MOBILE TELECOMMUNICATIONS COMPANY (ZAIN)

Personal Data Protection and Privacy Policy

August 2025

Personal Data Privacy Policy Statement

1. Introduction

This Personal Data Privacy Policy Statement (together with our Terms and Conditions and any other documents referred to on it) describes how Mobile Telecommunications Company KSCP (“Zain Group”) referred as Zain (hereinafter referred to as ("we," "us," or "our") the operator of this website or mobile app (where applicable) or service collects, uses, discloses, and protects the Personal Data and respects the privacy of Zain’s customers and business partners (herein referred to as "you" and "your"). We are committed to ensuring the privacy and security of your Personal Data and complying with the applicable 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.

Zain is an established, reliable telecom operator and provider of information technology, infrastructure, wholesale, and digital financial services across the Middle East and Africa. These operations are governed by applicable laws, regulations, and regulatory directives issued by the relevant legislative and oversight authorities within each jurisdiction in which Zain operates.

This Personal Data Privacy Policy Statement outlines our core principles and practices regarding data protection and privacy. It explains how we collect, use, disclose, and protect your Personal Data in connection with your use of Zain services and platforms. By using our services, you acknowledge that you have read and understood this Personal Data Privacy Policy Statement and Consent to the collection, use, and Processing of your Personal Data as described herein.

2. Definitions

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

Term	Definition
Personal Data	Refers to any information, regardless of its source or form, that relates to an identified or identifiable natural person. A person is considered identifiable if they can be identified directly or indirectly through reference to one or more identifiers, such as their name, identification number, voice, image, video, electronic identifier (e.g., IP address or cookies), geolocation data, or contact details, including addresses, contact numbers, and email addresses. It also includes financial data such as bank account and credit card numbers, as well as any information related to an individual’s physical, physiological, genetic, psychological, mental, economic, cultural, or social identity. When determining whether a person is identifiable, all means reasonably likely to be used by the Data Controller or any other party must be considered.
Sensitive Personal Data	A specific category of Personal Data that, due to its sensitive nature, requires enhanced protection. It includes data that reveals or relates to a person’s racial or ethnic origin, religious or philosophical beliefs, political opinions or affiliations, union or organizational membership,

Term	Definition
	genetic or biometric data (when used for unique identification), health data (including mental, psychological, or physical health, or data arising from healthcare services). It also encompasses information relating to criminal convictions or offences, security status, data concerning children, family or marital relationships, and—where specified by law—financial data such as banking and credit card information. Any data that, if disclosed or misused, could result in harm, discrimination, or infringement of an individual's rights may also be deemed sensitive, subject to the determination of the relevant data protection authority.
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 Personal 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 they signify their agreement to the Processing of their 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 distinguishable from other content and expressed in plain, accessible language.
Third Parties	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

Term	Definition
	the direct authority of the controller or processor, are authorized to process Personal Data
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.
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 the 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 utilized by the Users who use the website, the URI addresses (Uniform Resource Identifier), the time of the request, the method used 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 utilized 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.

3. Applicable Scope

This Personal Data Privacy Policy Statement applies to all Personal Data collected, processed, stored, or shared by Zain and its subsidiaries through their telecommunications, digital services, financial services, and technology platforms across jurisdictions where Zain operates, including the Middle East and Africa.

This Personal Data Privacy Policy Statement is applicable across all Zain Group entities and all relevant business lines, subsidiaries, suppliers, and affiliated operations.

The scope of this policy statement covers, but is not restricted to, the following:

- **Data Subjects**: Individuals who interact with Zain as customers, website or mobile app users, service subscribers, or participants in promotional or support activities.
- **Channels**: Where applicable, Data collected through Zain websites, mobile applications, customer service centers, retail locations, kiosks, digital campaigns, and network infrastructure.
- **Data Types**: Includes personal identifiers, contact details, financial information, service usage data, device and network metadata, engagement records, and other data categories as defined in this policy statement.
- **Processing Purposes**: Service delivery, account management, compliance, marketing (with Consent), analytics, support, fraud prevention, and legal obligations, among others.
- **Jurisdictional Applicability**: This policy statement is designed to comply with applicable Personal Data protection regulatory requirements in each jurisdiction where Zain operates. Where local regulations require specific variations or additions, those will be addressed in localized notices or supplementary statements.

4. Personal Data

4.1 What Data We Collect

We collect Personal Data from our customers and clients to facilitate the effective delivery of services, fulfill contractual obligations, and ensure compliance with applicable legal and regulatory requirements. We collect only the minimum data necessary for the specified purposes, and delete or anonymize it once no longer needed.

We do not knowingly collect or process Personal Data of individuals under the legal age as defined by local regulations without obtaining verified Consent from a parent or legal guardian.

We may collect, but are not limited to, the following categories of Personal Data where applicable:

- **Personal Identifiers:** Such as full name, email address, phone number, date of birth, capture images or videos, record audio, and national identification – used to verify your identity, confirm eligibility for services, and maintain accurate customer records.
- **Account Credentials**: Including usernames and encrypted passwords or PINs – these credentials are stored securely and used solely to authenticate your identity and safeguard your account access.
- **Financial Information**: Such as bank account numbers, payment methods, and transaction history, and billing addresses – collected to process payments, including payroll, manage financial transactions, issue invoices or refunds, and detect fraudulent activity.
- **Usage and Device Data**: Including browsing behavior, IP address, and device-specific details, session logs, location data, operating systems, and network diagnostics –

used to improve user experience, optimize service performance, and detect security or technical issues.

- **Engagement Data:** Collected through customer surveys, feedback forms, promotions, marketing campaigns, social media interactions, or customer service inquiries – to enhance service delivery, tailor marketing, personalize customer experiences, and gather feedback for continuous improvement.

4.2 How do we collect your data

We collect your Personal Data through multiple secure channels to provide services, respond to customer needs, and meet legal and operational obligations. The collection methods include, but are not limited to, the following:

Collection Method	Description
Website and Mobile Applications	We collect Personal Data through our secure digital platforms when you register an account, access services, submit forms, participate in promotional campaigns, or interact with our site features. We may also collect data through cookies, session logs, and similar tracking technologies, subject to your Consent where applicable.
Customer Care Channels (Call Centers, Chat, Email)	We collect Personal Data during your interactions with our call centers or customer support channels, including phone calls, live chat, and email, to address inquiries, resolve complaints, and provide service-related updates.
Retail Stores, Kiosks, and Sales Agents	We collect information during your in-person visits to our retail locations or interactions with our employees at conventions or meetings, or authorized agents, including during SIM issuance, identity verification, number portability, and device or service registration.
Telecommunication Network Infrastructure	We automatically collect metadata, such as call logs, IP addresses, device locations, and network diagnostics, during your use of our services. This is done in compliance with legal, telecom regulatory, and national security requirements.
Social media and Digital Engagement	We collect Personal Data from your interactions with our official social media pages, including messages, comments, survey responses, and participation in promotional campaigns.
Email and SMS Communications	We collect Personal Data from your responses to our official communications, such as emails, service confirmations, and feedback requests, to support service tracking, issue resolution, and analysis.
Mobile Device Usage	We collect Personal Data through our telecom applications installed on your devices, including usage analytics, crash logs, connectivity patterns, and device identifiers, with your Consent.

4.3 How do we process your Personal Data

We process your Personal Data for specific, limited purposes in accordance with applicable personal data protection regulations. Each Processing activity is based on a lawful basis and supports the delivery and improvement of our services. The table below outlines key purposes, descriptions, and the corresponding legal bases:

Purpose of Processing	Description	Legal Basis of Processing
Service Activation & Delivery	To set up, activate, and manage telecom and digital services you have subscribed to	Contractual necessity
Account Verification & Security	To verify your identity, enable secure login, and prevent unauthorized access to your account	Legitimate interest / Legal obligation
Billing & Payments	To process service transactions, generate invoices, and manage payments or refunds.	Contractual necessity / Legal obligation
Fraud Detection & Prevention	To detect, investigate, and prevent fraud, abuse, or security threats to our services	Legitimate interest / Legal obligation
Compliance with Laws	To fulfill our obligations under regulatory frameworks and lawful requests from regulatory authorities, in addition to the applicable Personal Data protection legislation	Legal obligation
Marketing & Promotional Offers (with Consent)	To send marketing promotional communications, service updates, and personalized content based on your preferences	Explicit Consent
Customer Support	To respond to your inquiries, manage service complaints, and provide technical support across our channels	Contractual necessity / Legitimate interest
Network Performance Monitoring	To monitor service quality, detect outages, and improve network efficiency.	Legitimate interest
Website & App Analytics	To analyze usage behavior, improve functionality, and personalize content on digital platforms	Legitimate interest / Consent (for cookies, tracking, etc.)
Product Development	To analyze trends and improve or develop new telecom products and features	Legitimate interest

5. Legal Basis for Processing Personal Data

Zain processes Personal Data in compliance with the applicable personal data protection regulatory frameworks. Each data Processing activity is carried out on a lawful basis, ensuring transparency, accountability, and the protection of individuals' rights. Processing may rely on one or more of the following legal bases:

- Consent of the Data Subject

  Concerning the relationship between Controller and Data Subject, where required by regulation, Zain obtains clear, specific, and informed Consent from Data Subjects before collecting or Processing their Personal Data. Consent may be acquired in

written or digital form, depending on the context of the service. Individuals have the right to withdraw their Consent at any time, without affecting the lawfulness of any prior Processing. Consent requests are presented clearly and never bundled with unrelated terms. To withdraw Consent, you may contact Zain through the methods listed in this policy statement.

- Performance of a Contract

  We process Personal Data when it is necessary to establish, manage, or fulfill a contractual relationship with the Data Subject. This includes enabling service activation, billing, customer support, mobile network access, and usage-based features. Without such data Processing, we may be unable to deliver the agreed services or respond to customer needs effectively. Data collected under this basis is strictly limited to what is necessary for contract execution.

- Compliance with Legal or Regulatory Obligations

  Certain Processing activities are mandated by applicable regulations. We may also be obligated to disclose specific data to government authorities or judicial bodies upon lawful request. Such Processing is essential for fulfilling our legal duties and maintaining regulatory compliance.

- Protection of Public Interest or Vital Interests

  In some cases, we process data to protect the vital interests of individuals, for example, during emergencies, public safety threats, or natural disasters. We may also process data to support broader public interest tasks, such as cybersecurity, fraud prevention, or ensuring the continuity of critical telecom infrastructure. These activities are carried out in line with data privacy principles and with appropriate safeguards in place.

6. Data Sharing & Third Parties

We may share Personal Data with carefully selected and contractually bound third parties, such as:

- Service providers (payment processors, delivery companies)
- Government authorities (if legally required)
- Analytics partners (Google Analytics, Firebase)

We 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
- 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 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

We may transfer Personal Data to third parties located in other jurisdictions, but only when such transfers are necessary and in full compliance with applicable Personal Data protection laws and regulations. These transfers are strictly limited to trusted third parties who are contractually bound to uphold appropriate confidentiality, security, and data protection standards.

Cross-border transfers are carried out only when one or more of the following conditions are met:

- Adequate data protection safeguards are in place in the destination country or organization
- The Data Subject has provided explicit Consent, where required by law or regulation.

All Personal Data is stored securely, and any transfer across borders is subject to rigorous safeguards to ensure the continued protection and lawful Processing of the data.

7. Data Subject Rights Under Data Protection Regulations

Concerning the relationship between Controller and Data Subject, as a Zain customer, you are entitled to exercise the following rights under the Personal Data Protection regulations:

- **Right to Be Informed**
  You have the right to know how we collect, use, process, store, and share your Personal Data, the legal basis for such Processing, and how long it will be retained.

- **Right of Access**
  You may request confirmation of whether we process your Personal Data and, if so, obtain access to the data and related information. This includes the purposes of Processing, categories of data, and details of any third parties with whom it has been shared. You may access specific data directly through your online account or by submitting a request via the contact details provided below. Please note that access may be limited in some instances to protect the rights of others or to comply with legal obligations.

- **Right to Correction**
  If your Personal Data we hold about you is inaccurate or incomplete, you may request correction or update by contacting us through the details provided below. Corrections will be processed promptly, and you will be notified once processed.

- **Right to Erasure (Right to Be Forgotten)**
  You may request deletion of your Personal Data under certain conditions where there is no legal or contractual reason for its continued Processing —for example, if the data is no longer needed for its original purpose. Legal or regulatory obligations may limit this right in some cases.

- **Right to Restrict Processing**
  You can request temporary or permanent restriction of your Personal Data Processing in certain circumstances —for instance, when contesting its accuracy or objecting to its Processing.

- **Right to a Data Request**
  You may request to receive your Personal Data in a structured, commonly used, and machine-readable format, where technically feasible.

- **Right to Withdraw Consent**
  If the Processing of your Personal Data is based on your Consent (e.g., for marketing communications), you may withdraw your Consent at any time through your account preferences or by contacting us. This does not affect the lawfulness of Processing carried out before such withdrawal.

- **Right to Object (Opt Out) to Direct Marketing**
  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 a Data Subject opts out, Zain will terminate all such Processing activities immediately.

- **Right to Submit Complaint: The customer** has the right to submit a complaint to DPO at Zain or the competent data protection authority. The Competent Authority shall take the necessary measures regarding the complaint submitted to it and inform the complainant of the outcome. Zain will cooperate fully with any investigation or inquiry and seek a resolution in line with applicable personal data protection legal and regulatory frameworks.

How to Exercise Your Rights:

You can exercise your rights by contacting our Data Protection Officer (DPO) at ZainDataProtectionandPrivacy@zain.com, or accessing your account through our online portal at: https://zain.com

We respond to all valid privacy inquiries within the timeframe required by applicable data protection regulations - within 5 business days (subject to responsible team confirmation) and complete Data Subject rights requests within 30 business days (subject to responsible team confirmation).

We will respond to all valid requests within the timeframe required by applicable data protection regulations. If additional time is needed, we will inform you accordingly.

8. Personal Data Retention and Deletion

We are committed to retaining your Personal Data only for as long as necessary to fulfill the lawful and clearly defined purposes for which it was collected. Our data retention practices are guided by internal retention schedules that consider the nature of the data, applicable legal and regulatory requirements, contractual obligations, operational needs, and your rights and freedoms as a Data Subject. The standard maximum retention period for Personal Data at Zain is 60 months from the date the data was last actively processed, unless an alternative retention period is stipulated in law.

Once no longer needed, data is securely deleted or anonymized in accordance with our internal data disposal procedures designed to prevent unauthorized access or recovery.

9. Data Security and Protection

Zain is committed to enhancing its effectiveness at safeguarding Personal Data through the established knowledge and competencies of its employees and contractors, supported by ongoing training and awareness programs in applicable privacy and data protection requirements across our footprint.

We are committed to protecting your Personal Data through the implementation of appropriate technical and organizational measures. These include:

- Encryption and access control mechanisms to safeguard data against unauthorized access
- An established incident response process to detect, manage, and resolve security incidents
- Regular security audits and assessments to identify and mitigate potential risks
- Adopt Privacy by Design by embedding data protection requirements into our systems, services, and internal practices from the outset
- Access to Personal Data is strictly limited to authorized personnel based on job responsibilities and need-to-know principles.

10. Data Breach Notification

In the event of a serious Personal Data breach that causes serious harm to the Data Subject, we are committed to notifying the affected individuals and the relevant data protection authority within the timeframes prescribed by applicable data protection regulations.

11. Confidentiality and Disclosure of Information

We prioritize the confidentiality and protection of your Personal Data and are committed to implementing appropriate technical and organizational measures to prevent its loss, misuse, unauthorized access, or alteration. Your Personal Data is stored on secure servers, and we only disclose it when required by applicable regulations, or when such disclosure is necessary to deliver our services, products, technical support, or for analytical purposes.

We do not share, lease, or disclose your Personal Data to any Third Party outside of Zain or its subsidiaries without your Consent. Where Third-Party service providers are engaged to support our operations, they are contractually obligated to maintain the confidentiality of your information and use it solely for the purposes for which it was shared.

12. Cookies

We use cookies and similar technologies on our websites and mobile applications to enhance user experience, analyze usage patterns and traffic, remember your preferences, and deliver relevant content and advertisements. These technologies help us understand how our digital platforms are being used and enable us to improve their functionality and performance.

You have the option to manage your cookie preferences at any time through your browser or device settings. Please note that disabling certain cookies may affect the functionality or performance of some features on our platforms.

13. Disciplinary Protocols

Zain is committed to safeguarding Personal Data and upholding the highest standards of privacy and data protection. All employees, stakeholders, contractors, suppliers, and third parties acting on behalf of Zain are required to comply with this Personal Data Privacy Policy Statement and all applicable data protection laws. Regular training and awareness programs are provided to ensure that all personnel have the necessary knowledge and capability to handle Personal Data responsibly and lawfully.

In cases of a violation, appropriate disciplinary action will be taken in accordance with applicable laws and regulations and Zain's policies, along with corrective and preventive measures to mitigate the risk of future breaches. In case of any discrepancies between the provisions of this Policy and applicable personal data protection laws and regulations, the laws shall prevail.

14. Updates & Complaints

This Personal Data Privacy Policy Statement may be updated from time to time to reflect, for example, changes to our practices or for operational, legal, or regulatory reasons. The last update to this policy statement was in 31-July-2025.

We may update this Personal Data Privacy Policy Statement, and it will be shared through the website and/or channels.

15. For Concerns or Complaints

If you have any concerns or complaints regarding how your Personal Data is handled, you may contact our Data Privacy Officer (DPO) at ZainDataProtectionandPrivacy@zain.com.

If you are not satisfied with our response, you have the right to escalate your complaint to the relevant data protection authority in your jurisdiction.