

CROME TRUST CENTER

Volume I

Privacy Policy

Version 1.0

Effective Date: July 2026

Our Commitment

At Crome, we believe artificial intelligence should enhance safety while respecting privacy, transparency, and human oversight. Our platform is designed to assist—not replace—human decision-making by providing intelligent alerts that help people respond more quickly to potential safety and security events. We are committed to responsible AI development, protecting customer information, minimizing data collection, and giving users meaningful control over their information.

1. Overview

Crome Smart Alerts provides AI-powered video and audio analytics for homes, businesses, healthcare organizations, schools, and enterprise customers. This Privacy Policy explains how information is collected, processed, protected, retained, and deleted. We follow five core principles: Privacy by Design, Data Minimization, User Control, Security, and Transparency.

2. Information We Collect

We may process customer-authorized video streams, audio streams (when enabled), event metadata, account information, camera names, device identifiers, diagnostic logs, and notification preferences. We collect only the information reasonably necessary to operate the requested services.

3. How We Use Information

Customer information is used solely to provide AI-powered Smart Alerts, authenticate users, generate notifications, improve platform reliability, investigate reported issues, provide customer support, detect fraud or abuse, and comply with legal obligations. We do not sell customer personal information.

4. AI Processing

Depending on user configuration, Crome AI may detect smoke, early fire, falls, requests for help, motion, face detection, and optional recognition of user-enrolled known individuals. AI results are advisory and should not replace emergency services or human judgment.

5. Ring Integration

When connected to Ring through an authorized integration, Crome processes only the data necessary to deliver the requested AI functionality. Ring customer data is not used to train Crome AI or machine-learning models.

6. Face Recognition

Known-person recognition is optional. Users choose whether to enroll known individuals. Biometric templates, where used, remain associated only with that customer's account and are not sold or used for unrelated purposes.

7. Data Retention

Information is retained only for as long as necessary to provide the requested service, maintain platform integrity, satisfy legal obligations, resolve disputes, and enforce agreements. Users may request account deletion and associated data removal, subject to applicable law.

8. Sharing Information

We share information only with trusted service providers that help operate the platform, such as cloud hosting, payment processors, and notification providers. These providers are contractually required to protect customer information.

9. Security

Crome employs industry-standard safeguards including encrypted communications, authenticated access, role-based permissions, monitoring, logging, and secure cloud infrastructure.

10. Human Access

Customer information is not routinely reviewed by employees. Access is limited to authorized personnel when necessary for customer support, troubleshooting, security investigations, or legal compliance.

11. Your Privacy Rights

Subject to applicable law, users may request access to, correction of, export of, or deletion of their personal information through Crome Support.

12. Policy Updates

We may periodically update this Privacy Policy. Material updates will be communicated through our website, application, or other appropriate channels.