ANNEX I – MULTINATIONAL COMPLIANCE APPENDIX OF THE IRRICONTROL ONE PLATFORM

INTRODUCTION

This Multinational Compliance Appendix forms an integral part of and supplements the Terms of Use, the Privacy Policy and the SaaS Agreement of the IRRICONTROL ONE Platform. It sets out the specific legal provisions and mandatory regulatory requirements that must be observed when the Platform is operated or when personal data is collected from data subjects located in the following jurisdictions outside Brazil:

Covered Jurisdictions: Brazil, Uruguay, Argentina, Chile, Paraguay, Peru, Colombia, Mexico, Bolivia, Venezuela, Australia, New Zealand, France, England (United Kingdom), Romania, Hungary, Italy, Moldova, Kazakhstan, Russia, Zambia, Egypt, Indonesia, Thailand, Algeria and the United States/Canada.

1. LATIN AMERICA

- 1.a. Uruguay (Law No. 18.331/2008)

Legal Basis: The processing of personal data of residents of Uruguay requires the prior, express, informed and written consent of the data subject, except in the cases provided for by law (such as the performance of contracts).

International Transfer: Uruguay is recognized by the European Union as a country with an adequate level of data protection. Transfers of data from Uruguay to IRRICONTROL's servers in Brazil are permitted, as Brazil adopts equivalent standards through the LGPD.

- 1.b. Argentina (Law No. 25.326/2000)

Data Subject Rights: Argentine data subjects have the right to access their data free of charge at intervals of no less than six months, unless they demonstrate a legitimate interest.

Database Registration: IRRICONTROL does not have a physical branch in Argentina at the time of the Platform's launch. Should the company establish a physical branch in Argentina in the future, databases containing personal information of local residents must be registered with the *Agencia de Acceso a la Información Pública (AAIP)*. IRRICONTROL will conduct full legal due diligence whenever a new market or branch is opened to ensure compliance with local laws.

- 1.c. Chile (Law No. 19.628 / Law No. 21.719/2024)

Legal Reform: In accordance with the recent legal reform (Law No. 21.719/2024), Chilean data subjects have robust rights of access, rectification, cancellation, objection and data portability.

Supervisory Authority: Complaints and inquiries from Users in Chile will be overseen by the new *Agencia de Protección de Datos Personales*.

- 1.d. Paraguay (Law No. 1.682/2001)

Consent: The processing of personal data in Paraguay requires the express consent of the data subject. Data relating to financial solvency and assets will not be collected or processed by the IRRICONTROL ONE Platform.

- 1.e. Peru (Law No. 29.733/2011)

Information Security: IRRICONTROL adopts the technical, organizational and legal security measures required by the Information Security Directive approved by Peru's Superintendency Resolution.

Data Flow: Peruvian Customers expressly authorize the transfer of their operational and personal data to IRRICONTROL's cloud servers located abroad.

- 1.f. Colombia (Law No. 1581/2012)

Prior Authorization: The processing of data of residents of Colombia requires the prior, express and informed authorization of the data subject, which must be obtained by the Customer (Controller) and kept available for audit.

Complaints Channel: Colombian Users may submit inquiries or complaints directly to IRRICONTROL, which will respond within the legal deadlines of 10 (ten) business days for inquiries and 15 (fifteen) business days for complaints.

- 1.g. Mexico (LFPDPPP/2010)

Privacy Notice: Customers and Users in Mexico will have access to the Privacy Notice in its short and full versions before any personal data is collected, in accordance with INAI guidelines.

ARCO Rights: Full guarantee of the rights of Access, Rectification, Cancellation and Objection (ARCO Rights) to Mexican Users.

- 1.h. Bolivia and Venezuela

Basic Compliance: In these jurisdictions, the processing of personal data is based on the general principles of informed consent, legitimate purpose, information security and confidentiality, in accordance with the respective national constitutions and general telecommunications laws.

2. EUROPEAN UNION AND UNITED KINGDOM (GDPR / UK GDPR)

- 2.a. Countries Covered: France, Romania, Hungary, Italy, England (United Kingdom) and Moldova

Territorial Scope: For all Users and data subjects located in these countries, the General Data Protection Regulation (GDPR – Regulation (EU) 2016/679) applies in full and, in the case of the United Kingdom, the UK GDPR and the Data Protection Act 2018. In Moldova, Law No. 195/2024, which fully transposes the GDPR, applies.

Legal Bases for Processing: The processing of personal data under the GDPR is based strictly on the Performance of a Contract (Art. 6(1)(b)) for billing and telemetry operational data, and on Legitimate Interest (Art. 6(1)(f)) for cybersecurity and technical improvements to the Platform.

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.

Right to Be Forgotten and Portability: European data subjects have the right to demand the permanent deletion of their data (the "right to be forgotten"). IRRICONTROL will provide a button in the user profile to download their data in JSON format (structured, machine-readable JSON). For the permanent deletion of data, the user must send a formal request to the Data Protection Officer (DPO) e-mail address: **dpo.brasil@irricontrol.com.br**. The operation is technically feasible and will be carried out upon formal documentation of the request.

Incident Notification (72 hours): In the event of a security incident resulting in a confirmed leak of personal data, IRRICONTROL will notify the Customer (Controller) immediately and will assist in notifying the respective supervisory authorities (such as the CNIL in France, the ICO in the United Kingdom or the CNPDCP in Moldova) within a maximum of 72 (seventy-two) hours after becoming aware of the incident.

International Transfer (Standard Contractual Clauses): Transfers of data from Europe to IRRICONTROL's servers in Brazil are backed by the Standard Contractual Clauses (SCCs) adopted by the European Commission, ensuring an adequate level of data protection.

3. ASIA-PACIFIC

- 3.a. Australia (Privacy Act 1988)

Australian Privacy Principles (APPs): The processing of personal data of residents of Australia fully complies with the 13 APPs set out in the *Privacy Act 1988*.

Notifiable Data Breaches (NDB): In the event of a data breach likely to result in serious harm to any individual, IRRICONTROL will immediately notify the affected data subjects and the *Office of the Australian Information Commissioner (OAIC)*.

- 3.b. New Zealand (Privacy Act 2020)

Information Privacy Principles (IPPs): Strict compliance with New Zealand's IPPs, including the new IPP 3A (in force since May 1, 2026), which requires greater transparency regarding the indirect collection of data.

Breach Notification: Mandatory notification to the *Privacy Commissioner* in the event of security incidents that cause or are likely to cause serious harm.

- 3.c. Thailand (PDPA/2019)

Explicit Consent: The processing of data of residents of Thailand requires the explicit consent of the data subject.

Data Subject Rights: Thai Users have the right to request the restriction of the processing of their data and to object to processing based on legitimate interest.

- 3.d. Indonesia (Law No. 27/2022)

Data Localization: Given that IRRICONTROL ONE ***does not store "critical operational data of national infrastructure"***, as defined by Indonesian law, it is not currently necessary to establish a database physically located in Indonesia. IRRICONTROL will periodically assess the need for local cloud database mirroring for Indonesian customers as regulations evolve.

4. NORTH AMERICA

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.

- 4.a. United States (CCPA and State Laws)

No Sale of Data: IRRICONTROL declares that it does not sell or commercially share the personal data of Users residing in the United States for targeted advertising purposes, in accordance with the *California Consumer Privacy Act (CCPA)* and other state privacy laws (such as those of Virginia, Colorado and Texas).

Right to Opt Out: Although IRRICONTROL does not sell data, U.S. Users are guaranteed the right to request that their data not be shared with third parties for non-essential purposes. Such requests may be made manually by formally contacting the Data Protection Officer (DPO) at: **dpo.brasil@irricontrol.com.br**.

- 4.b. Canada (PIPEDA)

Fair Information Principles: Processing complies with the 10 fair information principles established by the *Personal Information Protection and Electronic Documents Act (PIPEDA)*.

Incident Notification: Mandatory recording of all security breaches and notification to the *Office of the Privacy Commissioner of Canada* where there is a real risk of significant harm to individuals.

5. AFRICA, CENTRAL ASIA AND THE MIDDLE EAST

- 5.a. Egypt (Personal Data Protection Law of 2020)

Consent and Rights: Processing requires explicit written or electronic consent. Egyptian Users have the right to withdraw their consent at any time by submitting a formal request to the DPO's e-mail address. The withdrawal of consent will be recorded in the audit logs, identifying the internal user who executed it.

Licensing: Where applicable, IRRICONTROL will obtain the necessary licenses from Egypt's Personal Data Protection Authority for the processing of data of local citizens.

- 5.b. Russia (Federal Law No. 152-FZ)

Data Localization and Compliance: In accordance with Article 18(5) of Federal Law No. 152-FZ, IRRICONTROL ONE acknowledges that the processing of personal data of citizens of the Russian Federation must comply with the data localization requirements established by Russian law. The IRRICONTROL ONE Platform is structured to provide, as needed and upon the Customer's request or a regulatory requirement, a *mirror database* or storage infrastructure physically located in the territory of the Russian Federation, thereby ensuring full compliance with the applicable legislation.

Flexible Technical Architecture: IRRICONTROL adopts a modular and scalable technical architecture that allows data localization solutions to be implemented according to the specific requirements of each Customer and jurisdiction. If a Russian Customer requests it, or local legislation requires the storage of its personal data on servers located in Russia, IRRICONTROL will provide this functionality at previously agreed costs, ensuring compliance with Federal Law No. 152-FZ.

- 5.c. Kazakhstan (Personal Data Protection Law of 2013)

Data Localization and Compliance: Similarly to Russia, Kazakhstan's legislation establishes data localization requirements for the processing of its citizens' personal information. IRRICONTROL ONE is structured to provide, as needed and upon the Customer's request or a regulatory requirement, a *mirror database* or

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.

storage infrastructure physically located in the territory of the Republic of Kazakhstan, thereby ensuring full compliance with the applicable legislation.

Flexible Technical Architecture: IRRICONTROL adopts a modular and scalable technical architecture that allows data localization solutions to be implemented according to the specific requirements of each Customer and jurisdiction. If a Kazakh Customer requests it, or local legislation requires the storage of its personal data on servers located in Kazakhstan, IRRICONTROL will provide this functionality at previously agreed costs, ensuring compliance with Kazakh law.

- 5.d. Zambia and Algeria (Law No. 18-07/2018)

Prior Declaration: In Algeria, the processing of personal data of local residents requires a prior declaration to the National Authority for the Protection of Personal Data. Processing is based on express consent and the legitimate purpose of performing the SaaS agreement.

General Compliance: In Zambia, the processing of personal data follows the general data protection principles established in local legislation, with an emphasis on transparency, security and data subject rights.

6. GENERAL COMPLIANCE PROVISIONS

- 6.a. Data Subject Rights

In all jurisdictions, IRRICONTROL recognizes and respects the following data subject rights:

- **Right of Access:** Confirmation that data is being processed and access to it;
- **Right to Rectification:** Correction of incorrect or outdated information;
- **Right to Erasure:** Removal of unnecessary data or upon formal request;
- **Right to Portability:** Transfer of data in a structured format (JSON/XML);
- **Right to Object:** Refusal of processing for specific purposes;
- **Right to Withdraw Consent:** Revocation of previously granted authorization.

- 6.b. Channels for Exercising Rights

All data subject rights may be exercised through the following channels:

- **Data Protection Officer (DPO) E-mail:** dpo.brasil@irricontrol.com.br
- **General Support E-mail:** contato@irricontrol.com.br
- **Support Phone:** +55 19 2112-9856

- 6.c. Response Deadlines

IRRICONTROL undertakes to respond to requests to exercise rights within the following deadlines:

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.

- **GDPR (Europe):** 30 days, extendable by a further 60 days in complex cases;
- **LGPD (Brazil):** 15 business days;
- **Other jurisdictions:** In accordance with applicable local law, with an initial response within 15 business days.

o 6.d. Documentation and Audit

All requests to exercise rights, as well as the actions taken by IRRICONTROL in response, will be recorded in audit logs identifying the internal user responsible for execution, the date, the time and a description of the action taken.

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.