KYRO Technical and Organizational Security Measures

To protect Customer Personal Data, KYRO maintains the technical and organizational security measures described on this page. This description of KYRO's Security Measures is intended to accompany KYRO's Data Processing Addendum or, if applicable, the superseding written agreement between Customer and KYRO

At all times while KYRO Processes Customer Personal Data, KYRO will: (a) maintain and follow a written information security program (including the adoption and enforcement of internal policies and procedures) designed to (a) help Customer secure Customer Personal Data against accidental or unlawful loss, access or disclosure, (b) identify reasonably foreseeable and internal risks to Customer Personal Data and unauthorized access to the Services, and (c) minimize Customer Personal Data risks, including through risk assessment and regular testing. KYRO will designate one or more employees to coordinate and be accountable for the information security program. The information security program will include the following Security Measures (as updated from time to time):

- Physical Access Controls: KYRO takes measures, such as security personnel and secured buildings, designed to (i) prevent unauthorized persons from gaining access to Customer Data, (ii) manage, monitor and log movement of persons into and out of KYRO facilities, and (iii) guard against environmental hazards such as heat, fire, and water damage.
- System Access Controls: KYRO takes measures designed to prevent unauthorized use of Customer Data. These controls may vary based on the nature of the Processing undertaken and may include, among other controls, authentication via passwords and two-factor authentication, documented authorization processes, documented change management processes, logging of access on several levels, system audit or event logging, and related monitoring procedures to proactively record user access and system activity for routine review.
- Data Access Controls: KYRO takes measures designed to ensure that Customer Data is accessible and manageable only by properly authorized staff, direct database query access is restricted, and application access rights are established and enforced to ensure that persons entitled to use a data processing system only have access to the Personal Data to which they have privilege of access, and that Customer Data cannot be read, copied, modified, or removed without authorization in the course of Processing
- Access Policy: In addition to the access control rules set forth in Subsections 1.1–1.3 above, KYRO implements an access policy under which access to its system environment, to Personal Data, and to other Customer Data is restricted to authorized personnel only.
- Input Controls: KYRO takes measures to ensure that: (i) the Customer Data source is under the control of Customer; and (ii) Personal Data integrated into KYRO's systems is managed by secured file transfer from Customer and the Authorized User subject.
- Data Backup: KYRO ensures that backups are made on a regular basis, are secured, and are encrypted when storing data to protect against accidental destruction or loss when hosted by KYRO.
- Organizational Management: KYRO maintains a dedicated staff responsible for the development, implementation, and maintenance of KYRO's data privacy and information security programs.
- Audit: KYRO maintains audit and risk assessment procedures for the purposes of periodic review and assessment of risks to the organization, monitoring and maintaining compliance, and reporting the condition of its information security and compliance to senior internal management.

- Policies: KYRO maintains data protection and information security policies and makes sure that policies and measures are regularly reviewed and where necessary, improve them
- Integration: KYRO communicates with Customer applications utilizing cryptographic protocols such as TLS 1.2 or above to protect information in transit over public networks. At the network edge, stateful firewalls, web application firewalls, and DDoS protection are used to filter attacks. Within the internal network, applications follow a multi-tiered model which provides the ability to apply security controls between each layer.
- Operations: KYRO maintains operational procedures and controls to provide for configuration, monitoring, and maintenance of technology and information systems according to prescribed internal and adopted industry standards, including secure disposal of systems and media to render all information or data contained therein as undecipherable or unrecoverable prior to final disposal. or release from Controller possession.
- Incident Response: KYRO maintains incident procedures designed to investigate, respond to, mitigate and notify of events related to Customer's data. or information assets. A dedicated network operations and security operations staff performs rapid monitoring and response capabilities to address alerts.
- Network Security: KYRO engages in network security controls such as providing for the use of enterprise firewalls and layered DMZ architectures, and intrusion detection systems and other traffic and event correlation procedures designed to protect systems from intrusion and limit the scope of any successful attack.
- Risk Management: KYRO utilizes vulnerability assessment, patch management, and threat protection technologies and scheduled monitoring procedures designed to identify, assess, mitigate and protect against identified security threats, viruses and other malicious code.
- Business Continuity: KYRO maintains business resiliency/continuity and disaster recovery procedures, as appropriate, designed to maintain service and/or recovery from foreseeable emergency situations or disasters. Testing is performed to evaluate the plans and recovery capabilities.

Additional information: For additional information on KYRO's security measures and compliance please refer to the information made available and updated periodically on the KYRO Trust Center https://security.kyro.ai/.