IRRICONTROL ONE PLATFORM PRIVACY POLICY

Information Security and Cyber Defense

1. PRIVACY COMMITMENT STATEMENT

IRRICONTROL CONTROLE INTELIGENTE DE IRRIGAÇÃO S.A. ("**IRRICONTROL**"), together with **Grupo Bauer do Brasil**, is fundamentally committed to respecting privacy, protecting personal data and ensuring transparency in the processing of information collected through the **IRRICONTROL ONE Platform** (the "**Platform**").

This Privacy Policy (the "**Policy**") describes, in a clear and accessible manner, how we collect, use, store, share and protect the personal data of our Users and Customers, in strict compliance with the **Brazilian General Data Protection Law (LGPD – Law No. 13.709/2018)**, the ***General Data Protection Regulation (GDPR – Regulation (EU) 2016/679)*** for operations in the European Union, the ***California Consumer Privacy Act (CCPA)*** and other U.S. state privacy laws, Canada's ***Personal Information Protection and Electronic Documents Act (PIPEDA)***, and all other data protection laws in force in the 26 countries where the IRRICONTROL ONE Platform operates.

By using the IRRICONTROL ONE Platform, you acknowledge that you are aware of the terms of this Policy and consent to the processing of your personal data for the purposes described herein.

2. PROCESSING AGENTS AND THEIR ROLES

For the purposes of the applicable data protection laws, the roles in the processing of personal data within the IRRICONTROL ONE ecosystem are defined as follows:

Agent	Identification	Role and Description
Customer (Contracting Party)	The individual or legal entity that owns the farm and contracts IRRICONTROL's services.	**Data Controller**: The Customer is responsible for decisions regarding the processing of data of its employees and operators registered on the Platform.
IRRICONTROL	IRRICONTROL CONTROLE INTELIGENTE DE IRRIGAÇÃO S.A. (CNPJ/ME 26.941.490/0002-03).	**Data Processor / Service Provider**: Processes personal data on behalf of, and in accordance with the lawful instructions of, the Controller (Customer).
Sub-processors	Cloud infrastructure providers (such as AWS, Azure or Google Cloud) and payment gateways (such as Stripe).	**Data Sub-processors**: Entities engaged by the Processor to assist in the provision of technical and financial services.

3. PERSONAL DATA COLLECTED BY THE PLATFORM

The IRRICONTROL ONE Platform collects only the data strictly necessary to enable the technical operation, billing, support and security of the intelligent automation systems.

3.1. Registration and Billing Data (Provided by the Customer/User)

This data is essential for issuing invoices, billing and business communications:

- **Identification Data**: Full name, corporate name, CPF or CNPJ (or an equivalent international tax identification document) and State Registration number;
- **Contact Data**: E-mail address, mobile phone number and technical contact phone number;
- **Address Data**: CEP/*Postal Code*, full address, city, state and country (for billing and correspondence purposes).

3.2. Technical and Property Operation Data (Collected Automatically)

This data is collected to enable telemetry, automation and remote control features:

- **Geolocation Data**: Exact geographic coordinates (latitude and longitude) of the property and of the automated equipment (pivots, pumps, etc.);
- **Infrastructure and Equipment Data**: Complete technical specifications of the automated equipment used, the farm's time zone, and the billing day of the energy and water bills;
- **Access and Operation Logs**: Complete history of commands sent to the Platform (e.g., turning pivots on/off, changing speed, etc.), IP address, date, time and identification of the User who performed the action.

3.3. Payment Data (Processed by a Third-Party Gateway)

To process financial transactions and recurring subscription payments, we use the **Stripe** payment gateway. Credit card data and confidential payment information are entered directly into Stripe's secure, encrypted environment and are not viewed, processed or stored on IRRICONTROL's servers.

4. PURPOSES OF DATA PROCESSING

Personal data collected by the Platform is processed on the basis of internationally recognized legal grounds:

Data Category	Processing Purpose	Example of Legal Basis
Registration and Billing Data	Billing processing, tax management, invoice issuance and subscription charging.	Performance of Contract / Legal Obligation
Geolocation and Operation Data	Enabling remote control, automation and intelligent monitoring of equipment in the field.	Performance of Contract
Access and Security Logs	Access monitoring, command auditing, fraud prevention and assurance of the system's cybersecurity.	Legitimate Interest / Legal Obligation (e.g., Brazilian Internet Civil Framework – Marco Civil da Internet)

This document is controlled by the Information Security department. All rights to this document are reserved. Reproduction, use or disclosure to third parties without the express authorization of BAUER is prohibited. Copies of this document will be considered "uncontrolled" unless otherwise indicated and may be deemed intellectual property, and any infringer will be subject to all sanctions and the full weight of the applicable legislation.

Technical Contact Data	Provision of specialized remote technical support, resolution of field incidents and delivery of security alerts.	Performance of Contract

5. SHARING OF PERSONAL DATA

IRRICONTROL **does not sell, rent or transfer personal data to third parties for advertising or marketing purposes**. Data is shared strictly to enable the technical and financial operation of the Platform and is limited to the following partners:

- **Cloud Providers**: Data storage and hosting on highly secure global servers (such as AWS, Azure or Google Cloud);
- **Payment Gateways**: Secure, encrypted payment processing through the Stripe platform;
- **Bauer Group / Affiliates**: Internal sharing of administrative, support and corporate governance data, ensuring the same rigorous level of data protection worldwide;
- **Public Authorities**: Compliance with legal and regulatory obligations or court orders issued by competent bodies (such as the ANPD in Brazil or equivalent international authorities).

---

6. INTERNATIONAL DATA TRANSFERS

As a platform with global operations, Irricontrol One uses high-standard international cloud server infrastructure (such as AWS or Google Cloud). Consequently, personal data may be transferred, stored and processed on servers located outside the user's territory of origin (including the United States, the European Union or Brazil).

6.1. Legal Safeguards

IRRICONTROL ensures that all international transfers of personal data are carried out with the highest level of security and in strict compliance with applicable regulations, including ANPD Resolution No. 8/2025 for Brazil. We use appropriate safeguard mechanisms, such as:

- **Standard Contractual Clauses (*SCCs*)** incorporated into contracts with cloud providers;
- **Engagement of providers holding international certifications** in privacy and information security (such as SOC 2 and ISO 27001);
- **Assurance of compliance with GDPR guidelines** for data transferred to the European Union;
- **Compliance with specific data localization requirements** in jurisdictions that require them (such as Russia and Kazakhstan), as detailed in the Multinational Compliance Appendix.

6.2. Multinational Compliance Appendix

For users located outside Brazil, all specific legal provisions set forth in **ANNEX I – Multinational Compliance Appendix of the IRRICONTROL ONE Platform** also apply; it details the compliance requirements for each of the 26 countries in which the Platform operates.

This document is controlled by the Information Security department. All rights to this document are reserved. Reproduction, use or disclosure to third parties without the express authorization of BAUER is prohibited. Copies of this document will be considered "uncontrolled" unless otherwise indicated and may be deemed intellectual property, and any infringer will be subject to all sanctions and the full weight of the applicable legislation.

7. INFORMATION SECURITY AND DATA RETENTION

IRRICONTROL adopts robust technical, administrative and organizational information security measures to protect personal data against unauthorized access, loss, destruction, alteration or any form of improper or unlawful processing.

7.1. Security Measures Implemented

- Encryption of data in transit (SSL/TLS) and at rest on servers (AES-256 standard);
- Strict logical access control to servers and databases, with multi-factor authentication (MFA) for administrators;
- Continuous monitoring of access logs and command auditing;
- Periodic, automated backups to ensure data integrity;
- Penetration testing and vulnerability scanning to proactively identify and remediate security risks.

7.2. Data Retention Period

IRRICONTROL will retain personal data only for the period necessary to fulfill the purposes for which it was collected, including compliance with contractual, tax and regulatory obligations or for the defense of judicial or administrative proceedings.

- **Data Deletion upon Termination**: After the contractual relationship ends, operation and registration data will be retained for the legal limitation period (generally 5 years for tax and civil purposes). Thereafter, it will be securely and permanently deleted from our systems or fully anonymized, eliminating any possibility of association with the data subject. In the event of a confirmed security incident, IRRICONTROL will notify the Customer immediately and will assist in notifying the competent data protection authorities as required by applicable law.

---

8. DATA SUBJECT RIGHTS

In accordance with the applicable data protection laws (LGPD, GDPR, CCPA, PIPEDA and other international laws), Users and Customers have the following rights regarding their personal data processed by IRRICONTROL:

- **Confirmation and Access**: The right to confirm the existence of processing and to access their personal data processed by the Platform;
- **Correction**: The right to request the rectification of incomplete, inaccurate or outdated data;
- **Anonymization, Blocking or Erasure**: The right to request the restriction of processing or the deletion of unnecessary data or data processed in breach of the law;
- **Portability**: The right to request the transfer of their data to another service provider in a structured format;
- **Information on Sharing**: The right to know with which public or private entities IRRICONTROL has shared their data;

This document is controlled by the Information Security department. All rights to this document are reserved. Reproduction, use or disclosure to third parties without the express authorization of BAUER is prohibited. Copies of this document will be considered "uncontrolled" unless otherwise indicated and may be deemed intellectual property, and any infringer will be subject to all sanctions and the full weight of the applicable legislation.

- **Withdrawal of Consent**: The right to withdraw consent previously given for specific and optional purposes;
- **Non-Discrimination**: The right not to suffer any kind of discrimination, price change or service degradation for exercising their privacy rights.
- **Right to Be Forgotten (GDPR/CCPA):** The right to demand the permanent deletion of personal data in accordance with applicable international laws.

8.1. How to Exercise Your Rights

To exercise any of their rights or to ask questions about how their data flows, data subjects may submit a formal request to our Data Protection Officer (DPO) by e-mail at: **dpo.brasil@irricontrol.com.br**.

Requests will be reviewed and answered free of charge within the regulatory deadline set by applicable law (a maximum of 15 business days in Brazil, 30 days in the European Union under the GDPR, and equivalent deadlines in other jurisdictions).

---

9. UPDATES TO THIS POLICY

IRRICONTROL reserves the right to amend this Privacy Policy at any time to reflect Platform updates, ongoing cybersecurity improvements or global legislative changes.

Whenever there are material changes, Users will be notified through prominent notices on the Platform before the new rules take effect.

---

10. CONTACT AND DATA PROTECTION OFFICER (DPO)

For questions, suggestions or requests regarding the processing of your personal data, please contact us directly through our channels:

- **Data Protection Officer (DPO):** dpo.brasil@irricontrol.com.br

This document is controlled by the Information Security department. All rights to this document are reserved. Reproduction, use or disclosure to third parties without the express authorization of BAUER is prohibited. Copies of this document will be considered "uncontrolled" unless otherwise indicated and may be deemed intellectual property, and any infringer will be subject to all sanctions and the full weight of the applicable legislation.