PRIVACY & DATA PROTECTION

# Privacy Policy

We are committed to protecting your privacy and personal information. This policy explains how we collect, use, share and safeguard information when you visit our website, contact us, or use our products and services.

**Effective Date:** October 28, 2026
**Last Updated:** November 1, 2026

## 01 Who We Are

In this policy, “AIOT”, “we”, “us” and “our” refer to AIOT Technologies, including AIOT Technology Private Limited, a company incorporated in India (Corporate Identification Number U72900TG2020PTC139031), and its operations in Canada.

We provide artificial intelligence (AI) and Internet of Things (IoT) consulting, design, development, integration, implementation, testing, analytics, automation, cloud and related technology services. Our website is www.aiotcorp.com.

We use personal information only for the purposes described in this policy, in a product-specific notice, in an applicable contract, or as otherwise permitted or required by law.

## 02 Scope and Our Role

This policy covers our corporate website, business communications, recruitment activities, and AIOT-operated products or services that link to it. A customer application, device, website or platform that we build or operate may have an additional privacy notice describing its particular features and data practices.

> **Important for business customers:** When AIOT processes personal information on behalf of a customer to deliver an AI, IoT, software or managed service, the customer generally determines the purposes and means of processing. In those cases, the customer’s privacy notice and the applicable contract or data-processing terms also govern that information.

- **When AIOT decides why and how personal information is handled** (for example, website enquiries, recruitment or business administration), we are the organization responsible for that information under the privacy laws that apply.
- **When AIOT processes information for a customer** (for example, hosting an IoT solution, supporting an AI application or operating a customer workflow), we act on the customer’s documented

instructions and contract. The customer is responsible for its own notices, instructions and permissions where required by law.

- **Health information:** where we handle protected health information for a U.S. healthcare customer, we do so only under a Business Associate Agreement as required by the Health Insurance Portability and Accountability Act (HIPAA). Where we handle personal health information for a Canadian healthcare customer, we follow that customer's instructions and the applicable provincial health-information law.
- **When a customer or another provider independently operates an app or service**, that organization may have its own privacy policy and is responsible for the practices it controls.

## 03 Information We Handle

The information we handle depends on how you interact with AIOT and the particular service. We aim to collect only the information reasonably necessary for the purpose we have disclosed.

### Information you provide

- Business contact details, such as name, business email, telephone number, employer, role and company details.
- Enquiries, messages, meeting requests, feedback, survey responses and information you include in correspondence, including messages sent through our website contact form.
- Recruitment information, such as a CV or résumé, employment history, qualifications and information provided during recruitment.
- Account, support, project and billing information needed to establish or provide a service, where applicable.

### Website and technical information

- Device and browser type, operating system, IP address, timestamps, pages viewed, referring pages, interactions, error and diagnostic logs, and similar technical information.
- Cookies, analytics identifiers and related online information, where the website technology and your choices permit collection.

### AI and IoT service information

Depending on the project or product, this may include prompts and content submitted to an AI system, generated outputs, files, images, audio or video, device identifiers, sensor readings, telemetry, timestamps, equipment status, diagnostics, location or usage data. Some of this information may relate to an identifiable person. The applicable product notice, customer configuration or contract identifies the specific data involved.

### Sensitive or regulated information

We do not require sensitive personal information for ordinary website browsing, and we ask that you do not send it through our contact form. A specific service may process sensitive information, such as precise location, biometric, health, financial or identity information, only where the service requires it and the applicable permissions, notices, safeguards, contractual instructions and legal requirements are in place.

## 04 How We Use Information

Depending on the context, we may use information to:

- Respond to enquiries, prepare proposals, manage business relationships and provide customer support.
- Deliver, configure, operate, secure, troubleshoot and maintain contracted AI, IoT, software and related services.
- Process device data, user inputs and outputs to provide requested service functionality and generate requested analytics or insights.
- Manage recruitment, supplier relationships, billing, records and business administration.
- Monitor reliability, investigate errors, prevent fraud or misuse, protect systems, and comply with legal obligations.
- Understand and improve our website and services using appropriate analytics and feedback.

Where applicable law requires a legal basis or consent, we rely on the basis appropriate to the activity. This may include your consent, performance of a contract, compliance with a legal obligation, or legitimate interests that are not overridden by your rights. We provide additional information or obtain consent when the law requires it.

## 05 AI and IoT Services

Our AI services may include machine learning, generative AI, computer vision, natural-language processing, prediction, analytics and automation. Our IoT services may connect devices, sensors, gateways, edge systems and cloud platforms to collect or process operational data.

- **Service delivery:** inputs, device data and outputs are processed to deliver the functionality requested by the customer or end user.
- **Model providers:** if a service uses a third-party AI model or API, relevant inputs may be sent to that provider to generate a result. The provider, data categories, purpose, retention and available controls are described in the service-specific notice or customer documentation.
- **Model training:** by default, AIOT does not use customer confidential information, prompts, source code or customer-provided datasets to train general-purpose AI models without the customer’s written authorization.

- **Human review:** authorized personnel may access relevant data where necessary for support, safety, quality assurance, incident investigation or other disclosed service purposes, subject to access restrictions and contract.
- **AI outputs:** AI-generated or automated outputs can be incomplete or inaccurate and may require human review, particularly for consequential decisions. Any service that uses AI for decisions affecting individuals provides additional disclosures and safeguards appropriate to that use.
- **IoT telemetry:** device readings and operational telemetry may be used to provide monitoring, diagnostics, alerts, predictive maintenance and analytics as defined by the product or customer configuration.

Specific data flows and responsibilities are determined by the relevant service, technical configuration and customer agreement. A service-specific notice or agreement supplements this policy where needed.

## 06 Cookies and Analytics

Our website uses a small number of strictly necessary browser storage items, for example to remember your light or dark display preference and your cookie choice. These do not identify you and are not shared.

**Analytics (optional, only with your consent).** With your permission we use Google Analytics 4 to understand, in aggregate, which pages and services are useful and how visitors move through the site (for example, pages viewed, buttons clicked, scroll depth, device type and approximate country). Google Analytics is not loaded at all until you click “Accept analytics”. We have turned off advertising features, Google signals and ad personalization, and we never send your name, email, phone number or the text of your messages to Google Analytics. Google Analytics does not store full IP addresses. Analytics data is retained for up to 14 months. Google acts as our service provider, and data may be processed in the United States.

You can accept or decline analytics in the banner and change your choice at any time using **Cookie settings** in the website footer. Declining removes our analytics cookies. You can also block cookies in your browser.

**Security and server logs.** Like most websites, our hosting provider (Amazon Web Services) records standard technical logs, such as the requested page, time, IP address and browser type, to keep the site secure, prevent abuse and measure automated (bot) traffic in aggregate. We rely on our legitimate interest in operating a secure website for this processing and keep these logs for a limited period.

We do not use advertising or cross-site tracking technologies. If that changes, we will update this policy and ask for any consent the law requires.

## 07 Sharing and Transfers

We may disclose information, where necessary and appropriate, to:

- Cloud hosting, infrastructure, database, cybersecurity, IoT connectivity and device-management providers.
- AI model or API providers, analytics services, customer support systems and other technology vendors used to provide a service.
- Professional advisers, auditors, insurers and business service providers subject to appropriate confidentiality obligations.
- Customers, users or administrators authorized to receive the information as part of the relevant service.
- Regulators, courts, law-enforcement authorities or other parties where disclosure is required by law or reasonably necessary to protect rights, security or safety.
- A successor or transaction counterparty in connection with a merger, restructuring, financing, acquisition or sale, subject to applicable protections.

Service providers may process information only for authorized purposes under the applicable contract or other valid arrangement. Because we operate in Canada and India, information may be processed and stored in Canada, India, the United States or other countries where we or our service providers operate, and may be accessible to authorities in those countries under their laws. Where required, we use appropriate safeguards for international transfers.

AIOT does not sell personal information and does not use website visitor information for cross-context behavioural advertising. If a particular service or applicable law treats a disclosure as a sale, sharing or targeted advertising, we will provide any required notice and choices for that service.

## 08 Retention and Deletion

We retain information only for as long as reasonably necessary for the purposes described in this policy, to provide a contracted service, meet legal or accounting obligations, resolve disputes, maintain security, or enforce agreements. Retention periods vary by data type and service.

For customer-managed systems, retention and deletion may be controlled by the customer, the service configuration or the contract. On request and where authorized, we will assist customers with deletion or return of data under the applicable agreement. Copies may remain in protected backups for a limited period before being overwritten, and we may retain information where the law requires or permits it.

You can request deletion of information we control through our Contact Us page. If an application supports account creation, it provides account-deletion functionality where required by applicable law or app-store policy, and its app-specific notice explains how to request deletion and any exceptions.

## 09 Security

We use technical, organizational and contractual safeguards designed to protect information against unauthorized access, disclosure, alteration, loss or misuse. Depending on the service, safeguards may include access controls, encryption, secure development practices, logging, monitoring, vulnerability management, staff training and supplier review.

No website, network, device or storage system can be guaranteed to be completely secure. We assess and respond to security incidents in accordance with applicable law, contractual obligations and our incident-response procedures, including notifying affected individuals and regulators where the law requires.

## 10 Your Choices and Rights

Depending on where you live, the applicable law, and whether AIOT is the responsible organization or a service provider for a customer, you may have the right to request access to, correction of, deletion of, or a copy of your personal information; to withdraw consent; to object to or restrict certain processing; to request portability; or to file a complaint with a privacy regulator.

To make a request, please reach us through our Contact Us page. Tell us the product or service involved and the nature of your request. We may need to verify your identity before acting, and we will respond within the time required by applicable law. If AIOT processes the information on behalf of a customer, we may refer your request to that customer or help the customer respond.

You can stop receiving marketing messages from us at any time by using the unsubscribe link in the message or by contacting us. We send commercial electronic messages only in line with Canada's Anti-Spam Legislation (CASL) and other applicable laws. Service and transactional messages may still be sent when needed to provide a requested service or meet legal obligations.

This policy is intended to operate with applicable privacy laws, which may include Canada's Personal Information Protection and Electronic Documents Act (PIPEDA), Alberta's Personal Information Protection Act (PIPA) and other applicable provincial laws; India's Digital Personal Data Protection Act, 2023 and its rules as they come into force; the EU and UK General Data Protection Regulation (GDPR); and applicable U.S. federal and state privacy laws, including HIPAA where it applies. Rights and requirements differ by jurisdiction and context.

## 11 Children

AIOT's corporate website and general business services are not directed to children, and we do not knowingly collect personal information from children through this website.

Some customer projects or apps may be designed for children or involve data about children. Those services require a specific privacy assessment, age-appropriate disclosures, parental or guardian consent processes where required, and additional safeguards. This general policy does not replace those service-specific requirements.

## 12 Third-Party Links

Our website or products may link to or integrate with third-party websites, APIs, platforms, AI models, devices or services. Their own privacy notices and terms apply to data they collect directly or process under their own responsibility, and we encourage you to review them. The relevant service documentation or customer agreement explains important third-party integrations for AIOT-delivered solutions.

## 13 Policy Changes

We may update this policy to reflect changes in our services, technologies, legal obligations or privacy practices. We will post the revised policy on this page and update the “Last updated” date. Where required by law, we will provide additional notice or obtain consent for material changes. Please review this page periodically.

## 14 Contact Us

For privacy questions, requests or complaints, including questions for our privacy officer, please reach us through our Contact Us page. Choose “Privacy” as your subject so your message reaches the right team.

If you are not satisfied with our response, you may have the right to contact the privacy regulator where you live, such as the Office of the Privacy Commissioner of Canada or the Office of the Information and Privacy Commissioner of Alberta.