IRIUSRISK DATA PROCESSING ADDENDUM

May 2025

This Data Processing Addendum ("Addendum") is entered into by and between **IriusRisk, S.L.** ("IriusRisk," "we," "us," or "Service Provider") and the customer identified in the applicable Order Form ("Customer"), and forms an integral part of the CUSTOMER SUBSCRIPTION TERMS FOR IRIUSRISK CLOUD SERVICES ("Agreement").

To the extent any provision in this Addendum conflicts with a provision in the Agreement concerning the processing of personal data, the terms of this Addendum shall control.

This Addendum is required insofar as, in the course of providing the Services, IriusRisk may process two categories of Personal Data: (i) contact details of the Customer's personnel, in respect of which IriusRisk acts as an independent controller for its own business administration purposes; and (ii) additional Personal Data made available by the Customer when receiving support or related services, including but not limited to data relating to end users or employees, in respect of which IriusRisk acts as a processor on behalf of the Customer.

1. DEFINITIONS

Terms used in this DPA shall have the meanings given to them under Regulation (EU) 2016/679 (the General Data Protection Regulation or GDPR), including but not limited to "Controller", "Processor", "Data Subject", "Personal Data", "Processing", and "Supervisory Authority".

2. PURPOSE AND SCOPE

This Addendum governs the processing of personal data by IriusRisk on behalf of Customer as necessary to perform the services under the Agreement.
The nature, purpose, and details of the processing activities, including the categories of personal data and data subjects involved, are described in Appendix I.

3. COMPLIANCE WITH LAWS

Each Party shall comply with all applicable laws relating to privacy and data protection, including the EU General Data Protection Regulation (2016/679), the EU Privacy and Electronic Communications Directive (2002/58/EC) as implemented in each jurisdiction, and any amending or replacement legislation as updated or replaced from time to time (collectively and individually, "Data Protection Laws").

4. PROCESSOR OBLIGATIONS

IriusRisk, in its capacity as Processor, shall:
4.1. Process Personal Data solely on the documented instructions of the Controller, including in relation to international data transfers, unless required to act otherwise under Union or Member State law;
4.2. Ensure that all persons authorised to process the Personal Data are subject to appropriate confidentiality obligations;
4.3. Implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk (as further detailed in Appendix II);

4.4. Only engage subprocessors with prior specific or general written authorisation of the Controller, as set out in Appendix I;
4.5. Assist the Controller in responding to Data Subject rights requests and in complying with its obligations under Articles 32 to 36 of the GDPR;
4.6. At the choice of the Controller, delete or return all Personal Data at the end of the provision of the Services and delete any existing copies unless Union or Member State law requires retention;
4.7. Make available to the Controller all information necessary to demonstrate compliance with this DPA and allow for and contribute to audits conducted by the Controller or an auditor mandated by the Controller;
4.8. Ensure that Processing is conducted strictly under the Controller's instructions; and
4.9. Maintain a record of Processing activities as required under Article 30(2) GDPR.

5. CONTROLLER OBLIGATIONS

Customer, in its capacity as Controller, shall:
a) Ensure that it has all necessary rights and lawful bases to provide Personal Data to IriusRisk for Processing;
b) Implement appropriate technical and organisational measures to ensure and to be able to demonstrate compliance with the GDPR;
c) Make available to Data Subjects, upon request, the essential elements of this DPA;
d) Maintain records of processing activities under its responsibility, where required by law.

6. DATA SUBJECTS' RIGHTS

Each Party shall, to the extent applicable, assist the other Party in responding to requests from Data Subjects exercising their rights under the GDPR. Requests shall be handled without undue delay and, where feasible, within one month of receipt, in accordance with Articles 12–23 GDPR. Where a request is not fulfilled, the Data Subject shall be informed without delay and provided with the reasons, as well as their right to lodge a complaint.

7. SUBPROCESSING

IriusRisk may engage subprocessors to support the performance of the Services, subject to the following conditions:
a) Each subprocessor shall be bound by a written agreement that imposes data protection obligations no less protective, in substance, than those set out in this DPA;
b) The Controller shall be notified in advance of any intended changes concerning the addition or replacement of subprocessors and shall have the right to reasonably object on legitimate grounds;
c) A current list of authorised subprocessors shall be maintained in Appendix I and updated from time to time;
d) IriusRisk shall use reasonable efforts to ensure that any subprocessor performs its obligations in accordance with the applicable terms of this DPA, and shall remain responsible for its contractual obligations under this DPA where the subprocessor fails to fulfil its data protection duties.

8. INTERNATIONAL DATA TRANSFERS

Any transfer of Personal Data to a country outside the European Economic Area (EEA) shall be undertaken in compliance with Chapter V of the GDPR. Where required, such transfers shall be governed by the European Commission's Standard Contractual Clauses for controller-to-processor transfers, as referenced in Appendix III.

9. SECURITY INCIDENT NOTIFICATION

In the event of a Personal Data Breach affecting Customer Personal Data, IriusRisk shall notify the Controller without undue delay and in any event within seventy-two (72) hours of becoming aware of the breach. Such notice shall include all relevant information to assist the Controller in meeting its legal obligations.

10. RETURN OR DELETION OF DATA

Upon expiration or termination of the Agreement, IriusRisk shall, at Customer's written election, return or delete all personal data, unless otherwise required by applicable law to retain such data.

11. AUDITS AND ASSESSMENTS

Upon written request, and subject to reasonable confidentiality obligations, IriusRisk shall provide Customer with information reasonably necessary to demonstrate compliance with this Addendum, including participation in audits to the extent required by Applicable Data Protection Laws.

APPENDIX I

a) Details of the processing activities

Category	Details
Data Subjects	- Authorized users of the services - Employees and contractors of Customer
Personal Data Categories	- Identifiers (e.g., name, email address, alias) - Professional info (e.g., job title, company) - Location data (e.g., country) - Technical data (e.g., IP address, device identifiers, usage metrics)
Nature & Purpose of Use	Processing activities necessary to provide and support the services, including collection, storage, consultation, usage, and deletion, consistent with the Agreement.

b) Authorised subprocessors

Subprocessor	Service	Location
Amazon Web Services EMEA SARL	Platform hosting	AWS data center location as agreed between the Customer and IriusRisk (EU).
Cloudflare Inc.	Web Application Firewall (WAF)	United States Of America (USA)
New Relic Inc.	Full stack observability to monitor, analyze, debug, and improve performance.	United States Of America (USA) Data stored in EU data center.
IriusRisk Inc	Provision of the services and support	United States Of America (USA)
IriusRisk Ltd	Provision of the services and support	United Kingdom (UK)
UserPilot Inc	Optional User Enablement feature (onboarding and analytics)	United States Of America (USA)
Microsoft Ireland Operations Limited	Optional AI feature	Ireland (EU)
Google Cloud EMEA Limited	Optional AI feature	Ireland (EU)

IriusRisk will make reasonable efforts to notify Customer at least thirty (30) days in advance of any additions or replacements to its list of subprocessors. Customer may reasonably object to such changes in writing within that notice period only if the proposed change poses a material and demonstrable risk to the protection of personal data. In the event of such an objection, the parties shall work together in good faith to resolve the matter. Lack of objection within the notice period shall be deemed acceptance of the change.

APPENDIX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

1. Physical Access Controls. IriusRisk will take reasonable measures to prevent physical access, such as security personnel and secured buildings, to prevent unauthorized persons from gaining access to personal data.

2. System Access Controls. IriusRisk will take reasonable measures to prevent personal data from being accessed and/or used without authorization. These controls shall vary based on the nature of the processing and will include at minimum authentication via password and/or two-factor authentication, documented authorization processes, documented change management processes, and logging of access of the data.

3. Data Access Controls. IriusRisk will take reasonable measures to ensure that personal data is only accessible and manageable by properly authorized staff, direct database query access is restricted, and access rights to and within data processing systems are established and enforced to ensure that only authorized persons can access the data processing systems and the data within that they have the authorization to access. Moreover, these controls will be established and enforced to ensure that personal data cannot be read, copied, modified, or removed without authorization in the course of processing.

In addition to Sections 1-3, IriusRisk warrants it has an implemented access policy which requires that access to its system environment, to personal data, and to other data are limited to authorized personnel only.

4. Transmission Controls. IriusRisk will take reasonable measures to ensure that it is possible to check and establish to which entities the transfer of personal data by means of data transmission facilities is envisaged so personal data cannot be read, copied, modified, or removed without authorization during electronic transmission or transport. Without limiting the foregoing, IriusRisk shall ensure personal data is encrypted (at least 256 bit encryption) in transit and storage.

5. Input Controls. IriusRisk will take reasonable measures to make possible checking and establishing whether and by whom personal data has been entered into data processing systems, modified, or removed. IriusRisk will take reasonable measures to ensure that the personal data source is under the control of the Customer and the personal data integrated into the IriusRisk's systems is managed by a secure file transfer from the IriusRisk and the data subject.

6. Data Backup and Deletion. IriusRisk will ensure that secured backups are conducted on a regular basis and that personal data is encrypted when stored to protect against accidental destruction or loss when hosted by IriusRisk. IriusRisk will ensure that personal data can be permanently and irretrievably deleted in accordance with industry standards, including by wiping or disposing of storage devices.

7. Logical Separation. IriusRisk will ensure that Customer personal data is logically segregated on IriusRisk's systems to ensure that personal data that is collected for different purposes will be processed separately.

8. Additional requirements. IriusRisk will (a) implement detection, prevention, and recovery controls to protect its systems (network, hosting, and application) against malware and other threats to the confidentiality, integrity and availability of personal data, (b) conduct security awareness training to all personnel, and (c) will prohibit and disable the use of non-managed remote devices for storing or carrying, or in use with machines handling personal data Remote devices include without limitation flash drives, CDs, DVDs, external hard drives or other mobile devices.

APPENDIX III

STANDARD CONTRACTUAL CLAUSES

Controller to Processor

For the purposes of international data transfers in accordance with Article 46 of the GDPR, the Parties agree that the European Commission's Standard Contractual Clauses for Controller to Processor transfers (Module 2), as adopted by Commission Implementing Decision (EU) 2021/914 of 4 June 2021, shall apply and are hereby incorporated by reference into this Data Processing Addendum.

The full text of the Standard Contractual Clauses is available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021D0914.