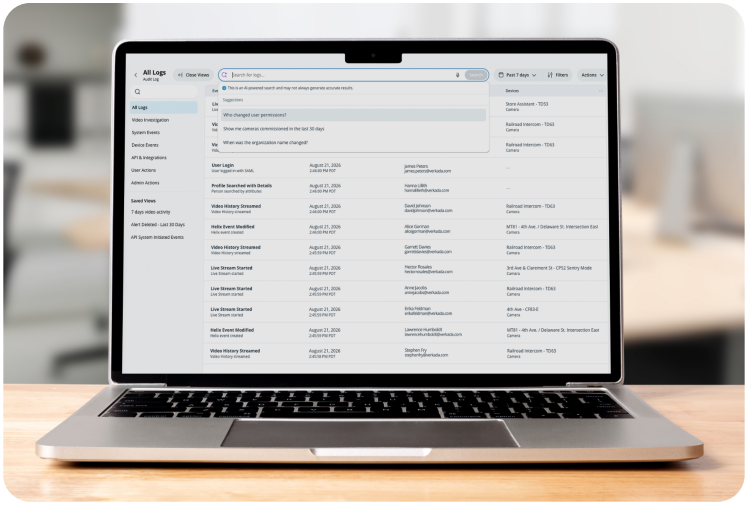
Scan. Review. Contact.
On-site signage gives building occupants immediate visibility into which technologies are active, how data is processed, and who to contact with questions.

PRINCIPLE THREE

Human-in-the-loop and agency

03

Our analytics are designed to support human judgment, not replace it. Key AI and analytics features are intentionally turned off by default, requiring organizations to make deliberate, informed choices about what capabilities to enable. When activated, tools like AI summaries help operators evaluate behavior over time for more contextual decision-making, while biometric access control workflows include built-in consent management options and configurable logging to support compliance record-keeping.



CONSENT GATES

Off by default.

High sensitivity features, such as facial recognition, vehicle history, and audio are disabled out of the box. These sensitive capabilities are “opt-in”, giving organization administrators the flexibility to align their settings and user access controls with their policies prior to activation. Verkada also restricts access to sensitive features, such as facial recognition, in some jurisdictions where prohibited by law (for example, Illinois, City of Portland, OR), further helping organizations align their compliance with local regulations.

Biometric features and data control

BIOMETRIC FEATURES & PROCESSING

AF64 Face Unlock enrollment consent

For organizations using our biometric access station (AF64), entry relies on a dedicated, opt-in enrollment process that enforces strict user consent before biometric processing takes place.

BIOMETRIC FEATURES & PROCESSING

Guest biometric ID verification

Our Workplace visitor kiosk supports a secure biometric check that matches a guest's live face capture to their driver's license photo during check-in, verifying identity in a single step without permanently archiving the biometric record.

BIOMETRIC FEATURES & PROCESSING

Biometric processing (face only)

Biometric capture is processed at the camera edge, rather than in the cloud.

DATA CONTROL

Support access

Verkada's support team does not have access to customer Command organizations unless a customer explicitly issues them a temporary, auto-expiring token to assist with troubleshooting. When a customer enables support team access, they can select the kind of media to share (for example, live video footage, audio, or images), the locations shared down to the site level, and the duration of access. Customers can revoke access at any time.

DATA CONTROL

Siloed archiving & selective sharing

Administrators decide exactly what footage is archived and who can view it. Because customer data is logically separated in dedicated, tenant-isolated cloud environments, it is not pooled or searchable in a shared network.

PRINCIPLE FOUR

Integrity and model quality

04

We systematically build computer vision and analytics tools focused on reliability, performance, and data integrity. Leveraging AWS cloud infrastructure, we deliver high availability and regional redundancy alongside options for extended cloud storage, long-term archival, and detailed system logging. Crucially, we maintain strict model training boundaries: Verkada does not train underlying models on customer video or data unless explicitly requested, or voluntarily donated, by the customer.

SEARCH MODERATION

AI-powered search & alerts moderation

To support responsible use of AI-powered search, queries are moderated to help prevent inappropriate, offensive or biased search terms in real-time.

MODEL TRAINING & INTEGRITY

Model training

Your organization's data is private and is not used to train Verkada's AI models without your explicit, opt-in consent.

MODEL TRAINING & INTEGRITY

No data selling

Verkada does not sell the data customers input into our Command platform.

Your data is yours.

Not pooled. Not sold. Not used to train models without your explicit, opt-in consent.

PRINCIPLE FIVE

Data minimization and privacy controls

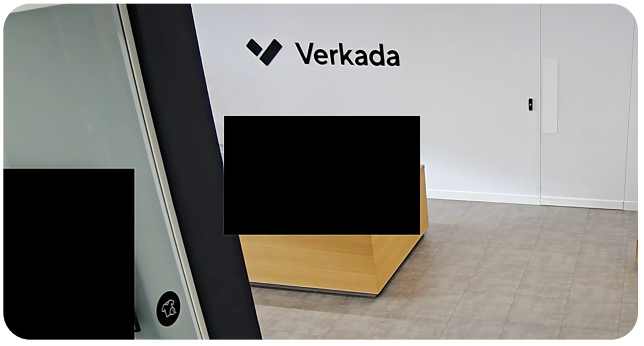
05

Maintaining safety shouldn't require collecting or storing unnecessary personal information. We engineer our platform with granular, customizable privacy settings—including live and recorded face blur, configurable privacy regions to block out sensitive areas, and flexible cloud and device retention schedules—enabling organizations to capture and keep only the data they strictly need, for only as long as they need it.

FEED & FOOTAGE PRIVACY CONTROLS

Granular privacy regions

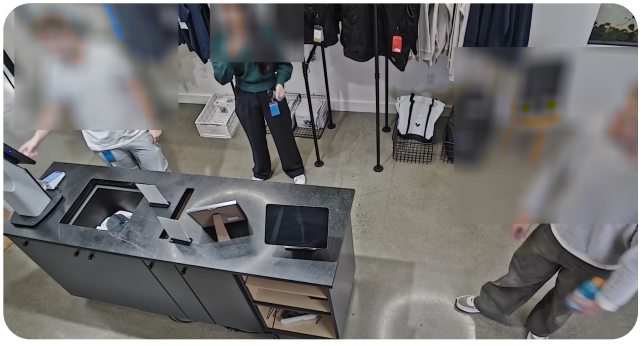
Mask sensitive areas of a camera's field of view so those pixels are never recorded.



FEED & FOOTAGE PRIVACY CONTROLS

Face blurring

Verkada cameras securely record unaltered video footage for use in investigations. However, admins can turn on face blurring on public-facing Verkada VX52 Viewing Stations so operators can monitor physical safety without displaying recognizable faces. When footage is exported, admins can also turn on face blur for individuals in the frame to protect privacy.



Data minimization and privacy controls

DATA RETENTION

- **Granular device-level retention**

  Administrators can set precise video storage windows on a per-camera basis—with hardware options ranging from 30 to 365 days of onboard retention—to help comply with regional data-minimization requirements and specific organizational retention policies.

- **Custom retention and deletion**

  Admins can automatically set their visitor records in Verkada Guest to be deleted after a custom duration to comply with local data-minimization regulations.

- **Biometric data handling**

  If an administrator chooses to opt in and enable person of interest (POI) faces only matching, the biometric data capture happens on the device where it is converted by an algorithm into a mathematical representation and instantaneously wiped from memory if there is no match.

AUDIO/VISUAL CONTROL

- **Continuous streaming (intercoms)**

  Admins can shut off continuous video and audio capture entirely on their Verkada Intercoms, leaving the units active only during direct calls.

- **Alarms temporary muting**

  Admins can temporarily mute a specific camera or sensor's monitoring capabilities for a set period rather than disarming the entire alarm partition, balancing short-term privacy needs and ongoing property security.

ACCESS CONTROL FOR NON-COMMAND USERS

- **Temporary location access**

  Admins can issue time-bounded physical or digital credentials to contractors or visitors without making them a Command user profile. Access can be assigned down to individual doors, ensuring short-term visitors only have access to locations they should.

PRINCIPLE SIX

Robustness, security, and accountability

06

Safeguarding privacy requires maintaining rigorous, independently-verified security controls over the underlying platform. We support our services with role-based access controls, robust encryption standards, and comprehensive audit logs—backed by industry-recognized certifications including ISO 27001, ISO 27017, ISO 27018, ISO 27701, and SOC 2 Type II compliance—to give organizations verified oversight over their security operations.

AUDIT LOG

Robust audit logs

Audit logs are immutable, meaning they cannot be altered by anyone. They collect a complete record of every action taken by users in Command—for example, who viewed a camera, changed a setting, or exported video. These logs can be searched instantly using filters or natural language, and exported as scheduled CSV reports for compliance reviews. Admins can also save pre-filtered, default audit views and schedule recurring CSV reports to be delivered automatically to stakeholders.

LPR search reason and audit

Users are required to enter an offense type and case number before searching or accessing license plate data in Command. The incident information entered is saved directly to an organization's audit log for maximum visibility into who accessed LPR data, when, and for what purpose.



Key certifications

SOC 2

SOC 2 Type 2

PRIVACY IN THE CLOUD

ISO/IEC 27001, 27017/27018

PRIVACY

ISO/27701

EU/SWISS/UK-U.S.

Data Privacy Frameworks

GOVERNMENT-GRADE

FedRAMP® & GovRAMP Moderate authorizations

Verkada has achieved FedRAMP and GovRAMP Authorized status at the Moderate impact level.

GOVERNMENT-GRADE

FIPS-validated products

Verkada offers government-grade hardware and software with FIPS-validated encryption.

HIGH-LEVEL SECURITY AND COMPLIANCE

- Hosted in AWS GovCloud
- TAA Compliant
- FIPS 140 Validated
- SOC 2 Type 2
- FedRAMP® Authorized
- FY2019 NDAA Compliant
- Zero Trust Architecture
- ISO 27001, 27017, 27018, and 27701

CUSTOMER STORIES

See what our customers are saying.

95%

faster incident investigations at Brookfield Community School

City of Las Vegas

Uses Verkada to secure public spaces while maintaining the privacy of private citizens.

Bath Spa University

Leverages role-based access controls to secure sensitive footage and support GDPR compliance across their campuses.

Brookfield Community School

Leverages automated face blurring and cloud-based analytics to protect student privacy while reducing incident investigation times by 95%.

Brighton Grammar School

Uses time-bounded, limited sharing controls in Command to securely share specific video clips with authorized staff and instantly revoke access at will, keeping student well-being and privacy at the forefront.

Lifeview Residential Care

Uses granular Command user permissions to ensure care areas are only monitored by authorized staff—protecting resident dignity, safety, and privacy.

Electric Research and Manufacturing Cooperative, Inc. (ERMCO)

Leverages granular, site-scoped role-based permissions to protect sensitive HR and administrative areas and uses audit logs to trace every platform action back to the individual user.

FREQUENTLY ASKED QUESTIONS

FAQ

Does Verkada share data with law enforcement?

Verkada's customers are the gatekeepers of their data. It is encrypted—they control if, when, and how it is shared with other stakeholders, such as when law enforcement is assisting with an active customer investigation. Verkada gives customers granular, feature-level control over who can access footage, for how long, and how much of it.

> **Time-limited, scoped sharing links.** If a customer chooses to share video security footage with law enforcement, they can generate and send a secure, time-limited link via text or email with a specific live camera feed or an archived clip. The customer sets the link's expiration and can revoke access at any time.

How does Verkada help prevent bias in AI-Search?

We use moderation to help prevent offensive search queries, and intentionally prevent AI-powered searches based on race, ethnicity, or other sensitive demographic information.

How do you help protect against misuse of your technology?

Cloud architecture allows us to build real-time accountability directly into Verkada Command. Unlike traditional systems that rely on shared logins—making it nearly impossible to trace misuse—Verkada Command captures comprehensive audit logs for all user and camera activities, giving administrators full visibility across their organization.





Learn more, visit
verkada.com/trust/privacy

© Copyright 2027 Verkada Inc. All rights reserved.