IRIUSRISK DATA PROCESSING ADDENDUM

May 2025

This Data Processing Addendum ("**Addendum**") is entered into by and between **IriusRisk, Inc.** ("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 necessary because, in the course of providing services, IriusRisk may access and process contact details of Customer personnel (for which IriusRisk acts as a business or controller), as well as additional personal data under Customer's control (e.g., data of end users or employees) when delivering support and related services, for which IriusRisk acts as a service provider or processor.

1. DEFINITIONS

Capitalized terms used in this Addendum and not otherwise defined shall have the meanings assigned to them under Applicable Data Protection Laws. "Applicable Data Protection Laws" means all U.S. federal and state laws and regulations concerning privacy and data protection, including but not limited to the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020 (collectively, "CCPA/CPRA"), and other similar U.S. state privacy statutes.

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 Data Protection Laws in connection with its performance of this Addendum and the Agreement.

4. ROLE OF IRIUSRISK AS SERVICE PROVIDER / PROCESSOR

When acting as a service provider or processor under Applicable Data Protection Laws, IriusRisk agrees as follows:

4.1. IriusRisk shall not retain, use, or disclose personal data except as necessary to provide the services under the Agreement or as otherwise permitted by law.
4.2. IriusRisk shall not sell or share personal data as those terms are defined under Applicable Data Protection Laws.
4.3. IriusRisk shall not combine personal data with other data except as expressly permitted under Applicable Data Protection Laws.

4.4. IriusRisk shall comply with all applicable obligations imposed on service providers under Applicable Data Protection Laws.

5. SECURITY SAFEGUARDS

IriusRisk shall implement and maintain appropriate administrative, technical, and physical safeguards designed to protect the security, confidentiality, and integrity of personal data, as further detailed in Appendix II.

6. INDIVIDUAL RIGHTS REQUESTS

To the extent required by Applicable Data Protection Laws, IriusRisk shall provide reasonable assistance to Customer in responding to verified consumer requests to exercise their rights.

7. USE OF SUBPROCESSORS

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 Annex 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. SECURITY INCIDENT NOTIFICATION

IriusRisk shall notify Customer without undue delay after becoming aware of any unauthorized access to or disclosure of personal data in IriusRisk's possession or control. Such notification shall include sufficient detail to enable Customer to comply with its legal obligations.

9. 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.

10. 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, Inc.	Platform hosting	AWS data center location as agreed between the Customer and IriusRisk.
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)
IriusRisk SL	Provision of the services and support and maintenance (HQ)	Spain
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 Inc	Optional AI feature	United States Of America (USA)
Google LLC	Optional AI feature	United States Of America (USA)

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.