PRIVACY POLICY

Last updated: 11th June 2026.

This Privacy Policy explains how HSC Holding s.r.l. ("HSC Holding", "HSC", "we", "us" or "our") collects, uses, shares and protects personal data when you visit our websites, use our products and services, or otherwise interact with us.

HSC Holding provides cloud-connected asset tracking and data logging solutions that monitor temperature-sensitive and other critical assets using our devices (ex. "Ecologger", "TempyTag") and associated web and mobile portals. Our customers are primarily organisations that deploy our devices and portals to monitor their assets and consignments in real time.

By using our websites or services, you agree to the practices described in this Privacy Policy.

1. Who we are and scope of this Policy

HSC Holding s.r.l. is a company incorporated in Italy, with its registered corporate office at:

Via della Codignola 71, zip code 26900, Lodi (LO), Italy.

This Policy applies to personal data that we process in the following contexts:

- Visitors to our public websites, including **hscholding.com** and related product or documentation sites ("Website").
- Representatives and users of our business customers who access our "Resilyera" portal, APIs, or other hosted applications ("Platform").
- Individuals who contact us, subscribe to our communications, or interact with us offline (for example, by email or at events).

This Policy does **not** apply to information processed by our customers in their own systems outside our Platform, or to third-party websites and services that are linked from our website.

2. Our Role – Controller vs Processor

Depending on how you interact with us, we may act as:

- Data Controller – For Website visitors, marketing contacts, business development, support requests and account administration, we decide what personal data is collected and how it is used.
- Data Processor / Service Provider – For data that our enterprise customers upload or generate through our devices and Platform (such as shipment, consignment and device data that may incidentally include personal data), we process that data only on our customer's instructions and in accordance with our contracts with them. In those cases, the customer is responsible for providing appropriate privacy notices to the relevant individuals.

If you believe your data is being processed on our Platform because a customer uses our services, please contact that customer (for example, your employer or logistics provider) in the first instance for any rights requests related to such data.

3. How we collect data about you

We may collect different data from or about you depending on how you interact with our Website and Platform. The table below summarises the main categories.

Category	How we collect it	Examples of personal data	Main purposes
Data provided by registered users	You or your organisation provide this when creating or managing a user account on the Platform or when using our services.	Name, business email address, username, company name, role, phone number, password (stored in hashed form), notification preferences.	To create and manage user accounts, authenticate users, provide access to the Platform, send service notifications, and administer the customer relationship.
Data provided by non-registered users	You submit this information via Website forms, emails, events, or other communication channels when you contact us or request information.	Name, business email, phone number, company, job title, country, your message/enquiry, marketing preferences.	To respond to enquiries, schedule demos, send requested information, manage leads, and send marketing communications where permitted by law and your preferences.
Data collected through automated means	Collected automatically when you visit the Website or use the Platform using cookies, server logs and similar technologies.	IP address, browser and device type, operating system, language, pages visited, features used, timestamps, error logs, basic location inferred from IP.	To secure our services, measure usage, troubleshoot issues, improve performance and user experience, and understand how our Website and Platform are used.
User-generated data	You or your organisation provide this when configuring and using the Platform or when interacting with our support team.	Names or identifiers for consignments, shipment references, asset names, notes or labels, contact details embedded in shipment metadata, support tickets, screenshots.	To operate the solutions (devices and platform), display relevant information in dashboards and reports, send alerts, and resolve support issues.
Data processed on behalf of customers	Our customers configure devices and upload or generate data	Device identifiers, telemetry data (e.g., temperature, humidity, motion, battery status), shipment/consignment	To provide our services to customers, including real-time monitoring, alerts, reporting, analytics and audit

	through the Platform while using our services.	metadata that may include names or contact details of responsible persons or recipients (as configured by the customer).	trails. In this context, we act as a processor/service provider and follow our customer's instructions.

4. Types of personal data we collect

4.1 Data you provide directly

Website and contact forms

When you fill out a contact form, request a demo, subscribe to our newsletter or otherwise reach out to us, we may collect:

- Name
- Business email address
- Company name and job title
- Country or location
- Phone number
- Your message or enquiry details
- Your marketing communication preferences

Platform user accounts

When your organisation creates an account for you on our Platform, or when you log in, we may collect:

- Name
- Business email address and username
- Company/organisation name and role
- Password or other login credentials (stored in hashed form)
- User preferences and notification settings

Customer support and business communications

If you contact us for support or business discussions, we may collect:

- Contact details (as above)
- Details of your support request, including logs or screenshots you choose to share
- Records of emails, tickets and other communications

We do not currently collect or store your payment card details through our Website or Platform. Any commercial transactions are handled via invoicing or separate payment channels managed outside the Website and Platform.

4.2 Data we collect automatically

When you visit our Website or use our Platform, we automatically collect certain technical data, such as:

- IP address
- Browser type, version and language
- Device type and operating system
- Referring pages and URLs
- Dates and times of access
- Pages viewed, features used and other interaction data
- Log data related to system performance, errors and security events

We collect this information through server logs, cookies and similar tracking technologies. For more details, please refer to our **Cookie Policy**.

4.3 Data we process on behalf of our customers

When customers deploy our devices and use our Platform, we process operational data on their behalf, which may include:

- Device identifiers and telemetry (e.g., temperature, humidity, motion, battery level)
- Asset or consignment identifiers, shipment references and related metadata
- Geolocation and movement data of devices/consignments
- Event data such as threshold breaches, alerts and audit logs
- Limited personal data related to consignments (for example, where shipment details include names or contact details of responsible persons or recipients, as configured by the customer)

In these cases, we act as a processor/service provider, and we only process such data in accordance with our customer contracts and applicable data protection laws.

5. How we use personal data

We use personal data for the following purposes, as permitted by applicable law:

- **Provide and operate our services**
- Create and manage user accounts on the Platform
- Configure devices and monitor their status
- Display shipment and asset information in the dashboard
- Send alerts, notifications and reports as configured by customers

- **Customer support and communications**
- Respond to enquiries, support tickets and technical issues
- Provide training, onboarding and updates related to our services
- Manage our relationship with customers, partners and suppliers
- **Safety, security and performance**
- Authenticate users and prevent unauthorised access
- Monitor, detect and prevent fraud, abuse and security incidents
- Maintain logs, conduct troubleshooting and improve reliability
- **Analytics and service improvement**
- Understand how our Website and Platform are used
- Analyse performance, improve features and develop new capabilities
- Generate aggregated, anonymised statistics for internal business insights
- **Marketing and business development**
- Send newsletters and information about our products, services and events, where permitted by law and your preferences
- Run campaigns, surveys and webinars to better understand customer needs
- Manage opt-ins and opt-outs for marketing communications
- **Legal and compliance**
- Comply with legal obligations, regulatory requirements and audit requests
- Enforce our contracts and terms of use
- Establish, exercise or defend legal claims

6. Legal bases for processing (GDPR and similar laws)

Where the EU/UK General Data Protection Regulation (GDPR) or similar laws apply, we rely on one or more of the following legal bases:

- **Performance of a contract:** To provide and manage the services you or your organisation have requested, including operating the Platform and supporting devices.
- **Legitimate interests:** To secure our systems, improve our offerings, communicate with you about our services, and conduct business operations, provided these interests are not overridden by your rights and interests.
- **Consent:** For certain marketing communications and the use of non-essential cookies or similar technologies. You can withdraw your consent at any time.
- **Legal obligation:** To comply with applicable laws, regulations, court orders and law-enforcement requests.

When we act as a processor/service provider on behalf of our customers, our legal basis is determined by the customer (the controller), and our processing is governed by our data processing agreements with them.

7. How we share personal data

We share personal data only with the categories of recipients described below, and only to the extent necessary for the purposes described in this Policy.

7.1 Service providers (processors)

We use trusted third-party service providers to support our operations, for example:

- Cloud infrastructure and hosting providers
- Email delivery and customer support tools
- Analytics and monitoring services
- CRM and marketing platforms
- Security, backup and disaster-recovery providers

These service providers may process personal data on our behalf and are contractually required to:

- Use the data only for the specified purposes
- Implement appropriate security measures
- Follow our instructions and applicable data protection laws

7.2 Customers and authorised users

If you are a user of our Platform, certain data (such as your name, email address, activity logs and alerts) may be visible to your organisation's administrators and other authorised users, in accordance with that organisation's configuration and policies.

7.3 Corporate transactions

If HSC Holding is involved in a merger, acquisition, restructuring, asset sale or similar transaction, personal data may be transferred as part of that transaction, subject to confidentiality and applicable law.

7.4 Legal and regulatory requirements

We may disclose personal data if we reasonably believe this is necessary to:

- Comply with laws, regulations, legal processes or government requests
- Protect the rights, property or safety of HSC Holding, our customers, users or others
- Detect, prevent or address fraud, security or technical issues

We do not disclose personal data to law-enforcement or government authorities except as required by applicable law.

8. International data transfers

Our services are used by customers in multiple countries. Personal data may therefore be processed in, or transferred to, countries other than the one where it was originally collected, including other jurisdictions where our infrastructure, service providers or support teams are located.

Where required by law, we implement appropriate safeguards for international transfers, such as:

- Contractual safeguards, including standard contractual clauses approved by relevant regulators
- Technical and organisational measures to protect the data in transit and at rest
- Due-diligence and oversight of our service providers

9. Data retention

We keep personal data only for as long as necessary to fulfil the purposes described in this Policy or as required by law, including:

- For Website and marketing contacts: as long as you remain engaged with our communications or until you opt out, plus a reasonable period to maintain suppression lists.
- For Platform accounts: for the duration of the customer contract and a defined period afterward (for example, to handle queries, audits and dispute resolution), in accordance with our agreements with customers.
- For device and consignment data processed on behalf of customers: according to the retention settings agreed with the customer or configured in the Platform.
- For legal, accounting and compliance purposes: as required under applicable laws.

When personal data is no longer required, we will delete it or anonymise it in a secure manner.

10. Security

We maintain technical and organisational measures designed to protect personal data against unauthorised access, loss, misuse, alteration or destruction, including:

- Access controls, authentication and least-privilege principles
- Encryption of data in transit and at rest where appropriate
- Network security controls and monitoring
- Secure development, change management and vulnerability handling practices
- Regular backups and business-continuity measures
- Staff training and confidentiality obligations

While we strive to protect your data, no system can be completely secure. You are responsible for keeping your login credentials confidential and notifying us promptly if you suspect any unauthorised use of your account.

10.1. Personal Data Breach Notification

In the event of a personal data breach that is likely to result in a risk to the rights and freedoms of individuals, we will assess the incident promptly and take appropriate remedial action.

Where required by applicable law:

- We will notify the relevant supervisory authority within the timelines prescribed by law (for example, within 72 hours under the GDPR, where applicable).
- We will notify affected individuals without undue delay where the breach is likely to result in a high risk to their rights and freedoms.
- Where we act as a processor/service provider on behalf of a customer, we will notify the customer without undue delay in accordance with our contractual obligations so that they may fulfil their regulatory obligations.

We maintain internal incident response and breach management procedures to detect, investigate and respond to security incidents.

11. Your privacy rights

Depending on your location and applicable law (for example, GDPR, UK GDPR, and similar laws), you may have the following rights:

- **Right to be informed** – to receive clear information about how we process your personal data.
- **Right of access** – to request a copy of the personal data we hold about you.
- **Right to rectification** – to ask us to correct inaccurate or incomplete data.
- **Right to erasure** – to request deletion of your personal data, in certain circumstances.
- **Right to restriction of processing** – to request that we limit the processing of your data in certain situations.
- **Right to object** – to object to our processing where it is based on legitimate interests, including the right to object at any time to direct marketing.
- **Right to data portability** – to receive certain personal data in a structured, commonly used and machine-readable format and to transmit it to another controller, where technically feasible.
- **Rights related to automated decision-making** – where applicable, to not be subject to a decision based solely on automated processing, including profiling, that produces legal or similarly significant effects.

We do not currently carry out automated decision-making that produces legal or similarly significant effects about individuals.

If we process your personal data on behalf of a customer (as a processor/service provider), we may need to refer your request to that customer to handle, in line with our contractual obligations.

You also have the right to lodge a complaint with a supervisory authority or relevant data protection regulator in your jurisdiction. If you have any queries or concerns with this Policy, please contact our Grievance Officer (refer Section 17)

12. Marketing communications

If you opt in to receive marketing communications from us (for example, by ticking a consent box on a Website form), we may send you:

- Product updates and feature announcements
- Newsletters, articles, webinars and event invitations
- Information about new offerings or promotions

You can opt out of marketing emails at any time by:

- Clicking the "unsubscribe" link in the email, or
- Contacting us using the details in the "Contact us" section below.

Even if you opt out of marketing, we may still send you non-marketing communications related to your account or our ongoing business relationship (such as security alerts, service notifications or invoices).

13. Cookies and similar technologies

We use cookies and similar technologies on our Website and Platform to:

- Enable basic functions and security
- Remember your preferences and sign-in details
- Understand how visitors use our Website and Platform
- Improve performance and user experience

Where required by law, we will ask for your consent before placing non-essential cookies. For more information about the types of cookies we use and how to manage your preferences, please refer to our **Cookie Policy**.

14. Children's privacy

Our Website and services are intended for business users and are **not** directed to children under the age of 18 (or such higher age as required under applicable law). We do not knowingly collect personal data from children.

If you believe that a child has provided personal data to us without appropriate consent, please contact us using the details below, and we will take steps to delete such information as required by law.

15. Third-party websites and services

Our Website and Platform may contain links to third-party websites, applications or services that are not operated by HSC Holding. If you follow such links, any data you provide will be subject to the privacy policies of those third parties.

We are not responsible for the privacy practices or content of such third-party sites and encourage you to review their privacy policies before providing any personal data.

16. Changes to this Policy

We may update this Privacy Policy from time to time to reflect changes in our practices, technologies, legal requirements or other factors. When we make changes, we will:

- Post the updated Policy on this page with a revised "Last updated" date, and
- Where appropriate, notify customers and users through our Website, Platform or email.

We encourage you to review this Policy periodically to stay informed about how we protect your data.

17. How to contact us

If you have any questions, concerns or requests related to this Privacy Policy or our data protection practices, you can contact us at:

General enquiries and support
Email: info@hscholding.com

Data Protection Officer (DPO)
Name: Luca De Toro
Role: Fouder & CEO
Email: luca.detoro@hscholding.com

Postal address (corporate office and headquarter):
HSC Holding s.r.l.
Via della Codignola 71, zip code 26900, Lodi (LO), Italy
Via Colle Eghezzone 1, zip code 26900, Lodi (LO), Italy

Please mention "Privacy – [your request]" in the subject line if you contact us by email and indicate whether you are contacting us as a customer, end user, or website visitor.

If you are located in a jurisdiction that grants you specific statutory rights (for example as a "data subject" under the GDPR), please mention your country or region in your request so we can handle it appropriately.