

Data Protection Policy

Policy Reference : JLW-ISMS-PL-18
Revision No. : 00
Date : 03.09.2026

REVISION HISTORY

Rev. No	Date	Remarks
00	03.09.2026	Initial issue

1. Introduction

James L Williams Middle East (JLW) is committed to protecting the privacy and personal data of its employees, clients, consultants, subcontractors, suppliers, visitors and other individuals whose personal data is collected or processed during the course of its business activities.

This Data Protection Policy establishes the principles and requirements for the lawful, fair, transparent and secure processing of personal data throughout its lifecycle. It supports JLW's commitment to protecting personal data against unauthorized access, alteration, disclosure, loss or destruction while ensuring compliance with applicable law, regulatory and contractual obligations.

This policy is designed to support compliance with applicable personal data protection legislation in the jurisdictions where JLW operates, including the Kingdom of Saudi Arabia (KSA) and the United Arab Emirates (UAE), together with ISO/IEC 27001:2022 and recognized information security best practices.

These requirements apply to all processing of Personal Data

Where these requirements conflict with a more stringent general legal requirements, the more stringent requirements shall prevail.

2. Purpose

The purpose of this Policy is to establish a consistent framework for the collection, use, storage, sharing, retention, transfer and disposal of personal data processed by JLW.

The Policy aims to:

- Protect the privacy rights of individuals;
- Ensure personal data is processed lawfully and securely;
- Establish responsibilities for protecting personal data;
- Support compliance with applicable data protection legislation;
- Reduce privacy and information security risks throughout JLW's business operations.

3. Scope

This Policy applies to:

- All JLW Staff;
- Consultants;
- Subcontractors;
- Suppliers;
- Third parties processing personal data on behalf of JLW;
- All business units, offices and project sites operated by JLW.

This Policy applies to personal data processed in any format, including electronic records, paper records, emails, databases, CCTV recordings, collaboration platforms, mobile devices and cloud-based systems, throughout its complete lifecycle, including collection, storage, use, disclosure, transfer, retention and secure disposal.

4. Data Protection Principles

JLW is committed to processing personal data in accordance with the following principles:

Lawfulness, Fairness and Transparency: Personal data shall be processed lawfully, fairly and transparently. Individuals shall be provided with clear and accessible information regarding the personal data collected, the purpose of processing, the applicable lawful basis, and any authorized third parties with whom the data may be shared.

Purpose Limitation: Personal data shall be collected and processed only for specified, explicit and legitimate business purposes, and shall not be processed in a manner incompatible with those purposes.

Data Minimisation: Only personal data that is adequate, relevant and limited to what is necessary for the intended processing purpose shall be collected and processed.

Pseudonymisation: Where appropriate and practicable, pseudonymisation or other privacy-enhancing techniques shall be used to reduce the risk of identifying individuals. Any information required to re-identify a data subject shall be stored separately and protected using appropriate technical and organisational controls.

Accuracy: Reasonable steps shall be taken to ensure that personal data is accurate, complete and kept up to date. Inaccurate or incomplete personal data shall be corrected or updated without undue delay.

Integrity and Confidentiality: Appropriate technical and organisational measures shall be implemented to protect personal data against unauthorized or unlawful access, use, disclosure, alteration, loss or destruction.

Storage Limitation (Retention): Personal data shall be retained only for as long as necessary to fulfil the purpose for which it was collected or to satisfy applicable law, regulatory, contractual and business requirements.

Data Subject Rights: The rights of individuals shall be respected and facilitated in accordance with applicable legislation, including the rights to access, correct, erase, restrict or object to the processing of their personal data, where applicable.

Accountability: Appropriate governance, policies, procedures, records and controls shall be maintained to demonstrate compliance with applicable data protection legislation, regulatory requirements and this Policy.

5. Personal Data Handling Practices

JLW shall ensure that personal data is managed throughout its lifecycle using approved business processes and security controls.

Personal data shall only be:

- collected for legitimate business purposes;
- processed using an appropriate lawful basis;
- protected against unauthorized access;
- retained in accordance with approved retention requirements;
- shared only with authorized parties;
- securely disposed of when no longer required.

6. Lawful Basis for Processing

Personal data shall only be processed where an appropriate lawful basis exists under applicable legislation.

Such lawful bases may include:

- Consent of the individual;
- Performance of a contract;
- Compliance with legal obligations;
- Legitimate business interests;
- Protection of vital interests;
- Any other lawful basis permitted by applicable legislation.

7. Cross Border Transfer of Personal Data

Personal data may be transferred between JLW offices, project locations, service providers or cloud service providers where required for legitimate business purposes. A cross-border Transfer or Disclosure shall be limited to the minimum necessary, shall not prejudice national security or the vital interests of the country and shall use an adequate level of protection or an appropriate safeguard permitted by the applicable transfer regulation.

Any transfer of personal data across national borders shall comply with applicable law and regulatory requirements and appropriate safeguards shall be implemented to protect the personal data.

8. Privacy by Design

Privacy and data protection requirements shall be considered during the design, acquisition, implementation and modification of business processes, projects, information systems and technologies that process personal data.

9. Technical and Organizational Measures

JLW shall implement appropriate technical and organizational measures to protect personal data against unauthorized access, disclosure, alteration, loss, theft, or misuse. These measures include, but are not limited to, the following:

- **Data Encryption:** Personal data stored and transmitted through JLW's systems and cloud services shall be protected using appropriate encryption protocols to ensure its confidentiality and integrity.
- **Logical Access Controls:** Access to personal data shall be restricted to authorized personnel based on the principle of least privilege and role-based access. Multi-factor authentication (MFA) shall be implemented where appropriate to strengthen access security.
- **Physical Access Controls:** Physical access to offices and server rooms shall be restricted using access control system and monitored through measures such as CCTV surveillance, security alarm systems, visitor management procedures, and other appropriate physical security controls to prevent unauthorized access.
- **Data Minimization:** In accordance with the principles of privacy by design and privacy by default, only the minimum amount of personal data necessary to fulfil a legitimate business purpose shall be collected, processed, and retained.
- **Network and Infrastructure Security:** Firewalls, encryption technologies, endpoint protection, and other appropriate security controls shall be implemented to safeguard personal data against unauthorized access and cyber threats.
- **Employee Training and Awareness:** Employees shall receive regular training and awareness on data protection obligations, information security, and applicable policies and procedures to ensure the secure handling of personal data.
- **Vendor and Third-Party Management:** Appropriate due diligence shall be performed on third-party vendors and subcontractors that process personal data on behalf of JLW. Contractual agreements shall include adequate data protection, confidentiality, and information security requirements to ensure compliance throughout the supply chain.
- **Risk Assessments:** Regular information security and privacy risk assessments shall be conducted to identify vulnerabilities affecting personal data. Appropriate corrective actions and risk mitigation measures shall be implemented based on the assessment results.

- **Records of Processing Activities:** Accurate and up-to-date records of personal data processing activities shall be maintained, including data collection, use, storage, sharing, retention, and disposal. Such records shall include, where applicable:
 - **Consent Records:** Documentation demonstrating that valid consent has been obtained where consent is the legal basis for processing. Records shall demonstrate that consent was informed, specific, freely given, and capable of being withdrawn.
 - **Processing Activity Records:** Documentation of processing activities, including the purpose of processing, categories of data subjects and personal data, recipients of personal data, applicable laws, retention periods, and implemented security measures. These records shall be reviewed and updated periodically.
 - **Data Sharing and Transfer Records:** Records of all disclosures or transfers of personal data to third parties or across borders, including the identity of recipients, purpose of the transfer, applicable law and safeguards implemented to protect the personal data and ensure compliance with applicable law and regulatory requirements.

10. Information Security Controls

JLW shall implement and maintain information security controls that are proportionate to the sensitivity of the personal data being processed and the associated business risks. These controls shall be designed to protect personal data against unauthorized access, disclosure, alteration, loss or destruction throughout its lifecycle.

Information security controls shall be reviewed periodically to ensure their continued effectiveness and alignment with evolving legal, regulatory, contractual and business requirements.

The following controls shall be implemented, where appropriate, to support the protection of personal data:

10.1 Encryption

- Personal data shall be protected through appropriate encryption controls while at rest, in transit and, where technically feasible and appropriate, during processing.
- Cryptographic standards and encryption key management practices shall be implemented in accordance with JLW's Information Security requirements.

10.2 Data Loss Prevention (DLP)

- Appropriate controls shall be implemented to prevent the unauthorized disclosure, transfer or loss of personal data.
- Data Loss Prevention (DLP) technologies may be deployed, where appropriate, to monitor, detect and control the movement of sensitive information.

10.3 Network Security

- Network infrastructure shall be protected through appropriate security controls, including firewalls, secure network architecture, intrusion detection and prevention mechanisms, and network segmentation where appropriate.
- Network security controls shall be maintained to reduce the risk of unauthorized access to systems processing personal data.

10.4 Endpoint Security

- Devices used to process or access personal data shall be protected through appropriate endpoint security measures, including endpoint protection, malware protection, encryption and secure configuration.

- Endpoint devices shall be regularly updated and security patches applied in accordance with JLW's Vulnerability and Patch Management processes.

10.5 Security Monitoring and Logging

- Security events relating to systems processing personal data shall be monitored, logged and reviewed to detect, investigate and respond to actual or suspected security incidents.
- Security monitoring solutions, including Security Information and Event Management (SIEM) technologies where implemented, shall support timely detection and response to security events.

10.6 Backup and Recovery

- Appropriate backup and recovery processes shall be implemented to ensure the availability, integrity and recoverability of personal data.
- Backup media shall be adequately protected, and recovery procedures shall be periodically tested to verify their effectiveness in supporting business continuity and disaster recovery requirements.

The information security controls described in this Policy shall form part of JLW's Information Security Management System (ISMS) and shall be implemented in conjunction with the Company's Information Security policies, standards and procedures to ensure the confidentiality, integrity and availability of personal data throughout its lifecycle.

11. Data Subject Rights

Individuals whose personal data is processed by JLW may exercise their rights in accordance with applicable legislation.

These rights may include:

- Right to be informed;
- Right of access;
- Right to rectification;
- Right to erasure;
- Right to restrict processing;
- Right to object to processing where applicable;
- Right to withdraw consent where consent is the legal basis;
- Right to data portability where applicable.

JLW shall establish appropriate procedures to receive, assess and respond to requests from data subjects within the applicable legal timeframes or within 30 days, whichever is shorter JLW shall verify the requester's identity, document oral and written requests, provide Personal Data in a readable and clear format where applicable, and protect the Personal Data of other individuals, intellectual property and trade secrets.

12. Data Breach Management

JLW shall establish, implement and maintain documented procedures for the timely identification, reporting, assessment, containment, investigation, response and recovery of personal data breaches.

All actual or suspected personal data breaches shall be managed in accordance with Personal data breach response and management procedure (JLW-ISMS-PR-15). Where required by applicable law or regulatory requirements, JLW shall notify the relevant regulatory authorities and affected individuals within the prescribed timeframes or within 72 hours of becoming aware of the incident, whichever is shorter.

The data breach management process shall, at a minimum, include the following:

- Identification and Containment: Prompt identification, reporting and containment of personal data breaches to minimise their impact and prevent further unauthorized access, disclosure, alteration or loss of personal data.
- Assessment and Notification: Assessment of the nature, scope and potential impact of the breach, including determination of notification requirements to affected individuals, clients, regulatory authorities and other stakeholders, where required by applicable legislation or contractual obligations.
- Mitigation and Recovery: Implementation of appropriate corrective actions to mitigate the impact of the breach, restore affected systems and services, prevent recurrence, and verify the effectiveness of the actions taken through monitoring and review.

13. Third Party Processing

Third parties processing personal data on behalf of JLW shall be subject to appropriate due diligence and contractual requirements.

JLW shall ensure that suppliers, consultants, subcontractors and service providers implement appropriate technical and organisational measures to protect personal data.

14. Data Inventory

JLW shall maintain an inventory of personal data processed throughout its business operations.

Examples include:

- Employee records;
- Recruitment records;
- Payroll information;
- Visa and immigration records;
- Client contact information;
- Consultant and subcontractor records;
- Supplier information;
- Visitor management records;
- CCTV recordings;
- Project contact information.

15. Data Protection Responsibilities and Appointment of the Data Protection Officer

Management has appointed the Compliance Manager to undertake the additional responsibilities of the Data Protection Officer (DPO).

The DPO shall perform their responsibilities in co-ordination with the relevant Heads of Departments and seek guidance from the Contracts Manager.

The DPO and the respective Heads of Departments is responsible for:

- Monitoring compliance with applicable data protection laws, regulations, and internal policies;
- Advising management and employees on data protection obligations and requirements;
- Supporting and providing guidance on Data Protection Impact Assessments and other privacy risk assessments;
- Co-ordinating communications with relevant regulatory and supervisory authorities;
- Promoting data protection awareness and supporting employee training;
- Supporting the identification, assessment, investigation, reporting, and management of personal data breaches and other data protection incidents; and
- Reporting significant data protection risks, compliance matters, and incidents to management.

Management shall ensure that the DPO is provided with sufficient authority, access, resources, and organisational support to effectively discharge these responsibilities.

16. Privacy Impact Assessments

16.1. Personal Data Protection Initial Assessment

JLW shall perform an initial personal data protection assessment to evaluate the current state of the personal data protection environment. The assessment shall include, at minimum, the following:

- Identification of types of personal data being collected.
- Location and method of storage of personal data.
- Current processing and uses of personal data.
- Privacy challenges to meet compliance with the National Data Management Office's Personal Data Protection Regulations.

16.2. Impact Assessment

JLW shall conduct Privacy Impact Assessments (PIAs), or equivalent data protection risk assessments, where new or significantly changed projects, systems, technologies, business processes, or processing activities involving personal or sensitive personal data may present privacy risks.

Impact assessments shall ensure that data protection requirements are considered from the earliest stages of project planning and throughout the system or process lifecycle, in accordance with the principles of Privacy by Design and Privacy by Default.

The designated Data Protection Officer (DPO), or other responsible person, shall work with the stakeholders to:

- Identify and assess potential privacy and data protection risks;
- Recommend appropriate technical and organisational controls to mitigate identified risks;
- Ensure that impact assessments and mitigation measures are documented and maintained as evidence of compliance with applicable law and regulatory requirements;
- Monitor the implementation and effectiveness of agreed controls;
- Conduct periodic reviews where there are significant changes to processing activities, business operations, technologies, or the applicable risk environment; and
- Promote continual improvement by incorporating lessons learned and best practices into future assessments.

Where appropriate, the outcomes of impact assessments shall be reported to the Senior Leadership to support informed decision-making and effective governance.

17. Record of Processing Activities

JLW shall establish, maintain and periodically review a Record of Processing Activities (RoPA) (JLW-CL-FM-20), where required by applicable law, regulatory or contractual obligations, to demonstrate accountability and compliance with data protection requirements.

The RoPA shall, as applicable, include information such as:

- The business function or controller responsible for the processing activity;
- The purpose and lawful basis for processing;
- Categories of personal data and data subjects;
- Categories of recipients with whom personal data may be shared;
- Cross-border transfers of personal data, where applicable;
- Applicable retention periods; and
- The technical and organisational measures implemented to protect personal data.

The designated Data Protection Officer (DPO), or other responsible person, shall ensure that the RoPA is regularly reviewed and updated to reflect changes in business processes, systems, legal requirements or data processing activities.

The RoPA shall be maintained as evidence of JLW's compliance with applicable data protection legislation and shall be made available to authorised regulatory authorities, auditors or other authorised parties, where required by applicable law, regulatory or contractual obligations. The RoPA shall be retained for a minimum period of five years in accordance with the Company's Records Retention Policy or in compliance with applicable law and regulatory requirements.

18. Training and Awareness

JLW shall establish and maintain a data protection training and awareness programme to ensure that all employees, contractors and other relevant personnel understand their responsibilities for protecting personal data and complying with applicable law, regulatory and contractual requirements.

The designated Data Protection Officer (DPO), or other responsible person, shall oversee the development, implementation and periodic review of the training and awareness programme to ensure its continued effectiveness and relevance.

The training and awareness programme shall, at a minimum:

- Provide employees with an understanding of JLW's data protection policies, procedures and their responsibilities for handling personal data securely;
- Include induction training for new employees and periodic refresher training for existing employees;
- Address applicable data protection legislation, privacy principles and recognised best practices relevant to business operations;
- Promote awareness of emerging privacy risks, information security threats and changes to legal or regulatory requirements;
- Include role-based training, where appropriate, for personnel with specific responsibilities for processing personal data;
- Encourage awareness through appropriate communication, awareness campaigns, practical examples and other educational activities;
- Assess the effectiveness of the training programme and maintain records of employee participation and completion; and
- Be periodically reviewed and updated to reflect changes in legislation, business processes, technologies, emerging risks and lessons learned from incidents or audits.

19. Monitoring and Audit

JLW shall establish and maintain processes to monitor, measure and periodically audit its personal data processing activities to ensure ongoing compliance with this Policy, applicable law and regulatory requirements, contractual obligations, and recognised information security and privacy standards.

The designated Data Protection Officer (DPO), or other responsible person, shall oversee the monitoring and audit programme to evaluate the effectiveness of JLW's data protection controls and identify opportunities for continual improvement.

The monitoring and audit programme shall, at a minimum:

- Monitor personal data processing activities to verify compliance with this Policy and applicable law and regulatory requirements;
- Establish appropriate performance measures and indicators to assess the effectiveness of data protection controls;
- Conduct periodic internal audits and reviews of data protection practices, with additional audits performed where warranted by business needs or identified risks;
- Identify non-conformities, compliance gaps and opportunities for improvement;
- Document audit findings, recommendations and agreed corrective actions;

- Report significant findings and recommendations to Senior Management;
- Ensure that corrective actions are assigned, implemented and monitored for effectiveness; and
- Conduct follow-up reviews, where necessary, to verify the timely implementation and effectiveness of corrective actions.

Monitoring and audit results shall be used to support continual improvement of JLW's data protection framework, policies, procedures and controls.

20. Compliance

Compliance with this Policy is mandatory for all employees, contractors, consultants, vendors and third-party service providers who collect, access, process or manage personal data on behalf of JLW.

Department Managers are responsible for ensuring that this Policy is implemented within their respective areas of responsibility. The Compliance Department, in coordination with the Information Security function, shall monitor implementation, support compliance activities, and report significant non-compliance issues to the Top Management, where appropriate.

All third-party service providers processing personal data on behalf of JLW shall comply with applicable law, regulatory and contractual data protection and information security requirements.

21. Regulatory Compliance

This Policy establishes the minimum requirements for the protection of personal data throughout JLW. JLW shall comply with all applicable data protection and privacy laws, regulations and contractual obligations in the jurisdictions in which it operates.

Where local legislation or regulatory requirements impose more stringent obligations than those set out in this Policy, the applicable law or regulatory requirements shall prevail. In such cases, JLW shall implement additional controls as necessary to ensure compliance.

22. Penalty for non-compliance

Breaches of this Procedure shall be reported promptly to the Compliance Manager and investigated in accordance with JLW's applicable policies and procedures.

Confirmed breaches may result in disciplinary action, contractual remedies, suspension of system or site access, termination of the relevant employment, consultancy or commercial relationship where appropriate, recovery of losses, and, where applicable, civil, regulatory or criminal proceedings.

Nothing in this Procedure limits JLW's obligations under applicable data protection legislation or the powers of competent regulatory authorities.

23. Exceptions

- Exceptions against this policy must be approved by James L Williams Middle East (JLW) 's ISSC. All exception must be documented and maintained for better traceability and required actions.
- Exceptions must be provided on a case-to-case basis.

24. Review & Update

The Compliance Manager and the Contracts Manager shall review this Procedure at least annually to ensure its continued adequacy, effectiveness and relevance. This Procedure shall also be reviewed whenever there are significant changes to business operations, processing activities, organisational structure, products, services or technologies, applicable laws or regulations, following significant information security incidents or personal data breaches, or where otherwise necessary to ensure continued compliance with applicable law and regulatory requirements.

25. Appendix

Particular Requirement for the Kingdom of Saudi Arabia (KSA)

Privacy notices and collection: Before or when collecting Personal Data, JLW shall make an appropriate privacy notice available to the Data Subject. The notice shall identify JLW as Controller, provide relevant contact details and DPO contact details where applicable, state the legal basis and specific purpose, identify the Personal Data collected and whether each item is mandatory or optional, state the storage period or retention criteria, explain the rights and how to exercise them, explain consent withdrawal, identify recipients and whether data will be transferred, disclosed or processed outside the Kingdom, and explain the potential consequences and risks of not providing the data. Where Personal Data is obtained from a third party, JLW shall, without undue delay and normally within 30 days, provide the required information together with the data categories and source, unless a lawful exception applies.

Lawful basis, consent and additional purposes: For KSA processing, JLW shall document the applicable KSA PDPL basis for each processing activity. Consent shall be freely given, informed, specific, documented and separately obtained for each purpose. Explicit consent is required where processing involves Sensitive Data, Credit Data or decisions based solely on automated processing. Withdrawal shall be as easy as giving consent and processing shall stop without undue delay where consent is the sole basis. Any new purpose shall be clearly defined, documented in the processing records, limited to the minimum necessary data and addressed in the privacy notice before the additional processing begins.

Collection and disclosure controls: JLW shall collect Personal Data directly from the Data Subject unless a permitted exception applies. Every disclosure shall have a specific and clear purpose, be limited to the minimum necessary data, protect the privacy of the Data Subject and other individuals, and be recorded with the date, method and purpose. Requests from public authorities shall be documented and the exact data required shall be identified. JLW shall not disclose Personal Data where a restriction under Article 16 of the KSA PDPL applies.

Data-subject requests and complaints: JLW shall provide practical channels for rights requests, including email or other lawful communication methods, and shall maintain a register of requests and outcomes. JLW shall inform Data Subjects of applicable refusals and reasons. Data Subjects shall retain the right to submit a complaint to the Competent Authority, subject to the applicable procedures and time limits.

Sensitive, health, credit and official-document data: Before processing Sensitive Data, health data, Credit Data or identifiable official documents, the responsible business owner and DPO shall confirm the legal basis, access restrictions, retention period, disclosure restrictions and whether a written impact assessment is required. Health Data shall be limited to the minimum personnel and operations necessary for health services or health-insurance purposes. Identifiable official documents shall not be copied unless required by law or requested by a competent public authority; they shall be protected and destroyed when the purpose ends unless retention is legally required.

Retention and destruction: JLW shall destroy Personal Data without undue delay when it is no longer necessary for the collection purpose. Retention after the purpose ends is permitted only where the data is rendered non-identifying, a legal basis requires retention for a specific period, or retention is necessary for a judicial case. Destruction controls shall address copies and backups where required and shall include notifying relevant recipients and requesting destruction where applicable.

Security and confidentiality: JLW shall adopt the relevant controls, standards and rules issued by the National Cybersecurity Authority where applicable, or recognized cybersecurity standards and best practices where those controls do not apply. All persons processing Personal Data shall protect its confidentiality during and after their employment, consultancy or contractual relationship with JLW.

Personal Data Breaches: The breach procedure shall require escalation to the DPO immediately, assessment against the 72 hour notification threshold, notification to the Competent Authority with the incident timing,

circumstances, data categories, affected numbers, risks, mitigation and contact details, and notification to Data Subjects without undue delay where damage or prejudice may occur. Reports, evidence, decisions and corrective actions shall be retained. These requirements do not replace any applicable National Cybersecurity Authority or other regulatory reporting obligation.

Cross-border Transfers: Before any Transfer or Disclosure outside the Kingdom, JLW shall record the purpose, legal basis, data map, destination, recipient, data categories and minimum necessary scope. JLW shall verify adequacy or apply an approved safeguard such as binding common rules, standard contractual clauses or another permitted safeguard. A transfer-risk assessment shall be completed before transfers made under an exemption and before continuous or large-scale transfers of Sensitive Data. The assessment shall address geography, safeguards, rights, breach response, destruction, security and potential material or moral impact. Transfers shall stop where the legal conditions or safeguards are no longer met.

Impact assessments: JLW shall prepare and document an impact assessment before or during processing where required for Sensitive Data, linking or comparing datasets from different sources, large-scale or repetitive processing involving persons lacking legal capacity, continuous monitoring, newly adopted technologies, solely automated decisions, or a product or service likely to cause serious harm to privacy. The assessment shall cover purpose and legal basis, data and sources, recipients, geographic scope, processing context, necessity and proportionality, severity and likelihood of harm, proposed mitigation and suitability of controls. The assessment shall be shared with relevant Processors and repeated where the assessment identifies harm.

Processors and sub-processors: Before appointment, JLW shall confirm that a Processor provides sufficient guarantees. The written agreement shall state the processing purpose, data categories, duration, breach-notification duty, foreign-law impacts, compulsory-disclosure handling, subcontractors and other recipients, documented instructions and audit or monitoring rights. A Processor shall obtain JLW's prior acceptance, or provide the agreed notice and objection period, before appointing a sub-Processor, and shall ensure equivalent protection in every subsequent contract.

DPO and governance: The DPO shall act as the direct contact with the Competent Authority, supervise impact assessments and audits, enable Data Subject rights, notify Personal Data Breaches, respond to requests and complaints, maintain RoPA records, and coordinate corrective action for violations. JLW shall provide the DPO with appropriate authority, access, resources and organizational support and shall publish the DPO contact details in relevant privacy notices.

Implementation records: The Compliance Manager, IT Infra and Security Lead and relevant business owners shall maintain evidence of privacy notices, consent, rights requests, disclosures, transfer assessments, DPIAs, processor due diligence, RoPA records, breach decisions, destruction and training. These records shall be available for internal audit and to the Competent Authority when lawfully requested.

UAE Federal Personal Data Protection Law Additional Requirements

Application and free-zone scope: These requirements apply to processing subject to UAE Federal Decree-Law No. 45 of 2021 Concerning the Protection of Personal Data, its Executive Regulations and applicable UAE decisions. JLW shall apply them to processing by a Controller or Processor in the United Arab Emirates, processing of Data Subjects in or outside the United Arab Emirates by an establishment in the United Arab Emirates, and processing of Data Subjects in the United Arab Emirates by an establishment outside the United Arab Emirates. JLW shall separately identify any DIFC, ADGM, health, banking, credit, government, security, judicial or other sector-specific regime that applies to the relevant processing.

Lawful basis and consent: For UAE processing, JLW shall not process Personal Data without the Data Subject's Consent unless a permitted legal basis applies, including public interest; data made public by the Data Subject; legal claims, judicial or security procedures; occupational or preventive medicine, employment capacity, health or social care, treatment or health insurance; public health; archival, scientific, historical or statistical purposes; protection of the Data Subject's interests; employment, social security or social-protection rights; performance or preparation of a contract; obligations imposed by UAE law; or another case permitted by the Executive Regulations. Where Consent is used, JLW shall be able to prove it, obtain it in a clear, simple, unambiguous and

accessible manner, explain the right to withdraw it, and make withdrawal easy. Processing after withdrawal shall cease where no other lawful basis applies.

Fair processing, purpose limitation and minimisation: JLW shall process Personal Data fairly, transparently and lawfully; collect it for a specific and clear purpose; avoid incompatible subsequent processing except where permitted; limit data to what is sufficient and necessary; keep it accurate and corrected; and erase it when the purpose is fulfilled unless retention is required by law or the data has been anonymised. JLW shall apply privacy by design and privacy by default, including appropriate Pseudonymisation where suitable.

Privacy information and Data Subject rights: Before starting Processing, JLW shall provide clear information about the Processing purposes, shared sectors or establishments inside or outside the United Arab Emirates, retention standards and applicable cross-border safeguards. JLW shall maintain clear channels for rights requests and complaints. Subject to the statutory conditions and exceptions, Data Subjects shall be able to request information about their Personal Data and Processing, obtain their data in a structured and machine-readable format where the legal conditions apply, correct or complete inaccurate data, request erasure, restrict or stop Processing, object to direct marketing and certain statistical or unlawful Processing, object to qualifying Automated Processing decisions, request human review of such decisions, and complain to the UAE Data Office.

Security and confidentiality: JLW shall implement technical and organisational measures proportionate to the nature, scope, purpose and risks of Processing to preserve confidentiality, privacy, integrity, availability and security. Controls shall include, where appropriate, encryption, Pseudonymisation, secure and resilient systems, timely restoration after physical or technical failure, and regular testing and evaluation of control effectiveness. Persons who process Personal Data shall maintain confidentiality during and after their employment, consultancy or contractual relationship.

Records and accountability: JLW shall maintain a special Personal Data record containing Controller and DPO details, Personal Data categories, authorised-access personnel, Processing duration, restrictions and scope, erasure/modification/Processing mechanisms, purposes, data movement and Cross-Border Processing, and the technical and organisational information-security measures. The record shall be kept accurate and available to the UAE Data Office when lawfully requested.

Data Protection Officer: JLW shall assess and document whether a DPO is required. A DPO shall be appointed where Processing creates a high-level risk because of new technologies or data volume, involves systematic and comprehensive assessment of Sensitive Personal Data including Profiling or Automated Processing, or involves a large amount of Sensitive Personal Data. The DPO shall have sufficient skills and knowledge, a stated contact address notified to the UAE Data Office, appropriate resources and timely involvement, no conflicting duties, protection from termination or discipline for performing DPO duties, responsibility for receiving requests and complaints, and a liaison role with the UAE Data Office.

Processors and subsequent processors: Before appointment, JLW shall select only Processors providing sufficient guarantees and shall document instructions and contracts defining the scope, subject, purpose, nature, Personal Data types and Data Subject categories. The contract shall address security by design, the Processing period, notification where Processing exceeds that period, erasure or return, non-disclosure, records and evidence of compliance, and roles and responsibilities where more than one Processor is involved. Processors shall not appoint subsequent Processors without the required contractual or documented approval and shall apply equivalent protections in every subsequent contract.

Personal Data Breaches: JLW shall immediately escalate suspected breaches to the DPO and assess whether the breach prejudices the privacy, confidentiality or security of Personal Data. The Controller shall report the breach and investigation results to the UAE Data Office within the period and in the manner prescribed by the applicable Executive Regulations, including the nature, form, causes, approximate number and records affected, DPO details, expected effects, measures taken or proposed, and corrective-action documentation. JLW shall notify affected Data Subjects where the breach prejudices the privacy, confidentiality or security of their Personal Data. Processors shall notify JLW immediately upon becoming aware of a breach.

Impact assessments: Before Processing, JLW shall assess the impact on Personal Data Protection where modern technologies may create a high risk to privacy or confidentiality, including systematic and comprehensive Automated Processing or Profiling producing legal or similarly serious effects, or large-scale Processing of Sensitive Personal Data. The assessment shall describe the Processing and purpose, assess necessity and suitability, identify risks, define mitigation measures, be coordinated with the DPO, and be reviewed when risk levels change.

Cross-border transfers and sharing: Before transferring Personal Data outside the United Arab Emirates, JLW shall document the destination, recipient, purpose, data categories, legal basis, minimum necessary scope and applicable safeguards. Where the destination has an adequate level of protection approved by the UAE Data Office, JLW shall comply with the applicable approval and control requirements. Where it does not, JLW shall use a permitted route, such as a contract containing the required protections, the Data Subject's express Consent where permitted and not contrary to UAE security or public interest, a transfer necessary for legal claims, a contract serving the Data Subject's interest, international judicial cooperation, or public interest. JLW shall also consider applicable local, free-zone and sectoral transfer restrictions.

Special categories and sectoral laws: JLW shall classify Sensitive Personal Data, Biometric Data and Health Data and apply enhanced access, security, minimisation, retention and disclosure controls. Health, banking and credit Personal Data may be subject to separate UAE legislation, and JLW shall identify and comply with the applicable sectoral requirements before Processing or disclosure.

Implementation evidence and regulatory cooperation: The Compliance Manager, IT Infra and Security Lead, and relevant business owners shall maintain evidence of notices, Consent, rights requests, complaints, lawful-basis assessments, records, DPO assessments, impact assessments, Processor due diligence, transfer assessments, breach decisions, erasure and training. JLW shall cooperate with the UAE Data Office and provide documents or information when lawfully requested. These requirements do not replace stricter applicable DIFC, ADGM, federal, local or sector-specific obligations.

Definitions as per law (Article 1 of KSA PDPL)

Term	Definition as per law
Law	The Personal Data Protection Law.
Regulations	The Implementing Regulations of the Law
Competent Authority	The authority to be determined by a resolution of the Council of Ministers.
Personal Data	Any data, regardless of its source or form, that may lead to identifying an individual specifically, or that may directly or indirectly make it possible to identify an individual, including name, personal identification number, addresses, contact numbers, license numbers, records, personal assets, bank and credit card numbers, photos and videos of an individual, and any other data of personal nature.
Processing	Any operation carried out on Personal Data by any means, whether manual or automated, including collecting, recording, saving, indexing, organizing, formatting, storing, modifying, updating, consolidating, retrieving, using, disclosing, transmitting, publishing, sharing, linking, blocking, erasing and destroying data.
Collection	The collection of Personal Data by Controller in accordance with the provisions of this Law, either from the Data Subject directly, a representative of the Data Subject, any legal guardian over the Data Subject or any other party.
Destruction	Any action taken on Personal Data that makes it unreadable and irretrievable, or impossible to identify the related Data Subject.
Disclosure	Enabling any person - other than the Controller or the Processor, as the case may be - to access, collect or use personal data by any means and for any purpose.
Transfer	The transfer of Personal Data from one place to another for Processing

Publishing	Transmitting or making available any Personal Data using any written, audio or visual means.
Sensitive Data	Personal Data revealing racial or ethnic origin, or religious, intellectual or political belief, data relating to security criminal convictions and offenses, biometric or Genetic Data for the purpose of identifying the person, Health Data, and data that indicates that one or both of the individual's parents are unknown.
Genetic Data	Any Personal Data related to the hereditary or acquired characteristics of a natural person that uniquely identifies the physiological or health characteristics of that person, and derived from biological sample analysis of that person, such as DNA or any other testing that leads to generating Genetic Data.
Health Data	Any Personal Data related to an individual's health condition, whether their physical, mental or psychological conditions, or related to Health Services received by that individual.
Health Services	Services related to the health of an individual, including preventive, curative, rehabilitative and hospitalizing services, as well as the provision of medications.
Credit Data	Any Personal Data related to an individual's request for, or obtaining of, financing from a financing entity, whether for a personal or family purpose, including any data relating to that individual's ability to obtain and repay debts, and the credit history of that person.
Data Subject	The individual to whom the Personal Data relate
Public Entity	Any ministry, department, public institution or public authority, any independent public entity in the Kingdom, or any affiliated entity therewith.
Controller	Any Public Entity, natural person or private legal person that specifies the purpose and manner of Processing Personal Data, whether the data is processed by that Controller or by the Processor.
Processor	Any Public Entity, natural person or private legal person that processes Personal Data for the benefit and on behalf of the Controller.

Reference

Standard / Framework / Regulation	Control/Clause Reference/Form/Procedure No.
KSA PDPL – Royal Decree No. (M/19) dated 16 September 2021 as amended by Royal Decree No. (M/148) dated 27 March 2023	Articles 1-31and, 41
UAE Federal Decree Law No. 45 of 2021	Articles, 1,2,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,26
Record of Processing Activities (RoPA)	JLW-CL-FM-20
Personal Data Breach Response and Management Procedure	JLW-ISMS-PR-15