AirEye Privacy Policy

Effective Date and Last Updated: November 10, 2026

This Privacy Policy describes how AirEye Ltd., an Israeli company ("AirEye", "we", "us" or "our"), collects, uses, discloses, stores and protects Personal Data in connection with our website at https://aireye.tech/ ("Website"), our cloud-hosted wireless-security platform and dashboard, authorized sensors or appliances (including "Halo" sensors), APIs and optional cloud-to-cloud integrations (collectively, the "Service"), and our business operations.

Important distinction: AirEye ordinarily acts as a processor (or service provider under analogous law) when it receives customer-controlled wireless telemetry through AirEye sensors or Customer-authorized integrations with third-party network and wireless-management platforms. The relevant Customer determines the purpose, lawful basis and scope of such processing and is solely responsible for legally required notices and permissions, including any notice required for its Authorized Users, employees, visitors and other individuals whose devices or network activity are monitored. AirEye acts as an independent controller for its own Website, business contacts, recruitment, account administration and legal compliance. Customer-controlled Personal Data is governed primarily by the applicable customer agreement (including the Service Terms and any signed order form or master agreement, the "Agreement") and Data Processing Addendum ("DPA"), including Schedule A to the AirEye Service Terms and Conditions available at https://aireye.tech/terms-and-conditions/ (the "Service Terms"), where applicable. This Policy is a public transparency notice and does not replace those agreements or override statutory privacy rights.

Personal Data means information relating to an identified or identifiable natural person, including identifiers such as names, user IDs, IP addresses or MAC addresses when linked or reasonably linkable to a person. Machine and network information can constitute Personal Data even if collected principally for cybersecurity. Capitalized terms used but not defined in this Policy (such as Customer, Authorized User, Customer Data, Customer Personal Data and Third-Party Integrations) have the meanings given in the Service Terms. "You" includes Website visitors, prospects, job applicants, business contacts, Platform users and individuals whose devices or network activity are processed in a customer-managed deployment, as relevant.

This Policy covers the following use cases:

1. When you browse or visit our Website.
2. When you contact us, request a demo or download materials.
3. When we process job applications.
4. When you use or interact with our Platform/Dashboard, AirEye sensors or customer-enabled integrations with compatible third-party wireless/network-management products.
5. When we meet you at marketing events or receive your business card.
6. When we obtain business contact data from third-party lead sources.
7. When we manage customer and service-provider contacts.
8. When we work with resellers, distributors, agents, technology partners and finders.
9. When you interact with us on social-media channels.

10. When an authorized Customer enables a supported connection to an external wireless-infrastructure, access-point, network or cloud-management provider (for example, Cisco Meraki, HPE Aruba Networking or RUCKUS Networks, where supported). Vendor names are illustrative, not a representation that a particular integration is currently available. Third-party names and trademarks belong to their respective owners, are used for identification only and do not imply endorsement, sponsorship or affiliation.

If we are only a processor of Customer Personal Data, requests about the legality, scope, purposes or retention of that data should ordinarily be directed first to the relevant customer as controller. We will cooperate as legally required. Nothing in this Policy restricts statutory rights or remedies. If you provide us with Personal Data of another person (for example, a colleague, employee or Authorized User), you confirm that you are authorized to do so and that the person has received any notice required by law.

Table of Contents

1. What information we collect, why we collect it, and how it is used
2. How we protect and retain your Personal Data
3. How we share your Personal Data
4. International transfers of Personal Data
5. Your privacy rights and how to delete your account
6. Use by children
7. Interaction with third-party products and integrations
8. Log files
9. Analytic tools, cookies and similar technologies
10. Specific provisions applicable under California privacy law
11. Contact us, changes, acknowledgment and general provisions

1. WHAT INFORMATION WE COLLECT, WHY WE COLLECT IT, AND HOW IT IS USED

The following categories describe our processing at a high level. We process only data relevant to the applicable relationship, licensed features, selected integrations and Customer configuration. The legal bases listed apply only where the GDPR or equivalent legislation requires them; where several bases are listed, the actual basis depends on the specific purpose and circumstances. “Legitimate interests” refers to the particular interests identified in the table, balanced against individual rights where legally required. Customer-controlled Platform telemetry, whether obtained using AirEye sensors or authorized vendor API connections, is ordinarily collected and processed on the Customer’s documented instructions, not on AirEye’s independent direct-marketing legal basis. For the purposes of section 11 of the Israeli Protection of Privacy Law, 5741-1981 (as amended, including by Amendment No. 13): for Personal Data that AirEye collects as controller, you are not under a legal obligation to provide it, and providing it depends on your will and consent, except where a contract or law requires particular information; the consequences of not providing it are described in the “What happens if not provided” column of each table below; the purposes and recipients are described in this Section 1 and in Section 3; the controller is AirEye Ltd., which may be contacted at privacy@aireye.tech; and your rights of access and correction are described in Section 5.

aireye

i. When you browse or visit our Website

Specific Personal Data we collect	Why we collect and use it	Legal basis (GDPR / where applicable)	Recipients / provider categories	What happens if not provided
IP address; browser/device characteristics; general location derived from IP; visit timestamps; requested pages; referral URLs; cookie and similar identifiers; consent preferences; diagnostics and security logs.	Operate and secure the Website; prevent misuse; remember privacy choices; measure performance and improve content; optional analytics or advertising only when lawfully enabled.	Legitimate interests or legal obligation for strictly necessary security/administration; consent for non-essential storage/access and related personal-data use where required.	Website hosting/CDN/security vendors; analytics and marketing providers where active and lawfully enabled (including Google, HubSpot and Cloudflare where relevant to the functions used).	Essential functions may be unavailable if required technology is blocked; non-essential analytics/marketing can ordinarily be declined without losing core Website access.

ii. When you contact us, book a demo or download content

Specific Personal Data we collect	Why we collect and use it	Legal basis (GDPR / where applicable)	Recipients / provider categories	What happens if not provided
Name; business email; employer; role; telephone; message and attachments; demo/product interests; related correspondence and lead activity.	Reply to inquiries; arrange product demonstrations; deliver requested content; manage sales conversations; maintain records; send lawful communications according to your preferences.	Pre-contractual steps where you are personally party to a contract; legitimate interests in responding and commercial relationship management; consent where required for particular marketing.	Email and productivity providers; CRM, marketing and customer-support providers; representatives assisting with the relevant request.	Without requested contact details we may be unable to reply, arrange a demo or send materials.

iii. When we process your job application

Specific Personal Data we collect	Why we collect and use it	Legal basis (GDPR / where applicable)	Recipients / provider categories	What happens if not provided
Name; contact details; employment and education history; CV and cover letter; references provided; interview correspondence; assessment information reasonably necessary for recruiting.	Review qualifications; communicate with applicants; make recruitment decisions; maintain lawful recruitment and compliance records.	Pre-contractual steps, legitimate interests in selecting personnel, legal obligations, or consent where independently required.	Authorized hiring managers, recruiters and business productivity/storage vendors; legal advisers where needed.	We may be unable to assess or pursue an application without sufficient information.

iv. When you use or interact with the Platform/Dashboard

Specific Personal Data we collect	Why we collect and use it	Legal basis (GDPR / where applicable)	Recipients / provider categories	What happens if not provided
Customer/company name; authorized user name, email, user ID, employee number where provided, role, authentication and access records, account settings and technical support messages.	Create and administer accounts; authenticate users; authorize access; provide support, billing and security; maintain audit records; deliver requested Platform functions.	For our controller-side operational records: legitimate interests, performance of contract where applicable, legal obligations; for customer user data processed on customer instructions: Customer determines applicable lawful basis.	Authorized customer administrators and contracted hosting, cloud infrastructure, security, logging, identity and support providers (which may include AWS, database and content-delivery vendors depending on the Service configuration).	Some identifiers and login records are required for an operational, secure user account; optional profile fields need not always be supplied.

v. When you attend marketing events or share a business card

Specific Personal Data we collect	Why we collect and use it	Legal basis (GDPR / where applicable)	Recipients / provider categories	What happens if not provided
Name; company; business contact details; job title; event name; correspondence; professional interests you choose to share.	Follow up on discussions; evaluate business relationships; arrange meetings; send marketing where permitted.	Legitimate interests in professional networking and B2B relationship development; consent where marketing law requires.	Event organizers where relevant; approved CRM/email/marketing providers.	Without contact details we may not be able to follow up.

vi. When we obtain contact data from third-party lead sources

Specific Personal Data we collect	Why we collect and use it	Legal basis (GDPR / where applicable)	Recipients / provider categories	What happens if not provided
Business name, role, corporate email, phone, organization, public professional profile, source and relevant marketing preferences.	Identify potential business customers; conduct proportionate B2B outreach; verify business relevance; honor objections/opt-outs.	Legitimate interests where permitted and balanced; consent or another lawful basis where required; direct-marketing rules apply independently.	Professional databases and lead providers (which may include LeadIQ where used), CRM and outreach providers; appropriate affiliates or partners.	Providing such data is generally not required of the individual; you may object or opt out as applicable.

vii. When we use Personal Data of customers and service providers

Specific Personal Data we collect	Why we collect and use it	Legal basis (GDPR / where applicable)	Recipients / provider categories	What happens if not provided
Professional name; employer; role; contact details; contracts; procurement, billing and payment-related records; correspondence.	Manage supply and customer relationships; deliver contracted services; handle invoicing, compliance, support, payment and disputes.	Legitimate interests in relationship management; legal obligations; performance of a contract where applicable.	Contracted finance, legal, accounting, mail, CRM and service-delivery processors and relevant customer/provider personnel.	Failure to provide necessary business contact or billing information may prevent normal commercial performance.

viii. When we work with resellers, distributors, agents, partners and finders

Specific Personal Data we collect	Why we collect and use it	Legal basis (GDPR / where applicable)	Recipients / provider categories	What happens if not provided
Professional contact and organizational data; commercial terms; referral/sales activities; contractual, payment and diligence records.	Manage partner onboarding, channel relationships, payments, compliance, training and opportunity coordination.	Legitimate interests; contractual necessity where applicable; legal obligations.	Authorized channel management personnel, payment/finance providers, legal advisers and operational service providers.	We may be unable to evaluate or maintain a relevant commercial partnership.

ix. When you interact with our social-media profiles

Specific Personal Data we collect	Why we collect and use it	Legal basis (GDPR / where applicable)	Recipients / provider categories	What happens if not provided
Public profile details; your messages, comments and reactions; any information you choose to share; limited interaction metrics provided by the platform.	Respond to questions; administer our presence; measure engagement; manage legitimate business communications.	Legitimate interests in responding and maintaining a professional presence; consent where legally required.	Social-media platform operators (such as LinkedIn, Facebook, YouTube or X where AirEye maintains a presence) and communications providers.	We may be unable to respond if you do not provide a way to contact you.

x. Sensor-based wireless security monitoring (Customer-controlled)

Specific Personal Data we collect	Why we collect and use it	Legal basis (GDPR / where applicable)	Recipients / provider categories	What happens if not provided
MAC addresses; device name, vendor, operating system/model when detectable; network names (SSID/ESSID); AP and device associations; connection and event metadata; wireless-security findings; technical identifiers and timestamps; IP or user association only where available or configured.	Provide authorized wireless visibility, classification, correlation, security monitoring, alerts, analysis, forensics and enabled response functions; maintain service diagnostics.	Customer determines the purpose, lawful basis, employee/visitor notice and monitoring permissions; AirEye ordinarily acts as processor under the Agreement/DPA.	Customer-authorized users; AirEye operational/subprocessor personnel on need-to-know basis; contracted hosting, logging and security subprocessors.	Some telemetry is necessary for selected features; disabling sensors or reducing permissions can limit coverage and functionality.

xi. Optional third-party wireless, network and cloud-management integrations (Customer-controlled)

Specific Personal Data we collect	Why we collect and use it	Legal basis (GDPR / where applicable)	Recipients / provider categories	What happens if not provided
When Customer enables a supported vendor connection through an API key, OAuth token, service account, webhook or equivalent authorization, relevant data may include device and access-point inventories; MAC and IP addresses; SSIDs; names, vendor/model/firmware and configuration metadata; connection and association histories; assigned user identifiers (such as username, business email, employee number or name); network events, alerts, timestamps, performance/usage statistics and security metadata. Actual fields depend on vendor API, scopes and settings; not all are collected in each integration.	Support wireless visibility, correlate inventory and client associations, analyze security events and threats, generate alerts, investigate incidents and, if expressly enabled, perform authorized response functions. Data retrieval follows the Customer-selected features and effective permission scopes. Routine metadata integrations do not require unrestricted capture of communications content.	The relevant Customer ordinarily determines the lawful basis, purposes, necessity, permissions and employee/visitor notices and enables the connection on documented instructions; AirEye ordinarily processes Customer Personal Data as processor under the Agreement/DPA. AirEye's separate use as controller, if any, requires its own lawful basis.	Customer-appointed vendor platform and its API operators (which do not automatically become AirEye subprocessors); AirEye-authorized hosting, security and support subprocessors as needed. Authentication secrets are treated as sensitive security credentials. Sharing is limited by customer-selected permissions and applicable contracts.	Integrations are optional and available only where supported. Declining or revoking access limits the related enrichment or response functions but does not necessarily affect separately supported sensor-based capabilities. Previously received records remain subject to the Agreement/DPA retention rules.

Additional use and limitations

AirEye may process information when reasonably necessary to detect and prevent fraud or abuse; investigate security incidents; meet legal obligations; answer regulators; protect legal claims; enforce contracts; operate the business; and maintain reasonable audit trails. We may produce security statistics, research and generalized threat intelligence from appropriately aggregated or effectively de-identified data only where it cannot reasonably identify Customer or individuals or disclose Customer Confidential Information, consistently with the Service Terms and DPA. Such aggregated or de-identified information is not Personal Data, and AirEye may use it to operate, develop, train and improve its detection models and Services. We do not treat merely pseudonymized device identifiers as anonymous.

We do not intentionally use Customer-controlled wireless telemetry for unrelated advertising or disclose identifiable Customer Personal Data to external advertisers as an ordinary part of the Service. Changes to these processing purposes require an appropriate legal basis, transparency, and any Customer authorization required by the Agreement and law. AirEye may use technical automation, rule-based correlation or machine learning to generate potential security findings; automated alerts are not a representation that any individual has engaged in misconduct. Material decisions about individuals should be reviewed by the Customer, which is solely responsible for any such decision and for compliance with its own legal obligations, as set out in the AirEye Service Terms and Conditions.

2. HOW WE PROTECT AND RETAIN YOUR PERSONAL DATA

2.1 Security

We apply technical and organizational measures intended to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure and access, appropriate to the nature of the data and risks involved. Such measures may include role-based access controls, authentication, encryption in transit and at rest where appropriate, logging, access reviews, segregation and incident response. The actual commitments for Customer Personal Data are set out in the applicable Agreement and DPA; this public notice does not replace negotiated security terms, and the measures described are examples that vary according to the nature of the data and the Service configuration. No internet-based service or electronic storage method can guarantee absolute security. Customers remain responsible for protecting their own devices, user permissions, network environments and credentials. To the maximum extent permitted by law, AirEye is not responsible for unauthorized access resulting from the compromise of credentials held by a Customer or its users, from a Customer's configuration choices, or from other circumstances beyond AirEye's reasonable control. Please notify us promptly at privacy@aireye.tech if you suspect that your account credentials have been compromised.

2.2 Retention

We retain controller-side Personal Data for as long as reasonably necessary for its stated purposes, taking account of the duration of the business relationship, the individual's preferences, legal retention and limitation periods, security and fraud-prevention needs, record integrity and dispute preservation. We periodically review records and delete or de-identify them when no longer required. Marketing contact data is retained only while necessary for lawful outreach or suppression of further messages following opt-out. Job applications are retained for recruitment and reasonable legal-compliance periods depending on jurisdiction. Operational account, acceptance and security logs may be retained for audit and evidentiary reasons proportionate to the applicable need. We may also retain records reasonably required to establish, exercise or defend legal claims for the applicable limitation period (under Israeli law, generally seven years under the Prescription Law, 5718-1958), and for any longer period required by law, a legal hold or a pending dispute.

Customer Personal Data is retained and returned or deleted in accordance with Customer's instructions, the Agreement, applicable DPA, the selected product settings and mandatory law. Under Section 21.3 of the AirEye Service Terms and Conditions, unless a higher-priority agreement specifies otherwise, a Customer may request export of then-available Customer Data within 30 days after termination; statutory personal-data deletion/return obligations remain governed by the DPA and applicable law, not by that request window. Residual restricted backup copies may persist until ordinary rotation or legally required deletion deadlines. We do not promise immediate deletion of all copies when law or secure backup design requires a controlled process.

2.3 Security incidents

We assess incidents in accordance with applicable law and the commitments applicable to our role. Where we are the processor of Customer Personal Data, we inform and assist the relevant Customer in accordance with the DPA and mandatory requirements. Where we are the controller, we will notify competent authorities and affected individuals when required by law. Report concerns to privacy@aireye.tech or contact@aireye.tech.

Product-security reporting is separate from Personal Data breach reporting. Where AirEye is subject to a mandatory cybersecurity product-reporting regime (including the EU Cyber Resilience Act for a product in scope), AirEye assesses and reports qualifying product vulnerabilities and security incidents according to that regime. The applicable triggers and timelines depend on the event, product, market and legal role; this Privacy Policy neither creates a contractual reporting deadline nor limits mandatory regulatory notification duties.

3. HOW WE SHARE YOUR PERSONAL DATA

Depending on the use case, Personal Data may be disclosed only as appropriate to: (a) authorized AirEye staff and affiliates; (b) contracted cloud hosting, content delivery, infrastructure, identity, logging, cybersecurity, communications, CRM, analytics, recruiting, finance or support providers; (c) Customer-designated administrators and Customer-selected external network-management or integration providers, where required to operate an expressly enabled connection; (d) professional advisers, auditors, insurers and lawful counterparties bound by appropriate duties; (e) government authorities, regulators, law enforcement or courts, where lawfully required or where we reasonably believe disclosure is necessary to comply with law or legal process, enforce our agreements, or protect the rights, property, security or safety of AirEye, our Customers, users or others; and (f) investors, prospective acquirers or successors in connection with confidential due diligence, restructuring, financing, asset sales, mergers or other corporate transactions (including in connection with insolvency or receivership proceedings), subject to applicable legal safeguards and contracts. A vendor platform already chosen and operated by the Customer is not automatically AirEye's subprocessor solely because an integration accesses that Customer account. We require our own processors/subprocessors to protect data as required by law and our contracts and do not grant unrestricted commercial exploitation rights in Customer Personal Data.

For example, the categories above may involve providers of business productivity, hosting, cloud infrastructure, security, analytics and marketing solutions, depending on the applicable Service configuration and functions (such as AWS, Google Workspace, Cloudflare, HubSpot, Salesforce or SalesLoft where used). We may change providers while maintaining legally required contractual safeguards, notice and choice. You may contact us for further information about material Service subprocessors, subject to reasonable confidentiality and security restrictions. Named providers are illustrative examples and not a representation that each is in use at any given time.

We may share effectively de-identified, aggregated statistics only consistently with the commitments described above and with applicable law. We do not disclose Customer-controlled wireless telemetry for third-party direct advertising without an independent, legally valid basis and any required Customer instruction.

4. ADDITIONAL INFORMATION REGARDING INTERNATIONAL TRANSFERS OF PERSONAL DATA

4.1 Storage and access. AirEye is established in Israel. Depending on the product, contract, infrastructure architecture and provider, information may be processed in Israel, the United States, the EEA/UK and other permitted locations, including remotely by authorized support personnel. Some Service data may be hosted using cloud providers such as AWS. AirEye does not promise a particular hosting location in this general notice; any binding data-residency or localization commitment must be expressly specified in the relevant customer agreement or DPA.

4.2 Safeguards. Where the GDPR/UK GDPR applies, transfers outside the EEA/UK use an applicable adequacy decision (including the EU recognition of Israel, where relevant), a valid EU/UK transfer mechanism such as Standard Contractual Clauses/UK Addendum when required, or another lawful derogation or safeguard. A Customer's signed DPA and any applicable SCCs govern processor-to-subprocessor transfers where legally required. We implement reasonable supplementary safeguards as required by the transfer assessment. Transfers from Israel are also subject to applicable Israeli cross-border data-transfer requirements, including the Protection of Privacy (Transfer of Data to Databases Abroad) Regulations, 5761-2001, and AirEye relies on the bases permitted under those regulations as appropriate to each transfer.

4.3 Rights and questions. Where required, you may request information about applicable transfer safeguards at privacy@aireye.tech, subject to proportionate redactions of confidential security details.

5. YOUR PRIVACY RIGHTS. HOW TO DELETE YOUR ACCOUNT

Subject to your location and applicable law, you may have rights to access and receive a copy of Personal Data; correct inaccurate information; request erasure; restrict or object to certain processing (including direct marketing); request portability; withdraw consent without affecting prior lawful processing; and lodge a complaint with an applicable supervisory authority. Other rights, including opt-outs relating to profiling, sale/sharing or certain automated decisions, may apply in particular jurisdictions. Not all rights apply to every data item, processing activity or individual; lawful exemptions and verification safeguards may apply. Where Israeli law applies, you may have the right to review Personal Data held about you and to request its correction or deletion under sections 13–14 of the Israeli Protection of Privacy Law, 5741-1981, and to lodge a complaint with the Israeli Privacy Protection Authority.

To exercise rights concerning AirEye as controller, email privacy@aireye.tech and describe your request. We may request proportionate verification and will respond within the timeframe required by applicable law. Where permitted by law, we may decline or charge a reasonable fee for requests that are manifestly unfounded, excessive or repetitive, and we may retain the minimum information necessary to record how a request was handled and to honor opt-outs. An authorized agent may act where permitted and properly verified. Requests concerning Customer Personal Data should ordinarily go to the relevant organization controlling the monitored environment; we will forward or assist where appropriate and permissible, subject to confidentiality and the DPA. We cannot independently delete records held for Customer where the Customer, rather than AirEye, controls the retention decision, except where the law requires otherwise.

To close an individual Platform account, contact the relevant Customer administrator or contact@aireye.tech. Closing a user account does not automatically terminate the Customer's subscription or compel immediate deletion of independently required logs or records. Data return and deletion follow the applicable DPA and Section 21 of the Service Terms, including any higher-priority agreement.

We respect objections to lawful direct marketing and provide unsubscribe mechanisms where applicable, including as required by section 30A of the Israeli Communications (Telecommunications and Broadcasting) Law, 5742-1982. You may withdraw consent to optional cookies at any time, separately from acceptance of the Service Terms, through the cookie settings described in our Cookies Policy at https://aireye.tech/cookie-policy/. The act of accepting the Service Terms is not blanket consent to optional cookies, unrelated marketing, employee monitoring or other third-party monitoring.

6. USE BY CHILDREN

The Website and Service are intended for adult professionals and enterprise customers. The Service Terms restrict users to persons at least 18 years old. We do not knowingly invite children to create accounts or solicit their Personal Data for our own marketing. Wireless telemetry generated by lawful customer deployments may incidentally relate to minors in environments managed by the relevant Customer; in that case the Customer is responsible for appropriate notices, legal bases and any special safeguards, and AirEye acts subject to the DPA. If we learn that we have collected Personal Data of a minor as controller without a lawful basis, we will take reasonable steps to delete it. If you believe we unlawfully hold a child's data, contact privacy@aireye.tech.

7. INTERACTION WITH THIRD-PARTY PRODUCTS AND INTEGRATIONS

Customers may enable supported Third-Party Integrations with external wireless infrastructure, network-management, cloud-management, identity or security platforms, using appropriately authorized API keys, OAuth grants, service accounts, webhooks, event feeds or comparable mechanisms. Depending on the selected provider, available features and customer-granted access scopes, AirEye may receive or retrieve device names and types, MAC/IP addresses, network and access-point identifiers, Wi-Fi-enabled asset inventory, SSIDs, connection and client associations, assigned identities (including usernames, employee numbers, business email addresses or names), event logs, alerts, status, timestamps, configuration and other technical security or performance metadata. The precise information varies: listing a category does not mean every supported integration collects it, and an example vendor is not a promise of integration availability. Routine metadata-based integration does not itself authorize AirEye to inspect private communication contents or to access the whole vendor tenant indiscriminately.

Customers decide which available integration to enable, which account/tenant to connect, and which lawful permissions to grant. Customers must hold necessary rights, comply with vendor terms, provide legally required employee, visitor or user notices, and ensure an appropriate legal basis. Customers should apply least-privilege access, securely administer, rotate and revoke credentials, and review enabled scopes and any permitted write or remediation actions. AirEye treats received API credentials or tokens as security-sensitive and uses them only for documented, authorized Service functions, subject to the Agreement, DPA and its own security obligations. Vendor providers control their own platforms and privacy practices; their product terms, availability and APIs may change. Once a connection is disabled, further collection by that connection ordinarily ceases after necessary technical processes, while data already lawfully received remains subject to the applicable retention/deletion rules. Changes that would materially expand data collection or uses require appropriate notice, lawful basis and any Customer authorization required by contract or law. AirEye is not responsible for the privacy, security or data practices of third-party vendors, platforms or websites that a Customer chooses to connect or that are linked from our Website; their processing is governed by their own terms and policies.

8. LOG FILES

We use Website and Service logs for authentication, reliability, abuse prevention, operational monitoring, performance diagnostics, auditability and security investigation. Logs may include IP addresses, timestamps, account identifiers, browser/user-agent details, integration events, system actions and error information. Some logs form part of Customer Personal Data and are governed by the DPA; others are retained by AirEye as controller for its own lawful security, contract-management and compliance purposes. Access to logs is restricted as appropriate.

9. ANALYTIC TOOLS, COOKIES AND SIMILAR TECHNOLOGIES

The Website may use strictly necessary technologies, functional preferences, analytics and marketing/advertising technologies, including web beacons, tracking pixels and tools operated by third parties. Analytics and marketing technologies may include tools offered by Google, HubSpot, SalesLoft or other providers depending on the current Website configuration. Where law requires prior consent, we use reasonable efforts to ensure that non-essential technologies are activated only after you have given consent for the relevant category through our cookie settings. We honor consent withdrawal in accordance with applicable law and present rights and choices in our Cookies Policy at https://aireye.tech/cookie-policy/.

Our Cookies Policy explains categories and gives examples of technologies that may be used for the stated purposes. Cookie settings are separate from acceptance of the Service Terms. Some providers may process usage data under their own terms; see their current privacy disclosures. We may add, replace or remove analytical and similar technologies from time to time, subject to applicable notice and consent requirements.

10. SPECIFIC PROVISIONS APPLICABLE UNDER CALIFORNIA PRIVACY LAW

10.1 Scope. This section applies only to California residents to the extent AirEye is a "business" or otherwise subject to relevant California privacy law. It does not assume that every instance of Customer Personal Data makes AirEye an independent business; when we act as a "service provider" or "contractor" to a Customer, our restricted processing duties and the Customer's rights-response role are governed by the relevant law and agreement.

10.2 Categories and sources. Depending on the individual and service, the categories collected in the preceding 12 months may include identifiers; commercial and professional information; internet/electronic network activity; approximate geolocation inferred from network data; inferences concerning potential cybersecurity risks; and personnel/application information. Sources include individuals, employers/customers, sensors, configured cloud APIs, device/network systems, service providers, professional directories and public business profiles. Purposes, recipient categories and retention criteria are detailed in Sections 1–4 above. We do not deliberately request sensitive categories beyond what is necessary for an authorized service or applicable legal obligation.

10.3 Applicable rights. Where statutory thresholds and definitions are met, California residents may request access/knowledge, correction, deletion, portability, limits on certain uses of sensitive Personal Information, and opt-out of any sale or sharing for cross-context behavioral advertising; they may exercise rights free from unlawful discrimination or retaliation. We will assess and honor valid opt-out preference signals, including Global Privacy Control (GPC), in contexts in which applicable law requires recognition. Some advertising or measurement technologies may qualify as "sharing" even when no money changes hands; where such technologies are enabled on the Website, the related opt-out choices are described in our Cookies Policy. We do not characterize the processing of Customer-controlled wireless security telemetry as an unrestricted advertising sale.

10.4 Requests and contact. Email privacy@aireye.tech with a sufficiently specific California privacy request. Where applicable, additional Website notices and opt-out methods may be made available in conjunction with relevant collection or advertising activities. We will verify and process requests and authorized-agent submissions as required by law. Shine the Light requests, to the extent applicable, may be submitted using the same contact.

10.5 Automated processes. AirEye may use automation to flag potential wireless risks, but AirEye does not itself use automated decision-making technology to make legally significant employment, credit or other decisions about individuals; any such decision is made by the relevant Customer, as described in Section 1 (Additional use and limitations). If this changes, we will update this Policy and provide any additional notices and rights required by law.

10.6 California disclosures and opt-out implementation. To the extent the CCPA/CPRA applies to AirEye as a business, additional disclosures, rights fulfillment methods and any required links or controls for sale/sharing or sensitive-data use are made available where required by law. The categories of Personal Data, recipient categories, purposes and retention criteria relevant to any such sale or sharing are described in Sections 1–3 of this Policy and in our Cookies Policy. Where applicable, you may opt out through the cookie settings described in our Cookies Policy or by emailing privacy@aireye.tech, and we treat qualifying opt-out preference signals as described in Section 10.3.

11. CONTACT US, CHANGES, ACKNOWLEDGMENT AND GENERAL PROVISIONS

11.1 Contact. AirEye Ltd. | Website: https://aireye.tech/ | Privacy requests: privacy@aireye.tech | General / contract inquiries: contact@aireye.tech. If a particular jurisdiction requires an additional local representative or data-protection officer, legally required contact details will be provided when the relevant appointment or requirement applies. For questions relating to Customer Personal Data, please also contact the organization responsible for the relevant monitored network.

11.2 Changes. We may update this Policy to reflect changes in products, integrations, infrastructure, business operations or law. We will post the revised notice at https://aireye.tech/aireye-privacy-policy/ with a new Last Updated date and, where legally required, provide additional or advance notice or obtain fresh consent before a materially changed use of Personal Data. Revised notice language does not amend any signed agreement with a Customer. The Cookies Policy at https://aireye.tech/cookie-policy/ and the AirEye Service Terms and Conditions at https://aireye.tech/terms-and-conditions/ (including Schedule A DPA, where applicable) should be read together with this Policy but remain distinct documents with their respective purposes.

11.3 Notice and acknowledgment. Where AirEye asks you to confirm that you have read this Policy or an updated version of it (for example, by checking a box when you log in to the Platform or accept the AirEye Service Terms and Conditions), that confirmation records that this notice, including the information required under section 11 of the Israeli Protection of Privacy Law, 5741-1981, was made available to you. It is not consent to processing for which applicable law requires separate and specific consent, such as non-essential cookies or direct marketing, which we request separately where required. An updated Policy applies from its Last Updated date to the extent permitted by law. Where we request acknowledgment of a material change, AirEye may restrict access to the Platform until it is given, consistent with Section 29 of the AirEye Service Terms and Conditions. AirEye may keep a record of each acknowledgment, including the Policy version, date, time and account, as evidence that notice was provided. To the extent permitted by applicable law, your confirmation, or your continued use of the Website or the Service after the Last Updated date of a revised Policy, also constitutes your acknowledgment of the revised Policy and your consent to the processing described in it for which consent is a valid basis and separate consent is not required.

11.4 Customer responsibilities. Each Customer that deploys the Service is responsible for making this Policy, or an equivalent notice, available to its Authorized Users and, where required by law, to employees, visitors and other individuals whose devices or network activity are monitored, and for obtaining any consent or authorization that such processing requires. As between AirEye and a Customer, responsibility for Customer-controlled processing, including the Customer's indemnity obligations, is governed by the AirEye Service Terms and Conditions (including Sections 7, 10 and 24) and any signed DPA.

11.5 Relationship with other documents. This Policy is a notice and does not form part of, or amend, any contract. If this Policy and the AirEye Service Terms and Conditions or a signed DPA describe the same processing differently, the Service Terms and the DPA govern the contractual relationship between AirEye and the Customer, and this Policy governs the information provided to individuals. Cookies and similar technologies are addressed in more detail in the Cookies Policy. Nothing in this Policy creates any warranty or third-party beneficiary right or limits any right that individuals have under mandatory law.

11.6 Limitation of liability. To the maximum extent permitted by applicable law, AirEye's liability to a Customer and its Authorized Users in connection with the processing described in this Policy is subject to the limitations and exclusions of liability in the AirEye Service Terms and Conditions or the applicable signed agreement. This Section does not limit liability that cannot be limited under applicable law, or any right of individuals under mandatory data-protection law.

11.7 Governing law. Unless mandatory law provides otherwise, this Policy is governed by the laws of the State of Israel, and any dispute relating to it is subject to Section 31 of the AirEye Service Terms and Conditions. This does not affect your right to lodge a complaint with the Israeli Privacy Protection Authority or another competent supervisory authority, or to bring proceedings where mandatory law gives you that right.

11.8 Language. This Policy is drafted in English. Any translation is provided for convenience only, and the English version prevails in case of inconsistency, except where applicable law requires otherwise.