IRONCHIP
CYBERSECURITY

Privacy Policy

Identity Platform and Mobile Application

Your Next Generation Identity

Table of Contents

This Privacy Policy describes how **IRONCHIP TELCO, S.L.** processes personal data in relation to the use of the Ironchip **Identity and Authentication Product**, available in its web, SDK, API, mobile application, desktop application, authenticators, tokens, NFC/RFID cards, delegated authentications, and any other associated module versions (hereinafter, the "Service").

This Policy applies to **authorized users** of the Service and to **Clients** (organizations) that contract the product.

1. Applicable Regulations

Our Privacy Policy has been designed in accordance with REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), hereinafter GDPR EU 2016/679. Insofar as it does not contradict the aforementioned Regulation, it is also governed by the provisions of Organic Law 3/2018, of 5 December, on the Protection of Personal Data and Guarantee of Digital Rights, hereinafter LOPDGDD 3/2018. Both regulations constitute the legal framework applicable to the data processing carried out through the Service and determine the obligations of Ironchip and the rights of users.

The use of the Service implies that the Client and/or user has been informed in accordance with these legal texts and understands the legal bases, purposes, and conditions under which their personal data will be processed as set forth in this Policy.

2. Technical Glossary

In order to facilitate understanding of how the Service works, some basic definitions of the technical concepts involved in the authentication process are included. The following are understood as:

- Token: the digital element that temporarily validates the user's identity without exposing their credentials;
- MFA or multi-factor authentication: the process by which more than one verification element is required to grant access;
- Device ID: the technical fingerprint that securely links a user to their usual device;
- Fingerprint: refers to the set of technical parameters that allow a device to be identified without the need to use direct personal data;
- Trusted perimeters: geographical or logical areas defined by the Client that reinforce access control through location-based restrictions;
- Metadata: refers to the technical information necessary to ensure the proper functioning of the Service, without including personal content from the user.

These definitions help both the Client and users understand what type of information is used and for what purpose, thereby strengthening the transparency of the Service without compromising its security.

3. Identity of the Controller and Contact Details

Data Controller	IRONCHIP TELCO, S.L. Registered office: Calle Beurko Viejo, 17 – 48902 Barakaldo, Biscay (Spain) Tax ID (CIF): B95880332 Contact: privacy@ironchip.com
Data Protection Officer (DPO):	María Llanas Villa – Compliance Team Contact: dpo@ironchip.com

4. Role of Ironchip and the Client (Controller / Processor)

The data processing carried out through the Service may involve different levels of responsibility depending on the nature of the information processed and who determines its purposes and means. With regard to the data necessary to ensure the security, stability, and proper functioning of the Service—including technical logs, information derived from system usage, events used for detecting unauthorized access, and those generated in the context of support - **Ironchip acts as the Data Controller**, as such processing forms part of its technical and operational obligations and does not depend on the Client's decisions.

Separately, when the Service is used within the Client's infrastructure to authenticate its own users, Ironchip acts as a **Data Processor**, processing personal data solely in accordance with the Client's documented instructions and under the terms set out in Article 28 of the GDPR. In this context, the **Client acts as the Data Controller**, as it is the entity that decides which data are integrated into the system, how access and authentication policies are configured, which users are involved, and the legal basis that legitimizes the processing within its organization.

As Data Controller, the Client must ensure that the personal data provided to the Service are lawful, accurate, and appropriate for the intended purposes, as well as manage user onboarding and offboarding, determine data retention criteria, and comply with any applicable internal and sector-specific regulations. For its part, Ironchip will limit its actions to providing the Service under such instructions, without using the data for its own purposes unrelated to the relationship with the Client.

5. Definition of the Service and Privacy Architecture

Ironchip's Identity Service is designed to provide a robust authentication system that combines various verification and protection mechanisms to ensure that only legitimate users can access authorized resources. To achieve this, the Service integrates advanced multifactor

authentication methods, context-based security techniques, and secure binding processes between the user and their devices. This is complemented by an encryption model that protects keys and critical elements directly within the user's environment, preventing Ironchip or third parties from accessing sensitive information.

In addition, the Service can operate through integrations that allow its use in corporate applications and systems via APIs, SDKs, or physical elements such as cards, tokens, or delegated authenticators, among others. The architecture includes verification mechanisms based on location or trust zones defined by the Client, as well as a continuous monitoring system that enables the identification of anomalous behavior and reinforces security without interfering with the user experience.

It is important to note that Ironchip does not store passwords in plain text, does not have access to the user's private keys, and does not use the processed information for marketing, commercial profiling, or any activities unrelated to the provision of the Service. The architecture is based on principles of data minimization, cryptographic protection, and privacy by design, ensuring that only the data strictly necessary to guarantee authentication and the security of the environment are used.

6. What personal data do we process?

The Service processes only those personal data that are essential to identify the user, verify their authenticity, and ensure the security of the environment. These data may vary depending on the configuration established by your organization—Ironchip's Client—but generally include the basic information required to recognize each user within the system, such as their name, surname, corporate email, or assigned identifier, as well as certain professional attributes managed by your organization, such as the user's role or level of permissions within the organization.

To enable authentication and protect access, the Service generates and uses information linked to security mechanisms, such as tokens and derived keys that validate the session, activated authentication factors, or the technical fingerprint of the device used to access the Service. The Service also processes information arising from the technical functioning of the system, such as the IP address, device type, regional settings, browser parameters, or telemetry strictly necessary to detect anomalies and ensure the integrity of the Service.

When the Client enables advanced context-based features, the system may process approximate location data as well as information related to trusted zones. These data are managed using encryption measures or pseudonymization techniques and are used exclusively to strengthen access security, never to track movements or create user location histories.

During use of the Service, logs associated with authentication activity are also generated, including date and time of access, security events, detected incidents, or configuration changes. This information is essential for traceability, fraud prevention, and incident resolution.

In the context of technical support, data voluntarily provided by the user—such as messages, screenshots, or logs needed to analyze an incident—may also be processed.

It is important to emphasize that Ironchip never processes passwords in plain text, does not access content stored by users, does not process special categories of data, nor receives raw biometric information. When a user employs biometric authentication on their device, Ironchip only receives a success or failure confirmation from the device itself, without accessing the biometric data itself.

7. Purposes of the processing and legal bases

The processing of personal data through the Service is based on clearly defined purposes and legal grounds fully aligned with the General Data Protection Regulation (GDPR). First and foremost, user information is used to enable their authentication and manage access to the Service, which includes credential validation, the creation of secure sessions, and the operation of the various available authentication factors. This purpose constitutes the core of the contracted service and is based on the performance of a contract, since without this data it would be impossible to provide the Service or ensure its operability.

Additionally, the Service processes data that are essential to preserve the security of the Client's digital environment, anticipate anomalous behavior, and prevent unauthorized access. This processing involves analyzing certain technical indicators, recording usage events, and applying automatic or manual security enhancement mechanisms when necessary. Such actions are supported by the legitimate interest of both Ironchip and the Client in protecting the integrity of accounts, credentials, and technological infrastructure—a legitimate interest that is also crucial for fulfilling cybersecurity, traceability, and fraud prevention obligations. This interest has been internally assessed to ensure the user's protection takes precedence and that safeguards are applied to avoid any disproportionate impact on their rights.

Certain technical data are also processed to improve the Service's performance, fix errors, optimize user experience, and ensure the platform remains available and stable. These activities, which do not significantly affect users, are also based on Ironchip's legitimate interest in maintaining a technically robust and continuously evolving system, while consistently applying minimization and pseudonymization measures.

When the user requests support or technical assistance, the data processed to resolve their request—including any data they voluntarily provide—are processed under the context of contract performance, as they form part of the contracted service and are necessary to appropriately address the reported issue.

Finally, there are processing activities that may be mandatory under current legislation, such as responding to requests from competent authorities or cooperating in administrative or judicial proceedings. In such cases, the applicable legal basis is compliance with legal obligations, and the processing is strictly limited to what is necessary to meet such requirements.

For optional features whose activation involves additional data processing—such as location or advanced authentication factors—the Client, as the Data Controller, must obtain the user's explicit consent when applicable, ensuring that such consent is freely given, informed, and revocable. Ironchip will only process these data when the functionality has been enabled by the Client and under the assurance that the Client has fulfilled the obligations set out in Articles 6 and 7 of the GDPR.

8. Automated Decision-Making

The Service includes automated mechanisms designed to enhance access security and to protect both users and the infrastructure itself from anomalous behavior. These systems analyze certain technical indicators—such as usage patterns, device consistency, or risk signals—with the sole purpose of identifying situations that may compromise the integrity of access. Based on this assessment, the system may apply preventive measures, such as requesting additional authentication or temporarily blocking an attempt that appears clearly suspicious.

Although these actions are based on automated processes, they do not in themselves produce consequences that irreversibly or significantly affect the user's rights. Any block or alert resulting from this analysis may be reviewed by a human team, and the user has the possibility of requesting such a review to ensure that no errors or incorrect decisions occur. In this way, we combine the speed and efficiency of automatic detection with the necessary human oversight to ensure fair processing in accordance with the GDPR.

9. Data Retention Periods

The retention of data processed through the Service is aligned with the periods established by Ironchip and the Client in the service contract, always within the limits set by applicable legislation. As a general rule, data associated with account and authentication management is retained for as long as the user remains active in the system, while technical and security logs are kept for the period necessary to ensure traceability, incident detection, and compliance with the security obligations contractually agreed upon.

However, these periods may be extended when there is a legal reason to do so, such as the need to respond to authority requests, comply with specific regulatory obligations of the Client's sector, or preserve evidence related to internal investigations or legal proceedings. In the context of technical support, data is retained only for the time strictly necessary to manage the incident and during the periods arising from applicable legal liability.

Once the applicable periods—contractual or legal—have concluded, Ironchip will apply the principles of data minimization and will limit retention in accordance with the GDPR, proceeding to delete the data through blocking, anonymization, or secure erasure. These operations will be carried out in compliance with applicable regulations and the procedures defined in Ironchip's Information Security and Privacy Management System.

10. Data Recipients and Disclosures

Data processed through the Service may be disclosed only to those third parties whose involvement is essential to ensure its proper operation and to comply with applicable legal obligations. First and foremost, the Client itself has access to the necessary information to manage its users, monitor access, and comply with its internal security and audit controls, as it acts as the Data Controller in relation to its users' data.

Additionally, certain technology providers collaborate with Ironchip in the delivery of the Service, providing hosting infrastructure, messaging systems for authentication factors, support tools, or essential technical solutions for log management and operational continuity. These third parties always act as Data Processors, bound by contracts that fully comply with Article 28 of the GDPR and that require them to process data solely for purposes related to the Service, under Ironchip's instructions and with appropriate security safeguards.

In situations involving a valid request from judicial, administrative, or law enforcement authorities, Ironchip may disclose the data it is legally required to provide, limiting such disclosure strictly to what is necessary to comply with the mandate and ensuring compliance with the GDPR and national regulations at all times.

Outside of these cases, Ironchip does not disclose personal data to third parties for purposes unrelated to the Service, nor does it sell such data or use it for third-party commercial or marketing actions. The processing of information is strictly limited to the secure, effective, and lawful provision of the identity product.

11. International Transfers

The processing of personal data associated with the Service is carried out, by default, within the European Economic Area (EEA), where Ironchip maintains its main infrastructure and applies the security safeguards required by European regulations. However, in order to provide certain components of the Service or to ensure its operational continuity, it may be necessary to rely on providers or infrastructures located outside the EEA. In such cases, any international transfer will only be carried out when it is essential for the provision of the Service and always under legal mechanisms that ensure a level of protection equivalent to that required by the GDPR. These mechanisms may include adequacy decisions, the signing of Standard Contractual Clauses, or the adoption of additional technical measures such as encryption or pseudonymization of the information, ensuring that the data remains protected at all times, even when outside the European environment. Ironchip will not carry out international transfers that do not strictly comply with applicable legal requirements or that compromise the security or confidentiality of the data processed.

12. Information Security

The protection of personal data is a core element of the Service and is integrated from its design, following the principle of privacy by design and by default, as established in Article 25 of the GDPR. With this approach, Ironchip applies a set of technical and organizational measures designed to ensure the confidentiality, integrity, and availability of information at all times. The Service uses encryption systems for both communications and stored data, as well as secure binding mechanisms between the user and their devices to prevent unauthorized access.

The processing of information is based on strict minimization criteria, meaning that only data essential for authentication and security is processed, applying pseudonymization or tokenization techniques where possible to further reduce data exposure. These measures are complemented by a robust identity management and access control model, along with continuous monitoring aimed at detecting potentially anomalous or risky activities.

The secure operation of the Service is also supported by an event logging system designed to maintain the necessary traceability for security purposes, as well as periodic testing to verify its resilience against threats and vulnerabilities. Additionally, Ironchip maintains incident management procedures, as well as continuity and recovery plans that ensure the restoration of the Service in the event of failures or contingencies. All of this is developed within a compliance framework aligned with internationally recognized standards such as ISO 27001 and ISO 27701, as well as the requirements of the National Security Framework (Esquema Nacional de Seguridad), reinforcing Ironchip's commitment to the secure and responsible processing of data.

13. Record of Processing Activities

Ironchip maintains its own Record of Processing Activities, in which it documents in detail all processes related to the operation of the Service, thus complying with the provisions of Article 30 of the GDPR. This record includes the necessary information to demonstrate the Service's proactive accountability, describing the categories of data processed, the associated purposes, the applicable legal bases, and the security measures in place to ensure their protection.

In parallel, the Client is required to maintain their own Record of Processing Activities regarding the personal data of their internal users, as they act as the Data Controller within their organization. Both records must be consistent with each other in those aspects where the data flow depends on the interaction between the Client and Ironchip, especially during audits, compliance reviews, or requests from supervisory authorities. This coordination ensures complete traceability and allows each party to demonstrate compliance with their respective legal obligations in terms of data protection.

14. User Rights

Users of the Service retain at all times the rights granted to them under the General Data Protection Regulation, which means they may request information from Ironchip regarding the processing of their personal data, correct any inaccurate data, request its deletion when no longer necessary or when they believe it has been improperly processed, object to certain uses, or request that processing be restricted in specific situations. They may also receive their data in a structured, commonly used format for transfer to another provider, and request human review of decisions based solely on automated processing that may significantly affect them.

To exercise any of these rights, users may contact Ironchip via email at dpo@ironchip.com or by written communication sent to Calle Beurko Viejo, 17 – 48902 Barakaldo (Bizkaia), clearly indicating the request they wish to make. Ironchip will respond to requests within the timeframes and conditions set out in the GDPR and Spanish data protection legislation.

If a user believes that their request has not been properly addressed, or that there has been a violation of their rights, they may file a complaint with the Spanish Data Protection Agency (Agencia Española de Protección de Datos) via its official website www.aepd.es, without prejudice to their right to first contact Ironchip in an attempt to resolve any issue directly and effectively.

15. Changes and Modifications to this Policy

Ironchip may modify this Privacy Policy when necessary to adapt it to new legal obligations, updated criteria from data protection authorities, or improvements and developments to the Service itself. Any changes will be incorporated with the aim of maintaining accurate and up-to-date information about the processing, ensuring that both users and the Client always have access to the current version.

When the modifications introduce relevant changes in the way data is processed or in the intended purposes, Ironchip will clearly and proactively notify both the Client and affected users, allowing them to understand the scope of the changes before they come into effect. In this way, the relationship with the Service remains informed and in compliance with the applicable legal framework.

Last Updated: January 2026