INTRODUCTION

Arxada places the utmost importance on Information Security and Data Privacy, implementing rigorous measures to ensure the highest standards of protection for our data, systems, and all stakeholders.

Outlined below are technical, organizational, and physical measures adopted by Arxada to safeguard information systems and data.

These controls ensure confidentiality, integrity, availability, and resilience.

MEASURES TO ENSURE THE SAFETY OF PERSONAL AND CONFIDENTIAL DATA DURING TRANSMISSION

Technical measures	
Encryption	Data is encrypted both in transit and at rest across the platform and at endpoints within Arxada. This encompasses the website, workspace, email communications, backups, and when using Arxada's company-provided VPN for secure remote access.
Secure communication	Secure communication protocols are deployed for email and file transfers.
Web Application Firewalls	These firewalls block attacks on our web application and APIs.
Network and Application Layer Firewalls	These firewalls block attacks against Arxada's network.
Data flows monitoring	Data flows are monitored to detect and block suspicious transactions.

Organizational Measures	
Global Information Security Policy	This policy governs the use of information resources and electronic communications systems by employees, consultants, and contractors of the company. All associates must comply with this policy.
Data Protection Policy	This policy establishes clear rules and guidance for Arxada employees, contractors and external agents on how to handle and protect personal data collected and processed by Arxada in compliance with the applicable data protection laws and regulations.
Global Acceptable Use Policy	Prescribes that corporate IT assets can be used only for work related purposes, along with the prohibition of installing third party tools without expressed approval.

Physical Measures	
Physical documents	Data transported in paper form is handled exclusively by authorized personnel within designated secure areas.
Shredders	Arxada provides secure means for destruction of paper documentation.
Confidential waste bins	Confidential data in paper format is disposed of within Arxada's confidential waste bins, which are securely transported offsite and destroyed.

MEASURES AGAINST DATA LOSS, DESTRUCTION, ALTERATION, AND UNAUTHORIZED ACCESS

To ensure protection against loss, destruction, alteration, or unauthorized access, Arxada implements additional technical, organizational, and physical measures:

Technical Measures	
Environment segregation	Separation of testing and production environments to prevent unauthorized access.
Resource access	Access to ARXADA information is controlled and monitored by conditional access policies.
Mailbox Security	Enhanced mailbox security through advanced threat detection with strict access controls and user awareness.
Endpoint vulnerability management	Continuous identification, assessment, and remediation of security weaknesses on all company devices using automated tools and patching workflows.
Intrusion detection and prevention systems	We use host-based intrusion detection and prevention systems to monitor and block malicious activities.
Secure authentication	Single sign on (SSO) and Multi-factor Authentication (MFA) is applied across Arxada's systems.
Automatic device lock	Automatic device lock is enforced after idle timeout to prevent unauthorized use.
Key management	Key Management Service with established rotation procedures to maintain security.
Limited access to logs	Audit logs are accessible only to authorized personnel to ensure confidentiality.
Suppliers Security Certifications	We operate with suppliers certified under ISO 27001, ISO 27017 and ISO 27018, SOC 1, SOC 2 and SOC 3, and BSI's C5.
Vulnerability Management	Regular vulnerability scanning to identify and mitigate risks.
VLAN segmentation	Network Segmentation uses VLANs to isolate network zones, limit threat propagation and protect critical systems.
Software assurance	Prior to deployment in the organization, all software is checked for threats.

Data leakage controls	We monitor and restrict the movement of sensitive data to prevent unauthorized disclosure.

Organizational Measures	
Authorization procedures	Access control management and authorization procedures are in place to ensure only authorized personnel can access intended systems and data.
Confidentiality and Data Processing Agreements	Contractual measures to ensure that data is accessed, used, and processed only by authorized parties, kept confidential, and handled in compliance with applicable data protection laws and defined security terms.
Policies and Procedures Review	Periodic system-driven reviews to ensure policies and procedures remain current and effective.
Password management	Employees must create strong, unique passwords in accordance with Arxada's Global Information Security policy.
Mobile device management	Associates must use only approved and managed devices, complying with Mobile Device Management settings.
Restricted admin access	Administrative privileges are granted strictly on a need-to-know basis and following the principle of least-privileges
Training and awareness	Includes onboarding security and data protection training with testing and annual refresher courses. Specific security training for individuals with privileged access.
Data retention policy	Defines retention periods, to ensure data is kept only as long as required by law, regulation, or business needs.
Asset Management	ARXADA maintains an up-to-date inventory of all information assets, including their classification and lifecycle management.
Cyber Incident Response	The company has established a cyber incident response policy, procedure and supporting structures. The response protocol is periodically tested.

Physical measures	
Access control	Physical access to Arxada facilities is restricted to authorized personnel using identification systems.
Badge	Employees and visitors are required to wear identification (i.e. badges) within Arxada premises.
Secure areas	Access to sensitive areas (server rooms, cabinets) is restricted to authorized personnel only.
CCTV	Video surveillance cameras are installed to monitor and record physical access to facilities.

VALIDATION AND SYSTEMATIC REVIEW OF SECURITY PRACTICES

Technical measures	
Security Frameworks	Arxada's security framework is aligned with NIST CSF 2.0., ensuring policies, procedures and processes systematically reviewed and updated when a significant change occur.
External audits and penetration tests	Scheduled security audits, penetration tests, and vulnerability scans are conducted across critical systems handling personal and confidential data.

Organizational Measures	
Change Management	A formal change management process evaluates the impact of proposed changes on data security and business resiliency.
Integrated Security Testing	Static and dynamic application security testing is embedded in development and deployment processes.
Architecture Reviews	Security considerations are incorporated into architecture reviews for new systems or technologies.
Third party security assessment	All SaaS products undergo a security assessment before implementation.

Security champions program	Selected employees promote security awareness and best practices within their teams.
Backup and Restore Procedures	Backup and restore procedures are documented and are tested monthly, to ensure data availability and integrity.
Risk management process	A structured risk management process identifies, assesses, and prioritizes risks to information assets, enabling timely mitigation.

MEASURES TO ADHERE TO THE PRINCIPLES OUTLINED IN THE GENERAL DATA PROTECTION REGULATION (GDPR), ARTICLE 5

Lawfulness, Fairness and Transparency
Arxada's Privacy Policy clearly outlines what personal data is processed, how it is processed, the purposes for processing, retention periods, and conditions for sharing data externally.
This information is publicly available through our Policy hub, Privacy Policy, Legal Disclaimer, ensuring transparency to data subjects.
Explicit and granular consent is obtained where required, with a simple mechanism allowing individuals to withdraw consent at any time.
Purpose Limitation
Data Flow enables Arxada to track when personal data is collected and to ensure that each processing activity is linked to a pre-defined and legitimate purpose. If a new purpose emerges, it is identified and assessed in line with established governance procedures before any processing takes place.
Records of Processing Activities (ROPA)documents Arxada's processing activities and supports purpose limitation by ensuring that purposes are clearly recorded, monitored, and reviewed periodically or when a significant change occurs.
Data Minimization
Use of pseudonymization and API connectors to reduce data duplication and ensure only necessary data is processed.

Project management for new initiatives includes a data assessment phase to determine what personal data is strictly required, preventing unnecessary collection.
Periodic reviews on processes and data retention schedules to confirm that data processing remains limited to what is essential and complies with defined retention periods.
Data Accuracy
Any data subject can request that their personal data be modified or updated. Employees can directly update their own personal data in HR systems.
Access controls ensure that only authorized personnel can modify data, based on a strict need-to-know basis.
Storage Limitation
Arxada's Global Records Retention Policy establishes guidelines for retention periods, considering applicable local requirements.
Periodic reviews are conducted to ensure adherence to the retention schedules and to confirm that data is not retained longer than necessary.
Integrity and Confidentiality
Security and privacy by design is embedded into our processes, supported by the security measures outlined in this document, ensuring that personal data is processed with appropriate technical and organizational safeguards against unauthorized or unlawful processing, accidental loss, destruction, or damage.
Accountability
Oversight by a DPO, CISO, and dedicated privacy and security teams.
ARXADA takes a top-down approach to data protection, enabling privacy and security by design and by default. Fostering a strong privacy culture across the organization.