MOBILE TELECOMMUNICATIONS COMPANY (ZAIN)

Personal Data Protection and Privacy Policy

August 2025

Documentation Authorization Control Sheet

This document has been created by Zain Regulatory Affairs based on the best practices and international Personal Data Protection frameworks. This document is owned by Zain Group, which is responsible for its control, release, and distribution, including any amendments that may be necessary.

Document Type	Policy
Custodian	Corporate Governance
Version	1.1

Version	Date	Author	Approved By	Comments
1	2023	Dr. Andrew Arowojolu	Board of Directors	Initial Version
1.1	2025	Nadia Al Saif	Board of Directors	Enhance and Extend the Policy controls. Incorporates enhancements, revisions, and control updates based on contributions from all participating stakeholders and OPCOs

Contents

1. Background

Mobile Telecommunications Company KSCP (“Zain Group”) and its subsidiaries and affiliates (“Zain”, "we", "us", or "our") operating in the telecommunications, information technology, infrastructure, wholesale and digital financial services domains in the Middle East and African region are subject to laws, regulations, determinations, and decisions enacted and promulgated by the relevant legislative bodies and regulatory authorities in each respective jurisdiction.

Zain is committed to protecting and respecting the privacy of all Data Subjects who engage with the company securely and transparently to comply with applicable Personal Data protection legislation in each of the jurisdictions where Zain operates including Kuwait, Saudi Arabia, Jordan, Bahrain, Iraq, Sudan, South Sudan and the United Arab Emirates.

This Personal Data Privacy Policy (“Policy”) sets out the principles and guidelines for collecting, Processing, storing, and disclosing personal and sensitive data in line with applicable Personal Data protection laws and regulations.

2. Applicable Scope

This Policy applies to all personal and sensitive Personal Data that is created, collected, stored, accessed, transmitted, or otherwise processed by Zain Group, whether in electronic or non-electronic form. It covers data entrusted to Zain by individuals with whom the organization engages, including but not limited to customers, clients, employees, contractors, suppliers, stakeholders, and both local and international strategic partners. The Policy governs the protection and responsible handling of such data across all business operations, systems, and jurisdictions in which Zain operates.

3. Policy Endorsement and Governance Oversight

This Personal Data Privacy Policy has been formally reviewed and endorsed by the Zain Group Board. The Board affirms its commitment to embedding a culture of data protection and privacy compliance across all subsidiaries, business units, and strategic operations. Through this endorsement, the Board ensures that data privacy remains a strategic priority and that sufficient resources, structures, and oversight mechanisms are established for the ongoing implementation and monitoring of this Policy. The Board shall receive periodic updates from the Group Data Office At Zain Group regarding the effectiveness of data privacy and protection measures, material risks, incidents, and mitigation strategies. This endorsement reinforces Zain’s commitment to regulatory authorities, Data Subjects, and other stakeholders.

4. Definitions

For the purposes of this Personal Data Privacy Policy, the following terms shall have the meanings set forth below:

Personal Data	Refers to any information, regardless of its source or form, which relates to an identified or identifiable natural person (categories of personally identifiable information (PII)). A person is considered

	identifiable if they can be identified directly or indirectly through reference to one or more identifiers. Personal Data includes: • A person's name, gender, date of birth, identity document number (including passport numbers, identification numbers, driving license, and employee numbers), voice, image and video. • A person's home, delivery or billing addresses, telephone number, fax number • A person's online identifiers including usernames, email addresses, social media handles, IP addresses, MAC addresses, device IDs, cookie identifiers, authentication and log-in identification information and credentials including passwords, one-time passcodes (OTPs), and multi-factor authentication details used to access mobile network systems or mobile applications. • A person's Subscriber identifiers including SIM card serial numbers, International Mobile Subscriber Identity, and device identifiers. • A person's employment ID, job function or job title or specific work location, when combined if these can be linked to a specific individual. • A person's biometric information • A person's geolocation data, current location information and location history • A person's financial information including bank account numbers, payment card information (credit/debit cards), and billing records • A person's demographic information, household income, interests, and activities • A person's preferences and behavioral data including service usage, call and message logs, data consumption patterns, purchase history, browsing and search activity on Zain platforms. • Customers Only - A person's telecom product usage, which could include traffic data and the date or time, duration and cost, device details, phone usage, purchasing habits, search and browsing history on our websites. • Employees Only - Employment information including compensation and remuneration history
Sensitive Personal Data	A specific category of Personal Data that, by their nature, presents a heightened risk to the rights and freedoms of the individual if improperly processed, accessed, or disclosed. Such data requires enhanced legal protection, stricter handling protocols, and where

	applicable explicit Consent or a valid legal exception for its Processing. For the purposes of this Policy, Sensitive Personal Data includes, but is not limited to, the following categories: • Information revealing a person's racial or ethnic origin, religious or philosophical beliefs, or political opinions. • Genetic and biometric data processed for the purpose of uniquely identifying an individual (e.g., facial recognition, voiceprints, fingerprint scans) • Health-related data, including medical records, physical or mental health conditions, health insurance details, or disability status. • Criminal convictions, offenses, or associated security measures • Financial data when processed in conjunction with identity, such as mobile wallet transactions, billing statements, and payment history. • Data used for profiling and targeted segmentation, including inferred preferences, service usage behavior, customer scoring, and engagement with marketing content. • Any combination of behavioral, technical, or transactional data that, when analyzed, reveals sensitive inferences about the individual. The definition of Sensitive Personal Data may also be expanded from time to time by legislation.
Processing	Any operation performed on Personal Data, whether automated or not, including collection, recording, organization, structuring, storage, adaptation, alteration, retrieval, use, disclosure, dissemination, restriction, erasure, or destruction.
Data Controller	The natural or legal person who determines the purposes and means of Processing personal and sensitive data.
Data Processor	A natural or legal person who processes personal or sensitive data on behalf of the controller as per controller instructions pursuant to the agreement entered into between controller and processor, pursuant to the applicable personal data protection law.
Data Subject	The identified or identifiable natural person to whom personal and sensitive data relates.
Consent	Consent is a fundamental requirement for the lawful Processing of Personal Data under most data protection laws in the MENA and GCC region and globally. It refers to a freely given, specific, informed, and unambiguous indication of the Data Subject's wishes, by which he/she signifies his/her agreement to the Processing of his/her Personal Data through a clear affirmative action. This may be

	expressed in writing, electronically, or orally, but silence, pre-ticked boxes, or inactivity do not constitute valid Consent. For Consent to be valid, it must be given voluntarily, without coercion or misleading practices, and cannot be bundled with other terms in a way that obscures its purpose. The Data Subject must be fully informed at the time of collection about the identity of the Data Controller, the purposes of Processing, and the types of data involved. If multiple Processing activities are involved, separate and independent Consent should be obtained for each purpose. Consent must be clearly expressed and documented in a verifiable manner, including the time, method, and scope of the Consent given. It must also be provided by a person with full legal capacity; in cases involving minors or others lacking capacity, it must be obtained from a parent, guardian, or legal representative. Furthermore, Data Subjects must be allowed to withdraw their Consent at any time, and this process should be as accessible and straightforward as the process for giving Consent. When presented in written form, the request for Consent must be clearly distinguishable from other content and expressed in plain, accessible language.
Third Party	A natural or legal person, public authority, agency, or body, other than the Data Subject, controller, processor and persons who, under the direct authority of the controller, processor and persons who, under the direct authority of the controller or processor, are authorized to process Personal Data
Data Protection Impact Assessment (DPIA)	Privacy-related impact assessment is conducted when Processing includes a systematic and comprehensive evaluation of the personal aspects of the Data Subject, using automated processing, including profiling, having legal consequences or a serious impact on the Data Subject, or if processing would be carried out on a large volume of Sensitive Personal Data. The DPIA aims to achieve the following as a minimum: • Describe the nature, scope, context, and purposes of the Processing. • Assess necessity, proportionality, and compliance measures. • Identify and assess risks to individual's rights and freedoms. • Identify any additional measures to mitigate those risks.
Personal Data Breach	Any incident that leads to Disclosure, Destruction, or unauthorized access to Personal Data, whether intentional or accidental, and by any means, whether automated or manual.
Data Protection Officer or Data Protection Guardian (DPO)	An employee or external contractor of Zain, formally appointed in accordance with Zain's Data Privacy and Protection Framework, to implement data privacy controls. The DPO is responsible for advising the organization, including its employees and affiliates, on their obligations under relevant data privacy and protection laws and

	regulations. The DPO's duties include monitoring compliance with legal and Policy requirements, providing guidance on data protection impact assessments, verifying the quality and correctness of the procedures in place at the controller and processor, facilitating awareness, and training programs, and serving as the primary point of contact for supervisory authorities and functions. The DPO also acts as a liaison between Zain and regulatory bodies, ensuring transparent cooperation and supporting the organization's obligations.
Contract	A formal agreement between the Data Controller and the Data Subject that establishes the terms and conditions under which services are provided. Where the Data Subject is affiliated with a corporate entity, the contract may be executed between the Data Controller and the company acting on behalf of the Data Subject in their capacity as an employee or authorized user. The contract outlines the scope of services, the roles and responsibilities of the parties, and the operational terms necessary for the delivery and management of the agreed services.
Performance of a Contract	Lawful and operational basis for Processing Personal Data when such Processing is necessary to establish, deliver, and manage services under a legally binding agreement with the customer. This includes all activities required to fulfill the telecom services provider's obligations and enable the customer to receive the subscribed telecommunications services
User	The individual using Zain website, which must coincide with or be authorized by the Data Subject, to whom the Personal Data refers
Usage Data	Information collected automatically through Zain website (or third-party services employed in the website), which can include: the IP addresses or domain names of the computers utilised by the Users who use the website, the URI addresses (Uniform Resource Identifier), the time of the request, the method utilized to submit the request to the server, the size of the file received in response, the numerical code indicating the status of the server's answer (successful outcome, error, etc.), the country of origin, the features of the browser and the operating system utilised by the User, the various time details per visit (e.g., the time spent on each page within the Website) and the details about the path followed within the Website with special reference to the sequence of pages visited, and other parameters about the device operating system and/or the User's IT environment.
Public Entity	A government establishment, agency, Ministry, including but not limited to Central Banks, Government Pension Authorities

5. Applicable Jurisdictions

Zain Group operates in multiple jurisdictions, providing telecommunications, digital, and financial services across the Middle East and Africa, including but not limited to Kuwait, Saudi Arabia, Bahrain, Jordan, Iraq, Sudan, South Sudan, and the United Arab Emirates.

This Personal Data Privacy Policy is applicable across all Zain Group entities, subsidiaries, branches, and affiliated operations within these jurisdictions. Where local data protection laws and regulations impose stricter or additional requirements, Zain commits to complying with the most applicable data privacy regulations. In some of Zain's markets, specific tailoring of the Policy may occur to include additional provisions or mention specific stakeholders which are pertinent to that market with the premise that the overarching principles reflected in this Policy will be adhered to.

This Policy governs the collection, use, Processing, storage, transfer, and disclosure of personal and sensitive data relating to the following categories of Data Subjects:

- Current, prospective, and former customers of any Zain entity
- Employees (current, former, and prospective) of Zain and its subsidiaries
- Website users and individuals interacting with Zain's digital platforms or mobile applications.
- Authorized representatives or individuals acting under legal authority.
- Shareholders and investors engaging with Zain Group
- Suppliers, vendors, contractors, franchisees, and both local and international strategic partners

All Zain Group personnel and partners are required to comply with this Policy irrespective of geographic location, and appropriate safeguards will be implemented if data is transferred across borders to ensure a consistent level of protection and adherence to local legal obligations.

6. Data Privacy and Protection Principles

Zain shall implement a comprehensive and multilayered set of physical, technical, and organizational safeguards designed to protect personal and sensitive information from unauthorized access, disclosure, alteration, and destruction. These measures shall include but are not limited to secure access controls, regular penetration testing, encrypted data transmission and storage protocols, role-based access permissions, and detailed incident response procedures. Safeguards shall be integrated across all Zain's business operations, including subsidiaries and external partners, and updated regularly in line with technological advancements and emerging threats.

Zain Group adopts the following foundational data privacy and protection principles, which guide all Personal Data and Sensitive Personal Data Processing activities across the Group and its affiliates:

- **Respect for Privacy**: Zain is committed to upholding the inherent privacy rights of all individuals whose data we process. We ensure that Personal Data and Sensitive Personal Data are handled with the highest degree of care, transparency, and responsibility to ensure that their data is collected, processed, and stored in in accordance with applicable national data protection regulations.

- **Lawfulness, Fairness, and Transparency:** We collect and process Personal Data lawfully, fairly, and transparently. All Processing activities are grounded on a valid legal basis and communicated clearly to Data Subjects, including the purposes of Processing, the categories of data involved, and the Data Subject's rights.

  Zain is committed to ensuring that transparency is embedded across all data practices. This includes providing accessible and easy-to-understand privacy notices, proactively disclosing how data is used, shared, and stored, and maintaining clear records of Processing activities. We aim to foster trust by enabling Data Subjects to make informed decisions about their data through timely updates, accessible policies, and direct communication channels for inquiries or concerns.

- **Purpose Limitation:** Personal Data is collected for specified, explicit, and legitimate purposes and is not further processed in a manner that is incompatible with those purposes.
- **Direct Marketing:** Where Personal Data is to be used for direct marketing purposes, the Data Subject will be duly informed and the Data Subject shall have the right to submit, free of charge, his/her objection to Zain with respect to such Processing (including profiling). In markets where the Consent of the Data Subject is required prior to the use of his/her data for electronic communications for the purpose of direct market, such Consent will be obtained.
- **Data Minimization:** We ensure that the Personal Data we collect is adequate, relevant, and limited to what is strictly necessary for the stated purposes. We avoid over-collection or retention of information that is not justifiable under our operational or legal obligations.
- **Accuracy and Integrity:** Reasonable and proportionate steps to be taken to ensure the accuracy and completeness of Personal Data and Sensitive Personal Data. Where Personal Data is found to be inaccurate or outdated, we promptly update, rectify, or erase it as required.
- **Storage Limitation and Retention:** Personal Data is retained only for as long as is necessary to fulfil the purpose for which it was collected or to satisfy applicable legal, regulatory, contractual, or operational requirements. Upon the expiry of retention periods, Personal Data is securely and irreversibly deleted or anonymized in accordance with approved destruction procedures.
- **Security and Confidentiality:** We implement appropriate technical, physical, and organizational safeguards to protect Personal Data from unauthorized access, alteration, disclosure, or destruction. This includes encryption, access control, data masking, multi-factor authentication, and staff awareness training, as well as routine vulnerability assessments and audits.
- **Accountability and Governance:** It is intended that Zain will maintain documented policies, procedures, and governance structures to demonstrate compliance with privacy laws and to enforce internal accountability. Designated privacy roles and oversight bodies will ensure that data protection obligations are monitored, reported, and continuously improved.
- **Data Sharing and Third-Party Transfers:** Zain only shares Personal Data with Third Parties (including processors, partners, or regulators) who provide adequate guarantees of compliance through appropriate contractual, legal, and technical safeguards. Zain endeavours to ensure that Third Party Personal Data transfers are subject to terms reflected in data transfer agreements.

- **International Data Transfers:** Where Personal Data is transferred across borders, Zain ensures that the destination country or entity provides an adequate level of data protection, or that appropriate safeguards are in place in accordance with applicable legal requirements and/or Personal Data protection laws.
- **Data Privacy and Protection by Design:** Zain shall ensure that the principles of data privacy and protection by design are mandatorily applied to the development and implementation of all future processes, products, services, and policies, when applicable. Privacy risk assessments must be conducted at the earliest stages of planning and design, and appropriate technical and organizational measures shall be implemented as a standard requirement. These measures must ensure that all Personal Data and Sensitive Personal Data Processing activities are fully compliant with applicable data protection laws and regulatory obligations in the jurisdictions where Zain operates, and that the rights and freedoms of Data Subjects are proactively protected by default throughout the data lifecycle.

7. Definition and Categories of Personal Data

Personal Data is defined in Section 4. Personal Data refers to any information, regardless of its format, source, or storage medium that directly or indirectly relates to an identified or identifiable natural person (Data Subject). A person is considered identifiable if they can be recognized, either directly or indirectly, by reference to identifiers such as a name, identification number, location data, online identifiers, or factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person.

Identifiability may arise when disparate pieces of information when combined make it possible to distinguish or profile an individual.

Zain implements comprehensive administrative, technical, and organizational controls to ensure the confidentiality, integrity, and availability of Personal Data throughout its lifecycle. These controls include access management based on roles and responsibilities, secure encryption protocols for data in transit and at rest, audit logging of data access and Processing activities, endpoint protection, regular system patching, and employee training on data handling procedures. Personal Data is stored in secured environments with restricted access and is subject to continuous monitoring and periodic reviews to detect, prevent, and respond to potential threats or unauthorized activity.

8. Definition and Processing of Sensitive Personal Data

Sensitive Personal Data is defined in Section 4. Sensitive Personal Data shall not be processed unless a lawful basis exists in accordance with applicable Personal Data protection laws. Where required, Zain shall obtain the explicit, freely given, informed, and unambiguous Consent of the Data Subject. In specific circumstances, such data may be processed without Consent when:

- Mandated by labor, health, or public interest laws.
- Required for the establishment, exercise, or defense of legal claims.
- Authorized by a competent data protection authority or competent public body to the extent necessary to perform its legitimate duties as prescribed by law.
- The data has been manifestly made public by the Data Subject.

9. Data Privacy Internal Governance Model

Zain Group shall establish and maintain a comprehensive internal data privacy governance structure to ensure enterprise-wide oversight, and alignment with applicable national Personal Data protection laws, regulations, and best practices. This structure includes the formal appointment of Data Protection Officers (DPOs) at both the Group, and/or Operating Companies and subsidiaries levels. For some operating companies, a Group appointed DPO will undertake all responsibilities. These individuals, who may be an official, an employee or an external contractor, formally authorised by Zain, shall be empowered with the authority, independence, and resources necessary to:

- Oversee the development, implementation, and continuous improvement of Zain's data protection and privacy management frameworks.
- Ensure the periodic evaluation and inspection of database systems, data Processing systems, and data security and protection systems, document the results of these evaluations, issue the necessary recommendations for data protection, and follow up on their implementation.
- Establish internal procedures for receiving and reviewing complaints, data access requests, and requests for data correction, erasure, anonymization, or transfer, and ensure these are made available to the Data Subject in accordance with the provisions of the law.
- Organize the necessary training programs for the controller's and processor's employees to qualify them to handle data in accordance with the requirements of this law and the regulations and instructions issued under it.
- Maintain and monitor privacy risk registers and compliance dashboards.
- Coordinate internal privacy awareness and training programs across all business units.
- Serve as the primary point of contact for supervisory authorities and regulatory bodies, regarding the application of Personal Data requirements as stipulated in the relevant Personal Data protection laws.
- serve as the first point of contact for all privacy-related inquiries, complaints, or suspected data privacy breaches.
- Advise business units on privacy-by-design requirements and/or technical evaluation of procedures and Personal Data protection systems and supervising data protection impact assessments (DPIAs) procedures and reports.
- Providing technical advice on evaluation procedures and periodic examination of Personal Data protection systems and intrusion prevention systems at the controller and/or processor, as the case may be, documenting the results of such evaluation and providing appropriate recommendations in this regard, including risk assessment procedures.

To uphold the objectivity and impartiality of oversight, DPOs shall report independently to executive-level data/security governance bodies. Zain shall also maintain clearly documented escalation and reporting pathways for addressing actual or suspected non-compliance incidents, ensuring timely investigation, mitigation, and remediation of any breaches. This governance structure forms a critical component of Zain's broader commitment to ethical data stewardship and regulatory compliance.

Zain shall align the data privacy and protection practices with the organization's broader enterprise risk management framework to ensure a cohesive and accountable approach to data privacy

governance. This alignment includes the integration of privacy-related risk indicators into internal audit programs, enterprise compliance monitoring tools, and strategic risk assessment processes. Business units, subsidiaries, and affiliated entities are required to identify, assess systematically, and document data privacy risks as part of their operational, programmatic, and project-level risk evaluations. By embedding privacy risk considerations into corporate risk governance and decision-making processes, Zain enhances its ability to proactively manage regulatory, reputational, and operational exposures, while maintaining compliance with applicable data protection obligations.

As part of performance monitoring, Zain shall also track and maintain records on the number of requests for personal or sensitive data sharing received from government or law enforcement authorities, including how many of these requests resulted in data disclosure. This information shall be used to assess the effectiveness, efficacy, and transparency of Zain's data privacy practices. It may be included in periodic internal reports to the board or relevant governance bodies.

The Controller is also obligated to retain records documenting the data that has been transferred or exchanged with any recipient, the purpose of such transfer or exchange, and to document the Data Subjects' Consents to the transfer.

10. Sources of Personal Data Collection

Zain collects Personal Data through a variety of channels and interaction points, ensuring all collection activities are conducted lawfully, transparently, and in alignment with the stated purposes of Processing. The collection of personal information may occur directly from Data Subjects or indirectly through authorized Third Parties and systems integrated into our business operations.

Personal Data may be collected from the following sources:

- When individuals interact with our digital platforms, including our official websites, customer portals, and mobile applications (e.g., browsing activity, registration details, cookies, and IP addresses)
- When visiting Zain retail stores, kiosks, or customer service centers
- When contacting our call centers or customer support teams by phone, chat, or email
- When using Zain's recharge channels, payment gateways, self-service terminals, or interactive voice response (IVR) systems
- When engaging with Zain's authorized agents, dealers, distributors, or franchise partners
- When participating in market trials, customer-experience pilots, promotional campaigns, surveys, contests, or research programs
- When applying for telecom or financial services that may require credit verification, including information received from licensed credit reference bureaus or financial institutions.
- When subscribing to services that require Know Your Customer (KYC) verification or identity validation, either directly or via authorized intermediaries
- When entering into employment or contractual relationships with Zain, including information collected from job applicants, employees, contractors, vendors, and strategic partners as part of HR, procurement, or onboarding processes.
- When engaging with us through social media platforms, referral programs, or online advertising technologies
- When Personal Data is provided to us by government authorities, regulators, or legal entities in the context of regulatory reporting, legal obligations, or lawful requests.
- When taking part in a competition, prize draw or survey.

- When using Zain apps or platforms that request device permissions and enabling camera access for photos or video-related features.
- When using Zain apps or platforms that request device permissions and allowing microphone access for voice or audio services.
- When using Zain apps or platforms that request device permissions and sharing device location for location-based services.
- When using Zain apps or platforms that request device permissions and granting storage access for file-related functions.

It is important to highlight that some of our operating subsidiaries – particularly those that do not engage with retail clients – may not collect or process all of the above-mentioned Personal Data.

Zain may also enrich Personal Data by associating it with publicly available information or third-party datasets, provided that such enrichment complies with applicable laws and maintains respect for individual rights and freedoms.

Each instance of Personal Data collection is governed by a lawful basis as outlined in this Policy and/or contract and is limited to the minimum information required to fulfill a defined business, legal, or operational need. Where required, explicit Consent or appropriate notification shall be provided to the Data Subject at or before the point of collection.

11. Lawful Basis for Data Processing

With respect to the relationship between the Data Controller and the Data Subject, the Data Controller shall implement transparent Consent management practices to ensure that Data Subjects are fully informed about the nature, purpose, and scope of data collection and Processing activities. Consent shall be obtained through affirmative, specific, and unambiguous user actions, recorded securely, and made revocable at any time through simple and accessible mechanisms.

Zain collects, processes, stores, and discloses Personal Data only when there is a valid legal basis to do so, as required by applicable data protection laws, regulations, and/or contracts. Where Zain intends to use the data for direct marketing purposes, in line with the specific requirements of legislation within a particular jurisdiction, Zain shall be required to inform the Data Subject, request Consent, and grant the Data Subject the right to object to Processing. We adopt a multi-basis approach that allows us to use the most appropriate legal basis depending on the specific purpose and context of the data Processing. We assess all lawful bases permitted under applicable legislation to support our operations, customer service, regulatory obligations, and innovation.

The lawful bases under which we process Personal Data include:

a. **Contractual Necessity**
Zain processes Personal Data where it is necessary to enter into or fulfill a contractual relationship with the customer. This includes delivering telecommunications and digital services, managing subscription lifecycles, issuing invoices, Processing payments, addressing service-related inquiries or complaints, and enabling the customer to exercise their rights under the terms of the service agreement. As part of these activities, Zain may also process location data and call-related information to ensure network connectivity and assess creditworthiness to determine eligibility for post-paid service offerings.

b. **Legal Obligation**
Zain processes Personal Data where necessary to comply with statutory or regulatory obligations imposed on Zain. This includes obligations related to telecommunications licensing,

financial reporting, record-keeping, fraud detection, consumer protection, anti-money laundering, tax compliance, and lawful interception. This includes retaining call detail records for a legally mandated period or responding to official requests from government or regulatory authorities.

c. **Legitimate Business Interests**
Zain may process Data Subject Personal Data where it is necessary to pursue our legitimate interests, provided that such interests do not override Data Subject fundamental rights and freedoms under Personal Data protection law. These interests may include:

- Maintaining network and service security
- Preventing and detecting fraud or service misuse
- Improving our services and customer experience
- Conducting anonymized research and statistical analysis
- Optimizing internal processes and operational efficiency

d. **Consent**
Concerning the relationship between the Controller and Data Subject, Zain shall establish and enforce end-to-end Consent management processes to govern the entire Consent lifecycle, ensuring that Consent is obtained, recorded, maintained, and withdrawn in a transparent and compliant manner. These processes shall guarantee that Data Subjects are clearly informed of the nature, purpose, and scope of data collection and Processing prior to providing Consent. Consent must be secured through explicit, specific, and unambiguous user actions, stored securely, and made revocable at any time through user-friendly and accessible channels.

Consent shall be obtained for defined purposes, including but not limited to direct marketing (where such is required by law or regulation), participation in optional surveys, and the Processing of sensitive Personal Data. Data Subjects retain the right to withdraw their Consent from Controller at any point without affecting the lawfulness of Processing conducted prior to such withdrawal, subject to contract.

e. **Public Interest or Official Authority**
In limited circumstances, Zain may process Personal Data to conduct tasks in the public interest, including support for national security, public health, or the detection of serious crime. Where applicable, this includes Processing authorized by government or judicial entities under lawful conditions.

f. **Commercial and Analytical Purposes (Aligned with Legitimate Business Interest or Consent)**
Zain may process anonymized or aggregated data for internal analytics, product development, marketing campaigns, cross-promotion strategies, and location-based services. This includes profiling for service improvements, provided the Processing is permitted under an appropriate lawful basis and does not result in legal or significant effects on the Data Subjects.

12. Processing Children's Data
Zain is committed to safeguarding the Personal Data of children. We do not significantly collect or process Personal Data of individuals under the applicable legal age (13, 16, or 18, depending on jurisdiction) without verified parental or guardian Consent. Services specifically designed for children will include tailored privacy notices and transparent Consent mechanisms.

13. Why Zain Uses Data Subject's Personal Information
The Data Subject's Personal Data may be processed for the following purposes, each of which is tied to one or more of the lawful bases described above, including but not limited to:

- To register and onboard Data Subject as a customer or user of our services.
- To provide telecom, digital, or value-added services that the Data Subject has subscribed to.
- To verify the Data Subject identity and assess eligibility for service packages.
- To manage billing, payments, collections, and credit assessments.
- To deliver customer support, respond to service inquiries, and resolve technical issues.
- To notify the Data Subject of service changes, planned maintenance, outages, or critical account alerts.
- For direct marketing purposes, subject to informing the Data Subject and (as required by some jurisdictions) requesting Consent and providing a mechanism that enables the Data Subject to opt out from receiving marketing materials when desired.
- To enable international roaming services (outbound for Zain customers and inbound for customers of other networks) and manage cross-border traffic.
- To analyse the Data Subject usage data for quality improvement and network optimization.
- To develop new products, applications, and platforms tailored to customer demand.
- To conduct satisfaction surveys, test user experience, and conduct market research.
- To detect and prevent fraudulent activity or unauthorized access.
- To comply with legal obligations and regulatory reporting requirements.
- To train and monitor customer service interactions for quality and regulatory assurance.
- To administer our relationship with our business partners, including responding to enquiries or complaints, providing our products and services, and managing our contracts.

Where legally required or appropriate, calls to and from Zain Contact Centres made by the Data Subject may be recorded for quality control, training, financial control, fraud prevention, and compliance verification purposes.

14. Sharing, Transferring, and Disclosing the Data Subject's Personal Data

Zain is committed to protecting the confidentiality and integrity of Personal Data throughout its lifecycle, including during any sharing or transfer activities. However, in certain legitimate and clearly defined scenarios, Zain may share or disclose Personal Data to authorized Third Parties. All such activities are conducted strictly in accordance with applicable Personal Data protection laws, regulatory requirements, and international best-practices.

14.1 Internal Sharing within Zain Group

Personal Data may be shared internally across Zain Group entities, including subsidiaries and affiliated companies, where necessary to deliver group-wide services, fulfil contractual obligations, enable consolidated reporting, or ensure operational efficiency. All intra-group transfers are governed by standardized contractual terms and internal policies that provide consistent levels of Personal Data protection across jurisdictions.

14.2 Third-Party Sharing and Disclosures

Zain may share Personal Data with carefully selected and contractually bound Third Parties, but only when necessary to:

- Deliver, manage, or improve the products and services requested by the Data Subject
- Utilise data for direct marketing subject to specific caveats according to the legislation within a specific jurisdiction.

- Perform technical, operational, or support functions such as billing, hosting, analytics, or fraud prevention.
- Enable engagement with agents, resellers, contractors, vendors, or business process outsourcing partners who process Personal Data strictly on Zain's behalf under written agreements.
- Comply with obligations under applicable laws, court orders, or legal proceedings.
- Respond to lawful requests from regulatory authorities, such as national data protection agencies, telecommunications regulators, financial services authorities, or law enforcement bodies.
- Protect vital interests, public safety, or the rights and freedoms of Zain, its customers, or other individuals in urgent or legally recognized cases.

Third-party recipients are obligated under data Processing agreements to process Personal Data only for the specified purpose, under Zain's documented instructions, and with appropriate confidentiality and security safeguards.

14.3 Conditions for Processing Without Consent

There are specific circumstances in which Personal Data may be processed without the Data Subject's explicit Consent. These specific instances are those only permitted or required by applicable law and occur when:

- A legal obligation mandates the disclosure (e.g., anti-fraud measures, procedures of legal claim or defense of rights, national security, tax compliance).
- Processing is necessary for the performance of a task conducted in the public interest or the exercise of official authority to the extent required to carry out its legitimate duties as laid down by a law or the execution of a contract or as required by law.
- If the Processing is necessary for the purpose of legitimate interest of the Data Controller, without prejudice to the rights and interests of the Data Subject, and provided that no sensitive data is to be processed, and all relevant controls as set out in the relevant Personal Data protection law or regulation are applied.
- If the Processing is necessary for the purposes of controller or Data Subject carrying out their obligations and exercising their legally established rights in the field of employment, social security or laws concerned with social protection, to the extent permitted by such laws.
- If the Processing is related to Personal Data which has become available and known to all by an act of the Data Subject.
- If the Processing is necessary for purposes of occupational or preventive medicine in order to perform medical diagnosis, providing health or social care, treatment or health insurance services, managing health or social care systems and services in accordance with the legislation in force in the relevant jurisdiction.
- If the Processing is necessary to perform a contract to which the Data Subject is a party, or to take measures at the request of the Data Subject to conclude, amend or terminating a contract.
- If Processing is carried out by a competent Public Entity to the extent required to carry out the tasks entrusted to it in accordance with the provisions of the legislation in force or through other contracting parties, provided that the contract includes compliance with all obligations and conditions stipulated in this Law and the regulations and instructions issued pursuant thereto.

- If Processing is necessary to protect the life or vital interests of the Data Subject
- If Processing is necessary for the purposes of scientific or historical research, provided such data is anonymised before Processing.
- if Processing is necessary for statistical purposes, national security requirements, or to achieve the public interest.

In all other cases, Zain shall seek the Data Subject's explicit, informed, and freely given Consent before disclosing their Personal Data to any unaffiliated party not involved in service delivery.

14.4 International (Cross-Border) Data Transfers

Zain may transfer Personal Data to its subsidiaries, affiliates, partners, or authorized third-party service providers located in countries outside the Data Subject's home jurisdiction where such transfers are necessary to provide services, operate their business, or fulfill contractual and regulatory obligations.

All cross-border data transfers are conducted in strict compliance with applicable data protection laws and with full respect for the rights and freedoms of the Data Subject. Zain ensures that:

- The recipient country provides an appropriate level of protection or is recognized by the competent regulatory authority as providing an adequate level of data protection, or
- Appropriate safeguards have been established, such as Binding Common Rules, Standard Contractual Clauses, approved codes of conduct, or certification mechanisms enforceable by the receiving entity.

Where the above conditions are not met, Zain will only proceed with the transfer if one of the lawfully recognized exceptions (derogations) applies, such as:

- The explicit, informed, and unambiguous Consent of the Data Subject
- The transfer is necessary for the performance of a contract between the Data Subject and Zain.
- The transfer is required to protect the vital interests of the Data Subject or another person.
- The transfer is made in response to a legitimate legal obligation, public interest task, or legal claim.

Zain enters into written data transfer agreements with all overseas recipients, ensuring that the Personal Data is handled in accordance with Zain's internal policies and applicable Personal Data protection laws, including adherence to security, confidentiality, and purpose limitation principles.

Zain applies strict access controls, encryption standards, and security policies for the handling, transmission, and storage of all sensitive Personal Data.

14.5 Oversight and Assurance

Zain endeavours to ensure that third-party processors and recipients undergo due diligence and are periodically monitored for compliance with Zain's data privacy and protection requirements. Regular assessments and audits shall be conducted to verify the effectiveness of contractual and technical safeguards. These audits may include both internal evaluations conducted by Zain's data governance, risk, and internal audit functions, as well as independent external audits commissioned to provide objective assurance of third-party compliance. Audit results should inform risk mitigation actions and contractual enforcement measures where necessary.

Zain considers such audits a critical component of its accountability framework and an essential mechanism to ensure ongoing alignment with applicable legal, regulatory, and Policy requirements.

15. Data Subject Rights

In accordance with applicable Personal Data protection laws, all Data Subjects whose Personal Data is processed by Zain are entitled to exercise specific rights to ensure transparency, control, and accountability in how their Personal Data is handled. These rights apply to all relevant Zain operations and jurisdictions, subject to any lawful exemptions or limitations under local regulations.

All Zain employees must ensure that any Data Subject request to exercise their data privacy rights, whether received in writing or electronically, is promptly referred to the designated Data Office or DPO or submitted through the official reporting channel specified in the Contact Us section of this Policy. The DPO/Data Office is responsible for coordinating the response in accordance with applicable legal timeframes. As a standard, Data Subject requests must be addressed within 10 Days to one calendar month from the date of receipt, depending upon the jurisdiction. If an extension is necessary due to complexity or volume, it must be duly documented, justified, and communicated to the Data Subject in accordance with regulatory requirements.

With regards to the relationship between the Controller and the Data Subject, the data privacy rights available to the Data Subject, granted by the Data Controller, include:

a. **Right to Be Informed**
The Data Subject has the right to receive clear, concise, and transparent information about how and why his/her Personal Data is collected, used, stored, disclosed, and retained. This includes being informed of the legal basis for Processing, his/her rights, and how to exercise them typically provided through this Personal Data Privacy Policy or at the point of data collection.

b. **Right of Access Personal Data**
The Data Subject may request confirmation as to whether Zain are Processing his/her Personal Data and, where applicable, receive a copy of the data Zain hold about Data Subject in a structured, commonly used, and machine-readable format. This includes the categories of data, purposes of Processing, and details of any third-party recipients.

c. **Right to Rectification (Correct) Personal Data**
The Data Subject has the right to request correction of any inaccurate, incomplete, or outdated Personal Data Zain hold. Where appropriate, Zain may request documentation to verify the changes.

d. **Right to Erasure (Right to Be Forgotten)**
The Data Subject may request the deletion of his/her Personal Data in certain circumstances, such as when it is no longer necessary for the purposes for which it was collected, when Consent is withdrawn (and no other legal basis applies), or when Processing was unlawful.

e. **Right to Restrict Processing/Using of Personal Data**
In specific scenarios, the Data Subject may request the restriction of Processing of his/her Personal Data. This may apply when a Data Subject contests the accuracy of his/her data, objects to Processing, or when the Processing is unlawful but he/she prefers restriction.

f. **Right to Object to the Use of Personal Data**
The Data Subject has the right to object, on grounds relating to a particular situation, to the Processing of his/her Personal Data based on legitimate interests. Zain will terminate such

Processing unless we demonstrate compelling, appropriate grounds or need the data for legal claims.

g. **Right to Withdraw Consent**
If the Personal Data of Data Subject is being processed based on Consent, he/she has the right to withdraw that Consent at any time without affecting the lawfulness of Processing conducted prior to withdrawal.

h. **Right to Object to (or opt out of) Direct Marketing**
The Data Subject may object at any time to the Processing of his/her Personal Data for direct marketing purposes, including profiling related to such marketing. Once Data Subject opts out, Zain will terminate all such Processing activities immediately.

i. **Right to Lodge a Complaint**
If the Data Subject believes that his/her privacy rights have been violated or his/her Personal Data has been mishandled, he/she has the right to lodge a complaint with the DPO or data protection authority in his/her jurisdiction. Zain will cooperate fully with any investigation or inquiry and seek resolution in line with applicable legal frameworks.

16. Personal Data Retention and Deletion

Zain is committed to ensuring that Personal Data is retained only for the minimum duration necessary to fulfil the lawful and clearly defined purposes for which it was collected. Data retention is governed by internal retention schedules that consider the nature of the data, the legal or regulatory context, contractual obligations, operational needs, and the rights and freedoms of the Data Subject.

Personal Data shall not be retained indefinitely or processed longer than necessary. Retention periods are defined based on the following criteria:

- The original purpose for which the Personal Data was collected or subsequently processed.
- The duration of any contractual relationship with the Data Subject
- The regulatory requirements (e.g., telecom data retention laws, financial reporting obligations, labor law requirements)
- Internal audit, legal, fraud prevention, or compliance monitoring needs
- Any relevant guidance issued by data protection authorities or industry regulators.

Unless otherwise mandated by applicable laws or sector-specific obligations, the standard maximum retention period for Personal Data at Zain is 60 months from the date the data was last actively processed (or longer based upon business needs). Exceptions to this period must be justified, documented, and approved by the Data Office.

Once Personal Data is no longer required for its original purpose and no legal ground exists for further retention, the Personal Data shall be securely and irreversibly deleted, destroyed, or anonymized and/or transferred back to the Controller or Data Subject, as per the terms of the contract.

Deletion and disposal procedures shall include:

- Secure digital deletion protocols for data stored in databases, servers, and archives.
- Secure shredding or destruction of physical media and documents
- Sanitization or destruction of backup tapes and redundant storage systems

- Validation of deletion actions through audit logs, certificates of destruction, or access logs

Zain shall ensure that data deletion applies equally to all environments and locations in which Personal Data resides, including cloud services, third-party platforms, backup systems, and offline archives. Data Processors and external service providers are contractually obligated to follow the same retention and deletion standards as outlined in Zain's data privacy and protection policies and/or contract.

The Group Data Office, in coordination with Group Regulatory, Group Legal, Group Information Security, and Group Internal Audit, shall periodically review retention practices and ensure alignment with evolving legal requirements, risk tolerance, and business needs.

17. Collection of Third-Party Data

Zain may collect and process Personal Data obtained from Third-Party sources in accordance with applicable data privacy and protection regulations and purpose limitation. Third Party data refers to personal information provided to Zain by entities or individuals other than the Data Subject, such as affiliates, business partners, regulatory bodies, public sources, or authorized data providers.

Such data may be collected through the following lawful and clearly defined methods:

- Data shared by suppliers, partners, and affiliates as part of service delivery or operational agreements.
- Information received from government authorities, regulators, or under legal obligations and lawful requests.
- Data obtained from licensed financial or identity verification institutions for eligibility checks, fraud prevention, or customer onboarding.
- Information from open data repositories, corporate registries, or official websites where disclosure is legally permitted.

All Third-Party data collected by Zain shall be:

- Used solely for specific, legitimate, and clearly communicated purposes, in line with the legal basis under which it was collected.
- Subject to data minimization and proportionality, ensuring that only the necessary data is collected to fulfill the intended purpose.
- Verified for accuracy and relevance before being used in Processing activities.
- Governed by contractual and technical safeguards, including data sharing agreements that define responsibilities, permitted uses, and retention conditions.
- Managed with full transparency, with appropriate privacy notices or disclosures made to the Data Subjects where required.

Zain shall not process Third-Party data for any secondary or unrelated purposes unless such Processing is compatible with the original purpose or has been authorized under applicable laws or regulations or through renewed Consent.

18. Cookies /IP Address Tracking

When users access any Zain digital channels or services, including websites, mobile applications, or self-service portals, certain technical information is automatically collected to enhance his/her user experience and ensure the functionality and security of Zain platforms. This information may include

User device's IP address, browser type, operating system, domain name, unique device identifiers, and stored browsing preferences.

Zain uses cookies and similar tracking technologies to support various functionalities. These technologies may perform one or more of the following roles:

- Enable core site features such as navigation, login authentication, and shopping cart memory.
- Recognize returning users and remember language, region, or accessibility preferences.
- Measure website traffic, user behavior, and interaction with site content to improve performance and service quality.
- Support customer analytics, digital marketing, and personalization efforts, where permitted.
- Facilitate integration with social media platforms or third-party services when explicitly enabled.

Where required by applicable data protection laws, Zain request user Consent before placing non-essential cookies on his/her device. A User has full control over his/her cookie preferences and can modify its settings at any time through his/her browser or device privacy controls. A User may also reject or disable cookies.

19. Personal Data Breach Notification

Zain is committed to timely and transparent communication in the event of a personal or sensitive data breach that may cause serious harm to the Data Subject. In accordance with applicable Personal Data protection laws/regulation/framework, Zain shall notify the competent data protection authority within the prescribed statutory timeframe (Maximum within 72 hours) from becoming aware of the incident and, where required, shall also inform the affected Data Subjects without unjustified delay.

In the event of a data breach, internal notification procedures shall include immediate escalation to senior management and the Data Protection Officer, activation of the incident response team within one hour of breach detection, and continuous updates to relevant internal stakeholders. These steps are intended to ensure timely containment, effective risk assessment, and coordinated mitigation efforts. This process should be read in conjunction with the "Zain Incident Management Policy".

The notification shall, to the extent known at the time of reporting, include the nature and circumstances of the breach, the categories and estimated number of Data Subjects and records affected, the potential consequences, and the remedial actions taken or planned to address and mitigate the impact.

Zain shall maintain a centralized and continuously updated data breach incident register documenting all confirmed or suspected breaches, whether or not they are subject to regulatory notification. This register shall be available for review by competent authorities upon request and shall be subject to periodic internal audits to support regulatory compliance and continuous improvement of the data breach response process.

20. Security Measures to Protect Personal Data

Zain shall implement appropriate technical and organizational measures to ensure the confidentiality, integrity, and availability of personal and sensitive Personal Data, in full compliance with applicable Personal Data Protection and Privacy regulations and relevant cybersecurity

standards. These measures are designed to prevent unauthorized access, loss, alteration, or disclosure of data throughout its lifecycle.

The security framework may include, but not be limited to, the following controls:

- Zain's Information Security Policies and Procedures (such as the Zain Data classification Policy and the Zain patch management Policy) to ensure that the measures taken are in line with our Information Security Management System (ISMS).
- Systems that process/store the data must not have any Critical or high vulnerabilities that could allow for any unauthorized access, modification, or disclosure of data.
- Encryption of personal and sensitive data at rest and in transit using approved, industry-standard cryptographic protocols to protect against unauthorized access and interception.
- Pseudonymization and anonymization techniques, particularly in non-production environments, testing, and during external transfers, to reduce the risk of direct or indirect re-identification.
- Access control mechanisms based on the principles of least privilege and need-to-know, ensuring that only authorized personnel with a clearly defined business requirement may access sensitive data.
- Role-based access restrictions that segregate access to sensitive Personal Data from general data Processing activities, with enhanced logging, approval workflows, and oversight.
- Multi-factor authentication (MFA) and strict session control for all systems and applications managing sensitive data, combined with automated access timeout and monitoring mechanisms.
- Periodic access reviews and privilege audits to verify that entitlements to sensitive data remain appropriate, justified, and limited to authorized individuals.
- Activity logging and audit trails for all access to sensitive Personal Data, ensuring traceability and accountability in line with internal and regulatory expectations.

These safeguards are reviewed and updated regularly to address evolving threat landscapes, business needs, and emerging compliance requirements. Zain commits to maintaining a risk-based approach to data security, prioritizing the protection of sensitive Personal Data through clearly defined access control policies and rigorous operational governance.

21. Changes to our Personal Data Privacy Policy

Zain Group reserves the right to update and change this Policy at any time without prior approval. Zain Group is committed to maintaining transparency and accountability in how Personal Data is collected, used, and protected. This Personal Data Privacy Policy is subject to regular review and may be updated to reflect:

- Changes in applicable Personal Data protection legislation or regulatory guidance
- Modifications to Zain services, technologies, or Processing activities
- Evolving industry standards and internal privacy governance requirements

All revisions to this Personal Data Privacy Policy shall be formally reviewed and endorsed by the Zain Board prior to publication. The updated Policy will then be accessible internally at (Internal Regulation Shared Folder) and clearly marked with the version number and the effective date of endorsement.

Where the updates materially affect how we process Personal Data or impact Data Subject rights, Zain will notify Data Subjects in advance through appropriate communication channels, including but not limited to website banners, digital notifications, customer emails, and/or SMS.

Zain encourages all users, customers, partners, and employees to periodically review the most current version of this Personal Data Privacy Policy to stay informed of our practices. Continued use of Zain services following the publication of an updated Personal Data Privacy Policy will constitute acknowledgment and acceptance of the changes, unless otherwise required by regulations.

This Personal Data Privacy Policy has been formally reviewed and endorsed by the Zain Group Board and is subject to annual review and approval.

22. Compliance and Disciplinary Measures

Zain expects full adherence to this Personal Data Privacy Policy by all personnel, contractors, and Third Parties acting on its behalf. Any violation of this Policy, whether due to negligence or deliberate action, may constitute a breach of Zain's internal policies and applicable Personal Data protection regulations.

Non-compliance with the data privacy and protection requirements outlined in this Policy may result in appropriate corrective or disciplinary actions. Such actions may include, but are not limited to, internal investigation, removal of system access, contractual penalties, disciplinary proceedings, or referral to relevant regulatory or legal authorities, depending on the nature and severity of the breach.

Zain reserves the right to apply these measures consistently and proportionately, in alignment with its internal compliance framework, to uphold accountability and maintain the integrity of its data privacy practices across all operations.

23. Contact Us

For queries regarding this Personal Data Privacy Policy, please write an email or letter to the following address:

Mobile Telecommunications Company KSCP
Group Corporate Communications, Corporate Governance, and Investor Relations
Airport Road,
Shuwaikh
Kuwait City,
Kuwait
Email: ZainDataProtectionandPrivacy@zain.com.

24. Privacy Escalation Procedures

- For Data Subject rights requests: Email ZainDataProtectionandPrivacy@zain.com
- For privacy complaints: Contact Zain's Data Protection Officer directly
- For urgent privacy concerns: Use our 24/7 privacy hotline.
- Response timeframes: We respond to all inquiries within five (5) business days and complete Data Subject rights requests within thirty (30) days.

Last updated on 31 July 2025.