



Tempy Tag – Mobile App Privacy Policy

Last updated: 13th July 2026

This Privacy Policy describes how HSC Holding s.r.l. ("HSC Holding", "HSC", "we", "us" or "our") collects, uses and protects data when you use the Tempy Tag mobile application ("the App") on iOS and Android.

Depending on how the App is used, HSC Holding may act as Data Controller for operation of the App itself and as Data Processor on behalf of customer organisations for operational monitoring data. Where HSC acts as Processor, the customer remains the Data Controller.

The App is a companion tool for our cloud-connected temperature and asset monitoring solution. It lets you read HSC "TempyTag" NFC data-logger tags, start and stop logging sessions, view temperature history, and synchronise that data with our backend so that your organisation can monitor temperature-sensitive assets and consignments.

This notice supplements, and should be read together with, the general HSC Holding Privacy Policy, which governs our websites and our "Resilyera" platform. Where this App notice is silent, the general Policy applies.

1. Data we collect through the App

The App is designed to collect the minimum data needed to operate. The App itself does not require users to create an account directly within the App. Where your organisation requires authentication, user account information is managed through the HSC Holding platform and is governed by the general HSC Holding Privacy Policy. We collect only the following two categories of data:

1.1. Location data (GPS)

- **What:** the geographic coordinates (latitude and longitude) of the device at the moment you scan or read a tag, and a human-readable address derived from those coordinates.
- **Why:** to record where a temperature-logging session was started or read, so that a scan can be placed on a map and associated with the asset or consignment being monitored. This is a core monitoring feature of the product.
- **How:** location is accessed **only while the App is in use** (foreground). The App does not track your location in the background. The address is resolved on the device via the operating system's reverse-geocoding service.
- **Your control:** location capture is **optional and off-limits at any time**. You can disable it from *Settings* → *General* → *Location*, and you can revoke the location permission entirely from your device settings. Location data enhances the monitoring functionality by allowing scans to be displayed on maps and associated with assets. The App remains functional if location permission is denied, although this feature will not be available. When disabled, the App works normally; scans are simply recorded without coordinates.

1.2. Device identifier

- **What:** randomly generated installation identifier. This is a random UUID generated by the App the first time it is installed, together with an opaque installation identifier issued by our server. Neither is derived from your device's hardware identity, and neither is linked to your name or to any personal account.
- **Why:** to distinguish one installation from another when synchronising scans, to avoid duplicate records, and to sign requests to our backend so that tampered or replayed data can be rejected. This is required for the App to function.
- **How:** the identifiers are stored on the device (in AsyncStorage / the OS secure store) and sent to our backend together with tag scans. Unsynchronised scan data remains stored locally until successfully uploaded or deleted by the user.

2. Data we do NOT collect

- We do **not** collect your name, email, phone number or any contact details in the App.
- We do **not** show advertising and we do **not** use third-party advertising or cross-app tracking SDKs.
- We do **not** track you across other companies' apps or websites (no "tracking" in the sense of Apple's App Tracking Transparency framework).
- The **camera** is used only on-device to scan QR codes / barcodes when you choose to assign a nickname to a tag. Camera images are processed locally and are **not** transmitted to us or stored.

3. Other data generated in the App

In addition to the two categories above, the App records the operational data that is the whole point of the product: tag identifiers (the tag's UID), temperature and sensor readings from the logger, logging configuration, and timestamps. This is device and asset telemetry, not personal data about you. It is stored locally on the device and synchronised to the HSC backend that your organisation uses.

4. How the data is used

We (and, where you use the App on behalf of an organisation, that organisation) use the data collected through the App to:

- provide the App's core functionality — reading tags, storing sessions, syncing data;
- enable temperature and asset monitoring, including placing scans on a map;
- secure the connection between the App and our backend and prevent abuse;
- troubleshoot and improve reliability of the service.

We do not use App data for advertising, profiling, or automated decision-making that produces legal or similarly significant effects.



5. How the data is shared

Scan data is transmitted only to the HSC backend configured for your deployment. We use trusted infrastructure and hosting providers (processors) to run that backend under appropriate contractual and security safeguards. We do not sell your data, and we do not share it with advertisers or data brokers. Where the App is used on behalf of an organisation (our customer), HSC acts as a data processor and handles the data on that customer's instructions; the customer is the controller of the operational data.

6. Data retention

- Data stored **on your device** remains until you delete it or uninstall the App.
- Data synchronised to the **backend** is retained according to the retention settings agreed with your organisation, as described in the general HSC Holding Privacy Policy.

7. Security

Data in transit between the App and our backend is protected, and the installation secret used to sign requests is held in the operating system's secure storage (iOS Keychain / Android Keystore). Processing is based on performance of a contract, legitimate interests and consent (for optional location permission where required).

Data synchronised from the App becomes available to authorised users through the TemyTag web portal in accordance with the permissions configured by your organisation.

No system is perfectly secure, but we apply access controls, encryption in transit and least-privilege principles as described in the general Policy.

8. International Transfers

International transfers, where applicable, are governed by the HSC Holding Privacy Policy.

9. Children's privacy

The App is intended for business use and is not directed to children. We do not knowingly collect data from children.

10. Your rights

Because the App does not collect data that identifies you personally, most of the data it handles cannot be linked back to an individual. Where any applicable data protection law (for example the GDPR) grants you rights over personal data, you may exercise them as described in Section 11 of the general HSC Holding Privacy Policy. If your data is processed on behalf of a customer, we may refer your request to that customer.

11. Changes to this Policy

We may update this App Privacy Policy to reflect changes to the App or to legal requirements. The "Last updated" date at the top will always reflect the current version.

12. Contact us

For any question about this App Privacy Policy or our data practices:

HSC Holding s.r.l.

Via della Codignola 71, 26900 Lodi (LO), Italy

General enquiries: info@hscholding.com

Data Protection Officer: Luca De Toro — luca.detoro@hscholding.com