



# Privacy Policy

Website

Your Next Generation Identity

# Table of Contents

<b>Applicable Regulations</b>	<b>4</b>
<b>BASIC INFORMATION ON DATA PROTECTION</b>	<b>4</b>
<b>1. Identity and Contact Details of the Data Controller</b>	<b>5</b>
Data Controller:	5
Data Protection Officer	5
<b>2. Purposes of Personal Data Processing</b>	<b>5</b>
Provision of Services, Technical Support, and Service Improvement and Development	6
Handling Requests and Inquiries	6
Communication and Marketing	6
Management of Electronic Forms	6
<b>3. Legal Basis for Processing</b>	<b>7</b>
<b>4. Categories of Personal Data Processed</b>	<b>7</b>
Identification and contact details:	7
Data derived from interactions with the company	7
Browsing data and use of electronic services	7
<b>5. Data Retention Period</b>	<b>8</b>
As a general rule	8
Electronic forms and specific inquiries	8
Data blocking and deletion	8
<b>6. Data Recipients</b>	<b>8</b>
Service providers and data processors	8
Competent authorities and legal compliance	8
International Data Transfers	9
<b>7. Data Subject Rights and How to Exercise Them</b>	<b>9</b>
Rights Recognized by the GDPR	9
How to Exercise Your Rights	10
Information to Include in Your Request	10
Sustainability and Accessibility	11
Response Timeframes	11
Cost of the Procedure	11
Complaints to the Supervisory Authority	11
Contact of the Data Protection Officer	11
<b>8. Source of Personal Data</b>	<b>11</b>
<b>9. Obligation to Provide Personal Data</b>	<b>12</b>
Mandatory Data	12
Optional Data	12
Responsibility for the Data Provided	12
Updating Personal Data	13
<b>10. Existence of Automated Decision-Making, Including Profiling</b>	<b>13</b>
<b>11. Social Media Policy</b>	<b>13</b>
Use of Social Media by the Data Controller	13

Commitment to Privacy	14
Social Media Interactions	14
External Links and Third-Party Content	14
User Rights	14
<b>12. Information on the Use of Cookies</b>	<b>14</b>
<b>13. Security Measures</b>	<b>15</b>
Security Measures Applied on the Website	15
Limitations of Internet Security	15
User Recommendations	15
<b>14. Sending of Commercial Communications</b>	<b>16</b>
User Consent	16
Objection and Withdrawal of Consent	16
Data Retention	16
Commitment of the Data Controller	16
<b>15. Acceptance and Consent</b>	<b>17</b>
<b>16. Privacy Policy Updates</b>	<b>17</b>

This Privacy Policy applies to the processing of personal data of customers and/or users of <https://www.ironchip.com>, hereinafter referred to as the WEBSITE, which is owned by the company IRONCHIP TELCO, S.L., hereinafter referred to as the DATA CONTROLLER.

## 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, and, insofar as it does not contradict the aforementioned Regulation, with 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.

By providing us with their data, the customer and/or user declares that they have read and understood this Privacy Policy and give their unequivocal and express consent to the processing of their personal data in accordance with the purposes and terms set out herein.

## BASIC INFORMATION ON DATA PROTECTION

<b>Controller</b>	IRONCHIP TELCO, S.L.
<b>Data Protection Officer (DPO)</b>	María Llanas Villa – Compliance Team Contact: <a href="mailto:dpo@ironchip.com">dpo@ironchip.com</a>
<b>Purpose</b>	<b>Service provision:</b> Technical support, free trials, product improvement and development. <b>Handling requests and inquiries:</b> Responses via forms, email, or chatbot. <b>Communication and marketing:</b> Sending newsletters, event invitations, and commercial communications with consent. <b>Electronic form management:</b> Processing of requests and inquiries.
<b>Legal Basis for Processing</b>	<b>Performance of a contract:</b> Management of contracted services and technical support. <b>Legal compliance:</b> Tax, accounting, and regulatory obligations. <b>Consent:</b> Sending of commercial communications and newsletters. <b>Legitimate interest:</b> Security, fraud prevention, and internal analysis.
<b>Categories of Personal Data</b>	<b>Identification and contact:</b> Name, address, phone number, email address. <b>Interactions:</b> Inquiries, requests, and data provided through forms. <b>Browsing:</b> Cookies, IP address, use of electronic services.
<b>Retention Period</b>	<b>General:</b> As long as there is an active relationship or until deletion is requested. <b>Forms and inquiries:</b> Until the request is handled. <b>Newsletters:</b> Until the data subject unsubscribes. <b>Blocked data:</b> Retained for legal periods for accountability purposes.
<b>Data Recipients</b>	<b>Service providers:</b> Technology, communication, and support services. <b>Authorities:</b> For compliance with legal obligations. <b>International transfers:</b> To the U.S. via HubSpot Inc., under the EU-U.S. Adequacy Decision.

<b>Data Rights</b>	<b>Subject</b>	Access, rectification, erasure, objection, restriction, and data portability. <b>Exercise:</b> By emailing <a href="mailto:dpo@ironchip.com">dpo@ironchip.com</a> with identification and details of the requested right. <b>Response time:</b> 1 month (extendable to 2 months in complex cases).
<b>Source of the Data</b>		<b>Direct:</b> Web form, inquiries, or communications. <b>Commercial relationship:</b> Data generated from traffic, browsing, or interactions.
<b>Data Security</b>		<b>SSL encryption:</b> Protection of data in electronic forms. <b>ReCAPTCHA:</b> Prevention of automated access. <b>Secure hosting:</b> Amazon servers within the European region.
<b>Use of Cookies</b>		The website uses cookies for functionality, analytics, and personalization. More information in the <a href="#">Cookies Policy</a> .
<b>Sending of Commercial Communications</b>		Sent only with consent. Free unsubscribe via <a href="mailto:dpo@ironchip.com">dpo@ironchip.com</a> .
<b>Policy Updates</b>		Modifications made to adapt to legal or technological changes. Notification will be provided on the website. Periodic review is recommended.
<b>Social Media Policy</b>		Profiles on LinkedIn, X, YouTube, and Instagram. Used to inform, share content, and respond to inquiries. Privacy is respected in accordance with each platform's regulations..

## 1. Identity and Contact Details of the Data Controller

### Data Controller:

- Company name: IRONCHIP TELCO, S.L.
- N.I.F.: B-95880332
- Address: Calle Beurko Viejo, 17 - 48902 Barakaldo, Bizkaia (Spain)
- Phone: (+34) 944 075 954
- Email: [info@ironchip.com](mailto:info@ironchip.com)

### Data Protection Officer

IRONCHIP TELCO, S.L. has appointed a Data Protection Officer, who can be contacted for any inquiry or request related to personal data protection at:

- Email: [dpo@ironchip.com](mailto:dpo@ironchip.com)
- Address: Avenida Manuel Gorria 63 – Local 1, Madrid - Spain.

## 2. Purposes of Personal Data Processing

The **DATA CONTROLLER** uses the personal data provided by clients and/or users for the following purposes:

## Provision of Services, Technical Support, and Service Improvement and Development

- Provide technical support and assistance for the products and/or services.
- Offer free trials of products and/or services upon user request.
- Conduct internal statistical and market studies to develop new functionalities and services.

## Handling Requests and Inquiries

- Respond to information requests and inquiries submitted through available contact channels, such as electronic forms, email, or chatbot.
- Contact data subjects to respond to specific questions regarding products and/or services.

## Communication and Marketing

- Send commercial communications related to products and/or services, provided the data subject has given their consent.
- Manage invitations to events, seminars, and webinars related to the company's activities.
- Facilitate subscription to the newsletter to inform about news, offers, and promotions.

## Management of Electronic Forms

The **DATA CONTROLLER** provides various electronic forms on its website, designed to facilitate interaction with clients and users. The personal data collected through these forms are processed for the following general purposes:

- Handling Requests and Inquiries: Respond to user inquiries and provide information about products and/or services, as well as send commercial communications, provided the data subject has given consent.
- Newsletter Subscription: Enable users to receive updates, offers, and promotions related to the products and/or services through electronic newsletters.
- Free Trials of Products and Services: Provide access to test environments or free versions of products and/or services offered by the company.
- Technical Support Management: Create and manage user accounts to provide support related to contracted products and services.
- Real-Time Communication: Provide a direct contact tool through a chatbot to address questions or receive specific user requests.

If any of the requested data on the forms is required to process the request, this mandatory nature will be clearly indicated at the time of collection. Failure to provide the required data may prevent the corresponding request or inquiry from being processed.

### 3. Legal Basis for Processing

The processing of personal data carried out by the **DATA CONTROLLER** is based on the following legal grounds, in accordance with the provisions of the General Data Protection Regulation (GDPR):

#### 1. Performance of a contract or pre-contractual measures

Processing is necessary for the management and provision of the contracted services, technical support, and required assistance.

#### 2. Compliance with a legal obligation

The processing of data is carried out to comply with applicable regulations, as well as to respond to requests from competent authorities.

#### 3. Data subject's consent

Where necessary, the processing of personal data—such as sending commercial communications, subscribing to newsletters, or participating in free trials of products and/or services—will be carried out only when the data subject has given their consent, which may be withdrawn at any time.

#### 4. Legitimate interest of the controller

Processing is based on the controller's legitimate interest in ensuring the security of systems, preventing fraud, optimizing services, and conducting statistical analyses or internal studies that enable the development of new features and improvements to the products and services offered.

### 4. Categories of Personal Data Processed

The **DATA CONTROLLER** collects and processes the following categories of personal data in the course of its activities, depending on the purposes described above:

#### Identification and contact details:

- First and last name
- Postal address
- Contact phone numbers
- Email address
- Identifiers on electronic communication platforms (e.g., WhatsApp, Telegram)

#### Data derived from interactions with the company

Information collected through electronic forms, emails, phone calls, or chats, such as: user inquiries, requests for free trials of products or services, and information provided for newsletter subscriptions or commercial communications.

#### Browsing data and use of electronic services

Information automatically collected during the use of the website, applications, cookies, and other similar technologies, as detailed in the Cookies Policy.

## 5. Data Retention Period

The **DATA CONTROLLER** will retain the personal data provided by data subjects for the following periods:

### As a general rule

Data will be retained as long as there is an active relationship between the data subject and the DATA CONTROLLER, unless the data subject requests its deletion.

### Electronic forms and specific inquiries

Data collected through electronic forms on the website will be retained for as long as necessary to respond to the data subject's request or while an active relationship exists, unless the data subject requests the deletion of their data or withdraws their consent.

In the case of data related to newsletter subscriptions or commercial communications, data will be retained until the data subject requests to unsubscribe.

### Data blocking and deletion

Once the relationship ends and the legal retention periods have been fulfilled, the data will be securely deleted.

If the personal data is relevant for the establishment, exercise or defense of legal claims, it will be duly blocked for the applicable statute of limitations period. Blocked data will be made available only to judicial authorities or competent public administrations and will not be used for any other purposes.

## 6. Data Recipients

The **DATA CONTROLLER** may disclose the personal data of data subjects to third parties only when necessary to fulfill the purposes described in this privacy policy or in cases provided by law. Specifically, the recipients of the data may include:

### Service providers and data processors

- Companies providing services to the **DATA CONTROLLER**, such as:
  - Technological services, including cloud storage providers and technical support.
  - Electronic communication services and newsletter management.
- These third parties will process personal data only in accordance with the instructions of the **DATA CONTROLLER**, under a contract that ensures data confidentiality and security.

### Competent authorities and legal compliance

- Public administrations, tax authorities, and regulatory bodies, when necessary to comply with legal obligations.

- Law enforcement agencies, judicial authorities, or supervisory bodies, in the event of legal requirements or investigations related to unlawful activities.

## International Data Transfers

The **DATA CONTROLLER** informs that, for the management of the commercial relationship, international transfers of personal data are carried out outside the European Economic Area (EEA) to the United States, through **HubSpot Inc.**, a service provider we use to optimize our business and communication activities.

These transfers are carried out under appropriate safeguards in accordance with the General Data Protection Regulation (GDPR), specifically through the **European Commission's Adequacy Decision of July 10, 2023**, known as the [EU-U.S. Data Privacy Framework](#). This framework ensures that personal data transferred to the United States benefits from a level of protection that is adequate and equivalent to that established under European regulations. For greater transparency, you can access HubSpot Inc.'s Privacy Policy through the following link: [HubSpot Privacy Policy](#).

The **DATA CONTROLLER** is committed to ensuring that these international data transfers are carried out in compliance with all necessary safeguards and security measures to protect your personal data, such as:

- Adequacy decisions issued by the European Commission, where available.
- Standard contractual clauses approved by the European Commission, in cases where they are required.
- Certification mechanisms or binding corporate rules, where applicable, to enhance the protection of personal data.

For more information about this protection framework or the safeguards applied, you may consult the details on the European Commission's website or contact us through the means indicated in this privacy policy.

The **DATA CONTROLLER** is committed to ensuring that international data transfers comply with the principles of security, confidentiality, and data protection established by the GDPR.

## 7. Data Subject Rights and How to Exercise Them

In compliance with the provisions of the General Data Protection Regulation (GDPR) (Regulation EU 2016/679) and the Spanish Organic Law on the Protection of Personal Data and Guarantee of Digital Rights (LOPDGDD), our company provides all data subjects with a clear, accessible, and sustainable procedure for exercising their rights in relation to their personal data.

### Rights Recognized by the GDPR

The following rights may be exercised by data subjects with respect to the processing of their personal data:

- **Right of access:** Allows you to obtain confirmation as to whether we are processing your personal data, access such data, and receive detailed information about its processing.
- **Right to rectification:** The ability to correct or complete inaccurate or incomplete personal data.
- **Right to erasure:** Also known as the “right to be forgotten,” it allows you to request the deletion of personal data when it is no longer necessary for the purposes for which it was collected, among other circumstances.
- **Right to object:** Allows you to object to the processing of your personal data based on legitimate interests or for direct marketing purposes.
- **Right to restriction of processing:** Allows you to temporarily restrict the use of your data in certain cases, for example, while its accuracy is being verified or a complaint is being resolved.
- **Right to data portability:** Allows you to receive the personal data you have provided to us in a structured, commonly used, and machine-readable format, and to transmit it to another data controller.

## How to Exercise Your Rights

To exercise any of your rights, our company provides data subjects with an exclusively digital method, in line with our Environmental Policy Commitment Statement, which prioritizes sustainability and the reduction of environmental impact. The enabled method is:

- Email: Please send your request to [dpo@ironchip.com](mailto:dpo@ironchip.com), attaching the rights request form, which you can download here: [Rights Request Form \(PDF\)](#).

## Information to Include in Your Request

To ensure proper handling of your request, you must provide the following information:

### 1. Identification of the requester:

- Full name.
- A copy of an official document proving your identity (ID card, passport, NIE).

### 2. Clear description of the right you wish to exercise:

- Specify the right you are exercising (access, rectification, erasure, objection, restriction, or portability), along with any additional information needed to process your request.

### 3. Contact method to receive the response:

- Email address.

### 4. Additional documentation:

- Any supporting documents or relevant information that may help in processing your request.

## Sustainability and Accessibility

By adopting this digital mechanism, we contribute to reducing unnecessary paper use and promote responsible business practices. If you encounter difficulties using the digital method, you may contact our customer service at (+34) 944 075 954, where you will receive personalized guidance to complete the process.

## Response Timeframes

Once your request is received, we will proceed to analyze it and provide a response within a maximum period of one month. In the case of complex or multiple requests, this period may be extended by an additional two months, with prior notice given to the data subject within the first month.

Responses to requests will be provided exclusively in digital format, via the email address provided by the data subject. Exceptionally, if a justified need for a physical response is demonstrated, the company will assess such requests on a case-by-case basis.

## Cost of the Procedure

Exercising your rights is free of charge. However, if the requests are clearly unfounded or excessive (e.g., repetitive), we reserve the right to charge a reasonable fee based on administrative costs or to refuse to act on the request.

## Complaints to the Supervisory Authority

If you believe that we have not properly addressed your rights request, you have the right to file a complaint with the Spanish Data Protection Agency (AEPD) via their website [www.aepd.es](http://www.aepd.es), or by contacting them directly.

## Contact of the Data Protection Officer

For inquiries related to data protection, you may also contact our Data Protection Officer (DPO):

- Email: [dpo@ironchip.com](mailto:dpo@ironchip.com)

## 8. Source of Personal Data

The **DATA CONTROLLER** may collect personal data from data subjects through different sources, detailed as follows:

**a) Data provided directly by the customer and/or user:** Data voluntarily provided by the customer or user, either:

- By completing electronic forms on the website or physical forms enabled for the collection of personal data.
- During the contractual relationship, through communications such as information requests, inquiries, complaints, or data updates.

The customer and/or user is responsible for ensuring the **truthfulness** and **accuracy** of the data provided.

**b) Data generated through the business relationship:** Data indirectly generated during the provision of contracted services and the maintenance of the business relationship. These include, among others:

- **Traffic and technical activity data**, such as access logs or configurations on platforms.
- **Website browsing data**, such as IP addresses or interactions within private areas of the website, provided that they comply with the applicable regulations on cookies and similar technologies.

The **DATA CONTROLLER** guarantees that all collected data, regardless of its origin, will be processed in accordance with current data protection regulations, applying appropriate measures to ensure their security and confidentiality.

If the customer or user updates or modifies their data, they must inform the **DATA CONTROLLER** to ensure that the data is accurate and up to date, in accordance with the data quality principle established by the GDPR.

## 9. Obligation to Provide Personal Data

Providing personal data to the **DATA CONTROLLER** is, in general, voluntary. However, in some cases, the provision of certain data is necessary to fulfill the specific purposes of the processing.

### Mandatory Data

- In electronic forms, the fields marked as mandatory are essential for:
  - The provision of contracted services.
  - Responding to requests or inquiries made by the customer or user.
  - Complying with legal or contractual obligations.
- If the data subject does not provide the required mandatory data, the **DATA CONTROLLER** will not be able to process the corresponding request or formalize the contractual relationship.

### Optional Data

Data not marked as mandatory in the forms or requests will be considered optional. Failure to provide such data will not prevent the provision of services, but it may limit their customization or enhancement.

### Responsibility for the Data Provided

- The data subject guarantees the **truthfulness, accuracy, and timeliness** of the personal data provided.

- If the data is inaccurate, incomplete, or not up to date, the data subject shall be responsible for any potential harm caused to the **DATA CONTROLLER** or to third parties.

## Updating Personal Data

To ensure that the information processed is accurate and up to date, it is recommended that the data subject notify the **DATA CONTROLLER** of any changes to their personal data.

The **DATA CONTROLLER** undertakes to process only the data necessary for the described purposes, ensuring compliance with the data minimization principle established in the General Data Protection Regulation (GDPR).

## 10. Existence of Automated Decision-Making, Including Profiling

The **DATA CONTROLLER** informs that **no automated decision-making, including profiling**, is carried out that produces legal effects concerning the data subjects or significantly affects them, in accordance with Article 22 of the General Data Protection Regulation (GDPR).

All decisions related to the processing of your personal data are made with human intervention, ensuring individual and transparent assessment in each case.

For any questions or inquiries related to the processing of your data, you may contact the **DATA CONTROLLER** through the channels indicated in this privacy policy.

## 11. Social Media Policy

The **DATA CONTROLLER** maintains active profiles on the following social media platforms:

- **LinkedIn:** <https://www.linkedin.com/company/ironchip>
- **X (formerly Twitter):** [https://twitter.com/Ironchip\\_Telco](https://twitter.com/Ironchip_Telco)
- **YouTube:** <https://www.youtube.com/@ironchip7626>
- **Instagram:** <https://www.instagram.com/ironchip.telco>

On these platforms, the **DATA CONTROLLER** acts as the controller of the personal data of users who interact with its profiles, including followers, subscribers, fans, and any person who posts comments, inquiries, or interacts through these social media platforms.

### Use of Social Media by the Data Controller

The **DATA CONTROLLER** uses its social media profiles to:

- Inform users about updates, services, products, or news related to the company's activities.
- Share relevant or interesting content, such as current events, third-party publications, or information considered useful to followers.

- Respond to inquiries or interactions made by users on social media, within the functional limits of each platform.

## Commitment to Privacy

- Under no circumstances will users' personal data be used for purposes other than those permitted by the social media platforms themselves without the data subject's explicit consent.
- The DATA CONTROLLER will not collect additional information about users beyond what is allowed by the platforms unless the user gives their explicit consent.

## Social Media Interactions

- Users are responsible for the information they post on these platforms, including mentions, comments, or inquiries, and must comply with the usage rules of each social network.
- If sensitive or confidential information is received from users through social media, the DATA CONTROLLER commits to handling such information with the utmost discretion and, where appropriate, requesting the use of more secure communication channels.

## External Links and Third-Party Content

- Social media platforms may include links to external websites or third-party content not managed by the DATA CONTROLLER. The company is not responsible for the accuracy, legality, or privacy policies of such content.

## User Rights

Users may exercise their rights of access, rectification, erasure, objection, restriction, and data portability in accordance with the GDPR, by directly contacting the DATA CONTROLLER through the means indicated in this privacy policy.

For more information on how these social media platforms handle personal data, users are encouraged to consult the privacy policies of each platform.

## 12. Information on the Use of Cookies

The **DATA CONTROLLER** informs that this website uses cookies and similar technologies to ensure its proper functioning, enhance the user experience, analyze web traffic, and, in some cases, personalize the content and services offered.

For detailed information about the use of cookies, the types of cookies used, their specific purposes, and how to manage or disable them, we invite you to consult our Cookies Policy, accessible via the following link: [Cookies Policy](#).

By continuing to browse our website, you accept the use of cookies in accordance with the terms set out in our Cookies Policy.

## 13. Security Measures

The **DATA CONTROLLER** guarantees the implementation of appropriate technical and organizational measures in accordance with the provisions of the General Data Protection Regulation (GDPR, EU 2016/679) and the Organic Law on Data Protection and Guarantee of Digital Rights (LOPDGDD, 3/2018), with the aim of protecting the personal data of clients and users, as well as their rights and freedoms.

### Security Measures Applied on the Website

#### 1. Data Encryption (SSL):

The website has an SSL certificate enabled across the entire domain, ensuring the encrypted transmission of personal data provided by users through electronic forms. This protects the information against unauthorized access during its transmission over the Internet.

#### 2. Protection Against Automated Traffic (reCAPTCHA):

The reCAPTCHA system is used to detect and block traffic generated by bots or automated programs, ensuring that only real users can interact with the electronic forms used to collect personal data.

#### 3. Secure Hosting:

The website is hosted on servers provided by Amazon.com, with an IP address assigned within the European range, complying with the security and data protection regulations applicable in the European Union.

#### 4. Confidentiality and Protection Against Unauthorized Access:

All collected information is stored and managed under strict confidentiality policies, using advanced security measures to prevent unauthorized access, misuse, manipulation, deterioration, or loss of personal data.

### Limitations of Internet Security

Despite the implemented measures, the client and/or user must be aware that absolute security in computer systems and data transmission over the Internet cannot be guaranteed. There is a possibility, albeit remote, that the information provided could be intercepted and processed by unauthorized third parties.

### User Recommendations

To contribute to information security, users are advised to:

- Use secure networks when sending personal information.
- Avoid sharing confidential data in public or insecure environments.
- Keep their devices protected by updating software and using appropriate security tools.

The **DATA CONTROLLER** is committed to continuously monitoring the implemented security measures, adapting them to technological advancements and new risks, in line with the security principles established by the GDPR and LOPDGDD.

For more information about our security policies, you can contact us through the channels indicated in this privacy policy.

## 14. Sending of Commercial Communications

In compliance with the provisions of Law 34/2002, of July 11, on Information Society Services and Electronic Commerce (LSSI-CE), as well as applicable complementary regulations, the **DATA CONTROLLER** guarantees that all commercial communications made electronically will be clearly identifiable as such and will contain the necessary information to identify the sender.

### User Consent

By completing the electronic forms available on the website and affirmatively checking the consent boxes, the client and/or user:

1. Accepts the processing of their personal data according to the purposes described in this privacy policy.
2. Gives their express, free, and unequivocal consent to receive commercial communications related to products and/or services offered by the **DATA CONTROLLER** through:
  - Email.
  - Telephone.
  - SMS/MMS.
  - Instant messaging platforms such as WhatsApp or Telegram.
  - Other equivalent electronic communication means.

### Objection and Withdrawal of Consent

The client and/or user has the right to object to the processing of their data for promotional purposes or to withdraw their consent to receive commercial communications at any time. This can be done through a simple and free procedure by sending an email to [dpo@ironchip.com](mailto:dpo@ironchip.com) with the subject: "**UNSUBSCRIBE**" or "**DO NOT SEND**".

### Data Retention

The personal data provided for the purpose of sending commercial communications will be retained:

- As long as the data subject does not withdraw their consent or request to unsubscribe.
- For the time necessary to comply with legal obligations, if applicable.

### Commitment of the Data Controller

The **DATA CONTROLLER** guarantees that:

- All commercial communications will comply with the principles of transparency and clarity established by applicable regulations.
- The necessary technical and organizational measures will be adopted to protect the personal information processed for commercial purposes.

For any further questions or clarifications related to the sending of commercial communications, the client and/or user may contact the **DATA CONTROLLER** through the means indicated in this privacy policy.

## 15. Acceptance and Consent

The client and/or user declares having been duly informed about the conditions related to the protection of their personal data, in accordance with the provisions of this Privacy Policy. By providing their data through the electronic forms available on the website or through other communication means, the client and/or user expressly accepts and consents to the processing of said data by the **DATA CONTROLLER**, in the manner and for the purposes detailed in this policy.

Likewise, the client and/or user acknowledges that certain services offered on the website may be subject to specific conditions that include provisions regarding the protection of personal data. In such cases, those conditions will be clearly and accessibly communicated to the data subject before the collection or processing of their data.

Acceptance of this policy implies the client and/or user's explicit consent to:

- The processing of their personal data in accordance with the purposes described herein.
- The use of electronic means to communicate relevant and commercial information, provided that the corresponding consent has been granted.

The client and/or user may withdraw their consent at any time, without affecting the lawfulness of the processing based on the consent prior to its withdrawal. To do so, they may exercise their rights through the channels indicated in this Privacy Policy.

## 16. Privacy Policy Updates

The **DATA CONTROLLER** reserves the right to amend this Privacy Policy in order to adapt it to:

- Legislative or judicial changes.
- New interpretations or guidelines issued by the Spanish Data Protection Agency or other supervisory authorities.
- Industry practices or technological advances that may affect the way we process personal data.

Any changes to the privacy policy will be communicated to users through this website, and, where appropriate, consent will be requested again in cases where the amendment involves personal data processing based on this legal basis.

Additionally, this Privacy Policy may be supplemented with other documents such as:

- Legal Notice.
- Cookie Policy.

- General Terms and Conditions of Contracting, if certain products and/or services include specific provisions on personal data protection.

Users are encouraged to review this Privacy Policy periodically to stay informed about how their personal information is protected and any potential updates. In case of questions, they may contact the **DATA CONTROLLER** through the channels indicated in this policy.

**Last Updated:** January 2026