Privacy Policy

[telemry.com, errport.com]

Last updated: 2025. 05. 01. (Version: 1.0)
Service name: Telemry - Telemetry and online management system or Telemry project, Telemry for short.
Developer and operator: Sándor Tóth (private individual)
Contact: toth.sandor@telemry.com

This privacy policy is prepared in accordance with the European Union (GDPR) legislation. Our service is available from any country in the world and we feel obliged to respect local data protection laws.

We store data in the EU, but we are committed to complying with other applicable international laws (e.g. GDPR, CCPA, LGPD). If the User's country requires stricter rules, we will treat them as a priority.

In the Telemry online administration system, End User data collected in forms created by you (registered User) (e.g. bug report, appointment booking) are stored on your behalf and at your instructions. You, as the Data Controller, are responsible for informing End Users and for data processing in accordance with the GDPR. As the Data Processor, we only provide technical support and do not use this data for our own purposes.

Certain functions of the mobile application (e.g. location, camera, notifications) require special permissions. These permissions are requested when installing or first using the application.

The privacy policy is available in English and Hungarian. For requests in other languages, please contact us.

International users are asked to use the email address privacy@telemry.com as their primary email address for privacy issues.

---

1. The Data Controller and Data Processor

1.1 Data Controller for registered users:

- Name: Sándor Tóth
- Contact: toth.sandor@telemry.com
- Legal basis:
- Article 6(1)(a) of the GDPR (consent – for registration).
- Article 6(1)(b) of the GDPR (performance of a contract – processing of company data necessary for the operation of the service).
- The service is available under several domain names, with different appearance and functionality (telemry.com, errport.com). Each domain is part of the same basic

system, and the data processing in each case applies to the Data Controller (the person indicated above).

1.2. Data Controller for End Users (error reporting/appointment booking forms):

- Users using the service who create their own forms.

1.3. Data processor:

- Sándor Tóth, who technically stores and manages the data.

---

2. Personal data processed

2.1. Registered users (Users):

- Name, email address, country.
- Data provided after login: Company information entered by users (e.g. company name, tax number, contact details).
- Technical data collected automatically:
- 1 cookie: For user identification and automatic login, valid for 14 days.
- IP address and browser data (only to the extent necessary for the operation of the service).
- The data collected on the error reporting and appointment booking forms are stored in the name of the User, and the User is responsible for the existence of the legal basis (e.g. consent or performance of a contract).

2.2. End users (via forms):

- Error reporting: Name, email, description of the error or complaint or opinion, photo attachment.
- Appointment booking: Name, email.
- Automatically collected: IP address, browser data, cookie identifier (randomly generated unique identifier).

2.3. Data related to IoT devices:

- Wi-Fi network name and password (stored encrypted).
- MQTT server credentials (username, password).
- Device identifiers (e.g. MAC address).

2.4 When using the mobile application, the following data is collected:

- Device information: Unique device identifiers, operating system and browser data.
- Location: Only if enabled (e.g. for appointment booking locations).
- Camera: for photo upload, barcode, QR code reading.
- Application activity: Error logs, usage statistics.

2.5. Users register with a specific domain (e.g. telemry.com, errport.com), but their data is stored centrally. A single account can be used across multiple domains, where functions and permissions may vary according to domain-specific settings.

---

3. Purpose of data processing

3.1. Registered Users:

- Account management, provision of services.
- Authentication and automatic login of Users using cookies.
- Operation of the service (based on the company information entered).
- Ensuring the security and integrity of the system.
- Operation of a multi-domain system, where:

- Users can access the service or part of it on multiple domains with a single account.
- Providing domain-specific functions (e.g. different permissions or appearance).

3.2. End users:
- Handling of bugs/complaints, recording of appointments.
- Fraud prevention (IP address, browser data and cookie ID).

3.3. IoT devices:
- Configuration and control of devices.
- Secure communication with the system.

3.4. The mobile application:
- Configuration and control of devices.
- Secure communication with the system.
- Usage statistics.

3.5. Optional AI feature:
- Convert tickets or appointment bookings into chat-based text or voice-to-text/text-to-voice using an external API (e.g. OpenAI, Gemini) (only with consent).

---

4. Legal basis for data processing

4.1. Registered Users: Performance of a contract (GDPR Article 6 (1) b).
- Consent: Processing of data required for registration (name, email, country).
- Performance of a contract: Processing of company information for the provision of the service.
- Legitimate interest: Protection of the security of the system (e.g. tracking of login attempts).

4.2. End users:
- Legal basis of the Data Controller (User) (e.g. consent).
- Security: Legitimate interest (GDPR Article 6 (1) f).

4.3. IoT devices:
- Performance of a contract (GDPR Article 6 (1) b).
- For Wi-Fi/MQTT passwords: explicit consent (GDPR Article 9).

---

5. Data retention period

5.1. Registered Users:
- Until account deletion.
- Company information: Until account deletion, unless a legal obligation requires separate retention.

5.2. End users:
- Form data: According to the instructions of the Data Controller (User).
- Cookies: 90 days after opening.
- Technical data (IP): 30 days.

5.3. IoT devices:
- Wifi/MQTT passwords: Until device deletion (encrypted).
- Device identifiers: For the duration of the service use.

---

6. Data transfer and processors

6.1. Telemry online business system:

- There is no data transfer to third parties. The system is completely independent, does not use SDKs, APIs or analysis tools loaded from external servers (e.g. Analytics, Tag manager, Like buttons). We fully strive for the security of Users' data.
- The external libraries used from third parties are stored locally.
- We store Users' data exclusively locally and do not share it with others.
- Although the service is available on multiple domains, all data is stored centrally. Only the Data Controller has access to Users' data.

6.2. External APIs (external website for reporting errors and booking appointments):

- In case of AI function: Data transferred to (API provider, e.g. OpenAI, Gemini).
- The AI function is only activated with explicit consent.

6.3. IoT communication:

- MQTT data is transmitted encrypted.
- No data is transferred to third parties, except to the server specified by the User.

---

7. Data protection measures

7.1. Encryption:

- SSL/TLS on the website and in IoT device communication.
- Wi-Fi/MQTT passwords stored encrypted.

7.2. Local data storage:

- Data is stored on our own virtual server.

7.3. Backups:

- Continuous backups of system and IoT data.

7.4. Access restrictions:

- Only the Operator has access to encrypted data. Where feasible or necessary, the data cannot be decrypted (one-way encryption).

---

8. Cookies and WebSerial

8.1. Management system Cookies:

- For registration: 1 session cookie: Required for user identification and automatic login.
    - Validity period: 14 days.
    - Type: "First-party" (self-created), non-tracking or analytical cookie.
- Cookie management: The user can disable or delete cookies in the browser settings.

8.2. Error reporting and appointment booking forms:

- We use a unique cookie to identify end users to limit the risk of spam and abuse. The cookie is valid for 90 days.

8.3. WebSerial (IoT firmware upload):

- HTTPS is required for browser firmware upload.
- User consent is required before upload.

---

9. Rights of the data subject

9.1. Registered Users:

- You can request access, correction, deletion of data related to your account.
- You can object to data processing.
- You can revoke your consent (in this case, your account will be deleted).
- Submit requests: privacy@telemry.com

9.2. End users:

- Rights must be exercised with the Data Controller (form creator).

9.3. IoT users:

- Delete passwords by resetting the device.

---

10. IoT-specific clauses

10.1. Firmware usage:

- The downloaded firmware (.bin files) can only be used on devices supported by the manufacturer.
- We are not responsible for any damages resulting from improper use.

10.2. Hardware independence:

- We are not responsible for the malfunction of third-party IoT devices.

---

11. Incident Detection

- If any Data Controller or Data Subject has detected an incident in any data processing or believes that it is likely to occur, please report it immediately.
- The Data Controller will immediately investigate the report and take the necessary steps
- provided for in the law.
- A data protection incident is considered to be: unauthorized access/viewing of personal data, transmission to an unauthorized person, use other than the purpose and method of data processing.

---

12. Update of the information

- Users will be notified of the changes upon their first login after the change.
- I reserve the right to modify the information in case of legal changes or service improvements. The current version is available here: https://telemry.com/document/hun/privacy

---

13. Multi-domain operation

13.1 Domains and functions

- The service is available on multiple domains, which have different appearance (e.g. background color, logo) and functionality.
- By default, Users can only use the functions of the domain where they are logged in.

13.2 Single account, multiple domains

- The data of registered Users is stored centrally, and the account can be used on any domain.

13.3 Domain switching

- The user always sees the functions available to him according to the specific settings of the selected domain.

Additional Information

- Minors: To use the service, registration is only allowed for persons over the age of 18.
- Responsibility for Company Information: Users undertake that the company information provided is accurate and that they have the authority to publish it.

Contact

Privacy Questions:

- If you have any questions about our privacy practices, please feel free to email us at: privacy@telemry.com

End Users:

- Contact the form creator.