Privacy Notice

ATSC Global Limited · how we use personal data when we decide why and how it is used

Field	Detail
Document reference	ATSC-PRIV
Version	2.0, November 2026
Effective date	[DATE OF PUBLICATION]
Controller	ATSC Global Limited, registration number 745470, First Floor, Penrose 2, Penrose Dock, Cork City, Ireland, T23 YY09
Data protection contact	legal@atsc.global · the address above, marked “Data Protection”
Lead supervisory authority	Data Protection Commission, Ireland

1. Who we are and when this notice applies

1.1 ATSC Global Limited (“ATSC”, “we”) is an Irish technology company that provides software platforms and AI services to businesses, public bodies and, for some products, individuals. This notice explains how we use personal data where we are the controller — that is, where we decide why and how it is used.

1.2 For most of our services we act for our customers. When a business, an estate, a municipality or another organisation uses an ATSC platform to manage its own information — about its staff, residents, visitors, customers or citizens — that organisation is the controller and we process the data on its instructions as its processor (or “operator” under South African law). In that case the organisation’s own privacy notice applies, and you should contact it first. We will help it respond to you.

1.3 Our group companies Sudo Sky Limited (Ireland) and its South African affiliate provide engineering and support to us. Where a third party supplies a service in a product under its own terms, such as a payment or verification service, the product tells you, and that party’s own privacy notice applies to it as an independent controller.

1.4 We have not appointed a Data Protection Officer, because we are not required to. Our data protection contact can be reached at legal@atsc.global. For South African data subjects, our Information Officer can be reached at the same address.

2. What we use, why, and on what basis

Who you are	What we use	Why	Lawful basis
Contact at a customer, prospect, partner or supplier	Name, job title, employer, business email and phone, correspondence, meeting notes	To sell, deliver and manage our services and contracts; to keep records	Contract (Art. 6(1)(b)) where you are the contracting party; otherwise our legitimate interest in running our business (Art. 6(1)(f))
Account holder or user of an ATSC product	Name, email, login and authentication data, account settings, support tickets	To create and secure your account, provide the product, and give support	Contract; legitimate interest in security
Any user of our services	IP address, device and browser data, logs of activity and errors (Service Data)	To operate, secure and improve the services, detect fraud and abuse, and fix faults	Legitimate interest in operating secure, reliable services
Paying individual customer	Billing name and address, transaction records, VAT details. Card numbers are handled by our payment provider, not stored by us	To take payment and meet tax and accounting obligations	Contract; legal obligation (Art. 6(1)(c))
Website visitor	Cookie and similar technology data, as described in our Cookie Notice	Strictly necessary operation; analytics and marketing only with your consent	Consent where required by S.I. 336 of 2011; otherwise legitimate interest
Recipient of marketing	Name, email, preferences, opt-out history	To send news about our products	Consent; or, for existing business customers, the soft opt-in under Regulation 13 of S.I. 336 of 2011, with an opt-out in every message
Job applicant	CV, application details, interview notes	To assess your application	Steps at your request before a contract; legitimate interest
Person who reports content or makes a complaint	Name, email, the report and our handling of it	To deal with the report and meet our Digital Services Act obligations	Legal obligation; legitimate interest

2.1 Where we rely on legitimate interests, we have balanced our interests against yours. You can ask us for details of that assessment, and you can object (section 6).

2.2 Where we rely on consent, you can withdraw it at any time, without affecting processing before withdrawal.

3. Special categories, children and AI

3.1 We do not seek special category data (such as health, biometric or ethnic origin data) for our own purposes, except in a product whose annexure to this notice says so. VitalLog, a personal and family health log, is one: there we rely on your explicit consent, given on its own screen and separately from any terms, and the VitalLog annexure explains what we use and why. Some other products process special category data for our customers — for example, facial recognition for estate access control — and in that case the customer is the controller, must rely on an Article 9 GDPR or section 27 POPIA ground, and must tell you so.

3.2 Some of our products are used by or about children, for example community and municipal apps and family health records. Where we are the controller, we do not knowingly collect the data of a child under 16 (under 18 in South Africa) without the consent of a parent or guardian, as the law requires; a product annexure may set a higher age. If you believe we hold a child's data without that consent, contact us and we will delete it.

3.3 We do not make decisions about you that produce legal or similarly significant effects based solely on automated processing. Where our products use AI, we tell you when you are interacting with an AI system, and the product's own notice explains what the AI does. We do not use the content you or our customers put into our services to train AI models made available to others.

4. Who we share data with

4.1 We share personal data only as needed for the purposes in section 2, with: our group companies and their engineering and support staff; service providers who process data for us, such as hosting, email, support desk and payment providers, listed at atsc.global/legal/sub-processors; our channel partners and distributors, where you deal with us through them; professional advisers and auditors; and authorities where the law requires. We do not sell personal data.

5. International transfers

5.1 We host data in the region recorded for each service, usually the EU for European customers and South Africa for South African customers. Our engineering and support teams work from Ireland and from South Africa, so personal data from the EEA may be accessed from South Africa.

5.2 South Africa is not covered by an EU adequacy decision. When EEA data is accessed from South Africa, or transferred to any other country without an adequacy decision, we use the European Commission's Standard Contractual Clauses (Decision (EU) 2021/914) together with a transfer impact assessment and supplementary measures such as encryption and access control. Transfers to US providers certified under the EU-US Data Privacy Framework rely on that framework. You can ask us for a copy of the safeguards.

5.3 Transfers of South African personal information out of South Africa comply with section 72 of POPIA.

6. Your rights

6.1 Under the GDPR you have the right to: access your personal data; have it corrected; have it erased; restrict its use; receive it in a portable format; object to processing based on legitimate interests, and at any time to direct marketing; withdraw consent; and not to be subject to solely automated decisions with legal or similarly significant effects.

6.2 Under POPIA you have equivalent rights, including to be told whether we hold your personal information, to request its correction or deletion, to object to its processing, and not to receive unsolicited direct marketing.

6.3 To exercise a right, email legal@atsc.global. We will respond within one month, which we may extend by two further months for complex requests, telling you why. We do not charge a fee unless a request is manifestly unfounded or excessive. We may need to verify your identity.

6.4 You have the right to complain to the Data Protection Commission, Ireland (www.dataprotection.ie), or to the supervisory authority where you live or work. In South Africa you may complain to the Information Regulator (inforegulator.org.za). We would welcome the chance to address your concern first, but you do not have to contact us before complaining.

7. How long we keep data

Record	Retention
Customer contracts and related correspondence	Term of the contract plus 6 years
Accounting and tax records, including invoices	6 years from the end of the financial year (Companies Act 2014; Taxes Consolidation Act 1997)
Records of your acceptance of our terms (name, time, IP address and the version accepted)	Life of the account plus 6 years, so that we can show what was agreed
Account and user data (where we are controller)	Life of the account plus 12 months, unless a longer period is required by law
Support tickets	3 years from closure
Security and audit logs	12 months, or longer where needed for an investigation
Marketing contacts	Until you opt out or 2 years without engagement
Job applications	12 months after the recruitment decision, unless you agree to longer
Content reports and DSA records	3 years

8. Security

8.1 We protect personal data with technical and organisational measures appropriate to the risk, including encryption in transit and at rest, access control with multi-factor authentication, logging and monitoring, and staff training. Our Security Schedule describes them in more detail.

9. Changes

9.1 We update this notice when our processing changes. Each version is dated and numbered, and previous versions are available at atsc.global/legal/privacy/archive. We will tell you directly about material changes that affect you.

Product annexures

Where a product has its own annexure to this notice, for example for health data or children, the annexure is published with that product and listed at atsc.global/legal. It forms part of this notice for that product.

End of Privacy Notice.