ORIENT INSURANCE PJSC

Standard Operating Procedure

DATA SUBJECT REQUEST (DSR) MANAGEMENT

SOP-DSR-001 | Version 2| February 2026

Document Reference	Value
Document Title	Data Subject Request (DSR) Management SOP
Document Reference	SOP-DSR-001
Version	2.0
Classification	Confidential - Internal Use Only
Owner	Data Protection Officer (DPO) Orient Insurance
Applicable Entity	Orient Insurance PJSC (Al-Futtaim Group)
Applicable Systems	Orient Online Portal (orientonline.ae) | InsuranceUAE.com | CRM | Policy Admin System
Regulatory Framework	UAE Federal Decree-Law No. 45/2021 (PDPL) | ADHICS | DHA Health Data Law | IA Circular
Effective Date	1st April 2026
Next Review Date	31st March 2027
Approved By	Data Privacy & Protection Office Orient

1. PURPOSE

This Standard Operating Procedure (SOP) establishes the end-to-end process by which Orient Insurance PJSC ("Orient", "the Company") receives, validates, processes, and responds to Data Subject Requests (DSRs). A DSR is a formal request made by an individual (the Data Subject) to exercise their privacy rights in respect of their personal data held by Orient Insurance.

This SOP applies to all lines of business offered through the Orient Online portal and InsuranceUAE.com, including individual and group medical insurance, motor, travel, home, and life insurance products.

2. REGULATORY & LEGAL BASIS

Orient Insurance's DSR handling obligations are drawn from the following legal and regulatory instruments:

Instrument	Key DSR Obligations
UAE Federal Decree-Law No. 45 of 2021 on Personal Data Protection (PDPL)	Right of access, correction, deletion, objection, data portability; 30-day response timeline; mandatory identity verification
UAE Federal Law No. 6 of 2007 (Insurance Authority Law) & IA Circulars	Data retention obligations; policyholders' right to access policy data; mandatory disclosure requirements
Dubai Health Authority (DHA) Health Data Law	Special category health data; explicit consent for medical records; data subject access to health records within defined timelines
Abu Dhabi Healthcare Information and Cyber Security Standard (ADHICS)	Technical and organisational controls for health data; access request logging; audit trail requirements; data minimisation
Orient Insurance Confidentiality Statement	Commitment to personal data correction and removal Rawad.Shaker@alfuttaim.com data use disclosure
UAE Federal Law No. 2 of 2019 (Use of IT in Health Fields)	Electronic health data protection; consent management for medical data processing
ISO/IEC 27001 Best Practice (ADHICS-aligned)	Incident logging; access control; audit trails for all DSR processing activities

3. SCOPE

3.1 In Scope

- All natural persons (policyholders, insured members, beneficiaries, claimants, website visitors) whose personal data is processed by Orient Insurance PJSC
- Personal data collected through: Orient Online portal, InsuranceUAE.com website, call center (800 ORIENT / 800 674368), branch offices, brokers/agents, and third-party service providers acting on Orient's behalf
- All request types: Access, Rectification, Erasure, Restriction, Portability, Objection, and Withdrawal of Consent
- Medical/health data (special category data) handled under ADHICS and DHA requirements

3.2 Out of Scope

- Data relating to deceased individuals (subject to estate/legal representative provisions)
- Data processed by third-party insurers, TPAs, or government authorities under their own legal basis
- Regulatory reporting data required for mandatory retention under Insurance Authority rules

4. DEFINITIONS

Term	Definition
Data Subject (DS)	A living natural person whose personal data is processed by Orient Insurance.
Personal Data	Any information that identifies or can identify a natural person — name, Emirates ID, passport, contact details, policy number, health data, financial data, IP address, etc.
Special Category Data	Sensitive personal data including health/medical information, biometric data, financial data. Requires heightened protection under PDPL and ADHICS.
DSR (Data Subject Request)	A formal request by a Data Subject to exercise one or more privacy rights.
Data Controller	Orient Insurance PJSC — determines the purposes and means of processing personal data.
DPO	Data Protection Officer — the designated contact point for all privacy matters within Orient Insurance.
Portal	The Orient Online portal (orientonline.ae) - the online transaction and policy management system.
TPA	Third Party Administrator — handles medical claims processing on behalf of Orient Insurance.
ADHICS	Abu Dhabi Healthcare Information and Cyber Security Standard — applies to health data processing.
Response Deadline	30 calendar days from date of verified request receipt, as per UAE PDPL. Extendable by 30 additional days with notification.
Identity Verification	The process of confirming the requester is who they claim to be before processing a DSR.

5. DATA SUBJECT RIGHTS UNDER UAE PDPL

Orient Insurance recognises and facilitates the following rights for all Data Subjects:

Right	Description	Orient's Obligation	Timeline
Right of Access	Request a copy of all personal data held about them	Provide a structured summary of data held, sources, purposes, and recipients	30 days
Right of Rectification	Request correction of inaccurate or incomplete data	Correct data in all relevant systems (portal, CRM, policy admin, TPA records)	30 days
Right of Erasure ('Right to be Forgotten')	Request deletion of personal data	Delete data subject to retention obligations (legal, regulatory, contractual hold periods)	30 days
Right to Restrict Processing	Request limitation of how data is used	Flag data for restriction; halt non-essential processing while	30 days

Right	Description	Orient's Obligation	Timeline
		maintaining compliance-required data	
Right to Data Portability	Request data in a machine-readable format	Export data in structured format (CSV/JSON/PDF) for transfer to another controller	30 days
Right to Object	Object to processing for marketing or legitimate interest	Cease processing for stated purpose; apply suppression flags in all systems	30 days
Right to Withdraw Consent	Withdraw previously given consent	Remove consent-based processing immediately; update all downstream systems	Immediate / max 7 days
Right to Non-Discrimination	Not to be denied service for exercising rights	Orient shall not penalise, delay renewals, or alter premiums as a result of DSR submission	Ongoing

6. DSR SUBMISSION CHANNELS

Data Subjects may submit a DSR through any of the following channels. All channels must be monitored and routed to the Privacy Office within 1 business day of receipt:

Channel	Mechanism	Responsible Team	SLA for Routing to Privacy Office
Email	Customer care with DSR line detials (dedicated DSR inbox will be rolled out)	Privacy Office	1 business day
Customer Care Hotline	800 674368 agent logs request and escalates	Customer Service / Call Centre	1 business day
Written Letter	Addressed to: Data Protection Officer, Orient Insurance PJSC, Dubai UAE	Branch Reception / Compliance	2 business days

7. END-TO-END DSR PROCESS

7.1 Overview Process Flow

The DSR process consists of six sequential phases. Each phase has defined responsible parties, tasks, and timelines:

Phase	Phase Name	Responsible	Max Duration	Key Output
1	Receipt & Acknowledgement	Privacy Office / Customer Service	Day 0–1	DSR Reference Number + Acknowledgement
2	Identity Verification	Privacy Office	Day 1–3	Verified / Rejected status confirmed
3	Request Validation & Classification	DPO / Privacy Office	Day 3–5	Assigned request type + internal routing
4	Internal Data Discovery & Processing	IT, Policy Admin, CRM, TPA, Compliance	Day 5–20	Data package / action completed
5	Review, Approval & Response	DPO / Legal	Day 20–28	Approved response letter + data package
6	Closure & Audit Logging	Privacy Office / IT	Day 28–30	Closed ticket + audit record

7.2 Detailed Phase Tasks

PHASE 1 - Receipt & Acknowledgement (Day 0–1)

Manual Channel Tasks (Email, Phone, Branch, Letter)

- Receiving staff complete the Orient Insurance DSR Intake Form (Form DSR-001 - see Section 9)
- Assign DSR Reference Number manually from the DSR Register
- Send written acknowledgement to Data Subject within 1 business day via their preferred channel
- Upload all supporting documents and completed Form DSR-001 to the DSR Register
- Route case file to Privacy Office inbox via customer support same day

PHASE 2 - Identity Verification (Day 1–3)

Orient Insurance must verify the identity of the Data Subject before processing any DSR. This is mandatory under UAE PDPL and ADHICS to prevent unauthorised disclosure.

Verification Level	Required Documents	When applied
Standard (Individual Policyholder)	Emirates ID (front + back) OR valid Passport + Visa page	All standard DSRs
Enhanced (Medical / Health Data)	Emirates ID + signed declaration + Policy Number + DOB verification	All DSRs involving medical records or health data (ADHICS requirement)
Third-Party / Legal Representative	Power of Attorney (POA) or Court Order + representative's Emirates ID	Requests submitted on behalf of another individual
Corporate / HR (Group Policy)	Company trade licence + HR authorisation letter + data subject employee ID	Group medical or group life policy DSRs submitted by employer

- < Data Privacy request handling Call center person> at 800 674368 sends identity verification request to Data Subject via email within 1 business day of receipt
- Data Subject has 14 calendar days to respond with verification documents
- If there is no response within 14 days - Privacy Officer sends one reminder, then closes the request as 'Abandoned' with full audit log
- If identity cannot be verified - request is rejected; written rejection notice sent to Data Subject with reasoning
- All verification documents must be stored securely, encrypted, and purged within 90 days of DSR closure (ADHICS requirement)

PHASE 3 - Request Validation & Classification (Day 3–5)

1. DPO reviews the verified request and confirms the following:
   a. Is the request within Orient Insurance's scope (correct data controller)?
   b. Is the data held by Orient or by a third party / TPA?
   c. Does the request qualify as a legitimate DSR under UAE PDPL?
   d. Does it involve special category (health) data requiring ADHICS protocols?
   e. Are there any legal holds, regulatory retention obligations, or insurance underwriting reasons that limit the response?

- Assign internal handling team for each relevant system: Portal IT Team, Policy Admin, CRM, Medical Claims / TPA, Finance (if financial data requested)

- If request involves a third-party data controller (e.g., TPA, reinsurer) notify that party within 3 business days and coordinate response
- Update DSR Register with classification, assigned team, and projected completion date

PHASE 4 - Internal Data Discovery & Processing (Day 5–20)

System-by-System Data Discovery Tasks

- Orient Online Portal: Export all personal data fields linked to the Data Subject's account (name, DOB, Emirates ID, address, login history, declared information, uploaded documents)
- Policy Administration System: Retrieve all active and historical policies, endorsements, schedule of benefits, premium history, renewal records
- CRM System: Pull all customer interaction logs, communications history, complaint records, marketing preferences
- Medical Claims System / TPA: Retrieve all claims submitted, diagnoses (ICD codes), treatment records, approvals/rejections, pre-authorisation history - ADHICS controls apply
- Finance / Accounts: Retrieve premium payment history, refund records, bank account details (masked per PCI-DSS)
- Document Management System: Identify all contracts, proposal forms, signed declarations, ID copies stored
- Marketing Platform: Pull consent flags, communication preferences, opt-out history
- IT / Logs: For access requests - provide system access log summary (not server logs) for last 12 months

Actions by Request Type:

Request Type	System Action Required	Responsible Team
Access	Export all data in structured format (PDF/CSV); compile Master Data Report	IT + Policy Admin + CRM + TPA
Rectification	Update data in all live systems; log changes with before/after values; notify TPA of corrections	IT + Operations + TPA
Erasure	Anonymised or delete data in non-restricted systems; apply retention hold flag in systems with legal/regulatory hold; document what was deleted vs. retained and why	IT + Compliance + DPO
Objection / Restriction	Apply processing suppression flag in all relevant systems; halt marketing communications; note in policy admin record	IT + Marketing + CRM
Consent Withdrawal	Update consent fields to 'Withdrawn' immediately; halt all consent-based processing; update TPA and service providers	IT + Compliance

PHASE 5 — Review, Approval & Response (Day 20–28)

2. Privacy Office compiles the complete DSR Response Package, which includes:

a. Formal DSR Response Letter (on Orient Insurance letterhead - see Section 9, Form DSR-003)
b. Data Subject's Master Data Report (for Access requests)
c. Actions taken log - what was done, when, and by whom
d. Any data withheld and the legal basis for withholding it
e. Data Subject's right to complain to the UAE Data Office if dissatisfied

3. DPO reviews and approves all responses before sending
4. Legal Counsel review is mandatory for: Erasure requests involving active policies, requests involving litigation, any partial refusal, any request from a minor or legal representative
5. Response is sent to the Data Subject through their stated preferred channel, encrypted where applicable
6. For health/medical data responses — output must be transmitted via secure encrypted channel (email encryption or secure portal link); hard copy handed only in-person with ID verification (ADHICS requirement)

PHASE 6 - Closure & Audit Logging (Day 28–30)

- Update DSR Register: mark as Closed, record actual closure date, outcome category (Fulfilled / Partially Fulfilled / Rejected / Abandoned)
- Attach all documentation to the case file: intake form, identity documents (encrypted), internal communications, response letter, data package
- Purge identity verification documents from live systems after 90 days (retain case reference only)
- Generate monthly DSR metrics report for DPO review (volume, type, response times, rejection rates)
- Retain DSR case files for a minimum of 3 years from closure date (UAE PDPL obligation)

8. SPECIAL HANDLING REQUIREMENTS

8.1 Medical / Health Data (ADHICS & DHA Requirements)

- All health-related DSRs must be escalated to the DPO on Day 1 - no delegation to junior staff
- The Medical Claims / TPA team must be engaged within 2 business days of request classification
- Health data responses must include a clear summary of: diagnosis codes processed, treatment types, insurance claim history, pre-authorisation decisions
- Data Subject has the right to request correction of incorrect medical coding - corrected codes must be notified to the TPA and updated within 5 business days of correction decision
- ADHICS requires a full audit trail log for any access to health data records during DSR processing - log must include: who accessed, when, from which system, for what purpose
- Medical data exports must be encrypted using AES-256 minimum and transmitted over TLS 1.2+ channels
- Under DHA Law, DSR response for health records must not exceed 30 days from identity-verified receipt

8.2 Grounds for Refusal (Partial or Full)

Orient Insurance may refuse or partially refuse a DSR on the following grounds (which must be documented and communicated to the Data Subject in writing):

Ground for Refusal	Example	Required Action
Regulatory Retention Obligation	Insurance Authority mandates 10-year retention of policy documents	Inform Data Subject of specific law; delete what is not retained
Ongoing Legal Proceedings	Data is subject to court order or regulatory investigation	Legal Counsel sign-off; inform Data Subject of legal hold
Third-Party Rights	Data file contains personal data of another individual that cannot be separated	Redact third-party data; provide the Data Subject's own data only
Manifestly Unfounded or Excessive	Same request submitted repeatedly within 30 days with no new basis	DPO documents reasoning; written refusal sent; right to complain communicated
Prevention of Crime / Fraud	DSR appears linked to ongoing fraud investigation	Legal Counsel and Compliance approval required; partial or full refusal
AML/CFT Obligations	Data retention required under anti-money laundering law	Inform Data Subject; retain data per regulatory requirement

8.3 Extensions & Delays

- If Orient Insurance requires more than 30 days to respond (complex or voluminous requests), the Privacy Office must notify the Data Subject in writing within the original 30-day window
- Maximum extension: 30 additional calendar days (total maximum: 60 days from verified receipt)
- Extension notification must state: the reason for delay, the new expected completion date, and the Data Subject's right to complain to the UAE Data Office

8.4 Minor Data Subjects

- If the DSR relates to a person under 18 years of age, the request must be submitted by a parent or legal guardian with supporting documentation (birth certificate + guardian Emirates ID)
- Heightened protection applies: DPO must personally review and approve all responses

9. FORMS AND TEMPLATES

Form Reference	Form Name	Purpose	Available At
Form DSR-001	DSR Intake Form	Used by staff to capture manual DSR submissions (phone, branch, letter)	Staff intranet; branch office
Form DSR-002	Customer DSR Request Form	Completed by customers to formally submit any DSR type	Orient Online portal; email on request; branch
Form DSR-003	DSR Response Letter Template	Formal Orient Insurance response to Data Subject	Privacy Office - DPO controlled
Form DSR-004	Identity Verification Checklist	Staff checklist for identity verification process	Staff intranet; embedded in portal workflow
Form DSR-005	DSR Refusal Notice Template	Formal written notice when a DSR is refused in whole or in part	Privacy Office - DPO controlled
Form DSR-006	DSR Extension Notice Template	Formal notice to Data Subject when response will exceed 30 days	Privacy Office - DPO controlled
Form DSR-007	DSR Register / Case Log	Master register tracking all DSRs received (Excel/SharePoint)	Privacy Office

FORM DSR-002 — CUSTOMER DATA SUBJECT REQUEST FORM

IMPORTANT: Please complete all sections of this form clearly. Orient Insurance PJSC is committed to responding to your request within 30 calendar days. A copy of this completed form and proof of identity must be submitted. All fields marked * are mandatory.

SECTION A — YOUR DETAILS (DATA SUBJECT)

Field	Your Information
Full Legal Name *	
Emirates ID Number *	784 - _____ - _____ - _
Passport Number (if no Emirates ID)	
Date of Birth *	DD / MM / YYYY
Nationality	
Email Address *	
Mobile Number *	+971
Preferred Language	English Arabic Other: _____
Preferred Response Channel *	Email Post Portal Branch Pick-Up

SECTION B — YOUR RELATIONSHIP WITH ORIENT INSURANCE

Field	Your Information
Policy / Member Number (if known)	
Type of Policy	Medical Motor Life Travel Home Other: ____
Your Role	Policyholder Insured Member Beneficiary Claimant Website Visitor Other
Period of Relationship	From: _____ to (if applicable): _____
Are you acting on behalf of another person? *	No Yes — please complete Section C

SECTION C — THIRD PARTY / AUTHORISED REPRESENTATIVE (Complete only if acting on behalf of another person)

Field	Information
Representative Full Name *	
Representative Emirates ID *	784 - _____ - _____ - _
Relationship to Data Subject *	Parent / Guardian Legal Representative Power of Attorney Employer (HR)

Field	Information
Supporting Document Attached *	Power of Attorney Court Order Parental Consent HR Authorisation Letter

SECTION D — REQUEST TYPE (Select all that apply)

#	Request Type	Select	Description of What You Are Requesting
1	Right of Access	☐	I would like a copy of all personal data Orient Insurance holds about me
2	Right of Rectification	☐	I would like to correct the following inaccurate/incomplete data: _____
3	Right of Erasure	☐	I would like Orient Insurance to delete my personal data (subject to legal retention obligations)
4	Right to Restrict Processing	☐	I would like Orient Insurance to limit how it uses my data
5	Right to Data Portability	☐	I would like my data provided in a structured, machine-readable format for transfer
6	Right to Object	☐	I object to Orient Insurance processing my data for (specify): _____
7	Withdrawal of Consent	☐	I withdraw my consent to the following processing: _____
8	Other	☐	Please describe: _____

SECTION E — ADDITIONAL DETAILS OF YOUR REQUEST

Field	Your Information
Please describe your request in detail:	
Specific data or records of concern:	
Time period of concern (if applicable):	From: _____ to: _____
Is this request related to a complaint?	No Yes — Complaint Reference: _____

SECTION F — IDENTITY DOCUMENTS ATTACHED

Document	Attached?	Document Reference/Number
Emirates ID (front and back)	Yes No	
Passport + UAE Visa page	Yes No N/A	

Document	Attached?	Document Reference/Number
Power of Attorney / Court Order (if applicable)	Yes No N/A	
Other Supporting Document	Yes No N/A	

SECTION G — DECLARATION

DATA SUBJECT DECLARATION: I confirm that the information provided in this form is true and accurate to the best of my knowledge. I understand that Orient Insurance PJSC may require additional information to verify my identity before processing this request. I understand that Orient Insurance will respond within 30 calendar days of verifying my identity. I understand that certain data may be subject to legal retention obligations and may not be erasable.

Field	
Data Subject Signature *	
Printed Name *	
Date *	DD / MM / YYYY
Place of Signing	

Submit this form to:

- Online: Login to orientonline.ae → My Profile → Privacy Request
- Email: customer care
- Post / In Person: Data Protection Officer, Orient Insurance PJSC, Dubai, UAE
- Phone: 800 674368

10. ROLES AND RESPONSIBILITIES

Role	Responsibilities
Data Protection Officer (DPO)	Overall accountability for DSR compliance; approves all responses; handles complex/sensitive cases; maintains DSR Register; reports to Board quarterly
Privacy Office	Day-to-day DSR management; identity verification; internal coordination; drafts response letters; maintains audit trail
IT / Systems Team	Data discovery across all systems; data exports; anonymisation / deletion in portal and CRM; access log retrieval; encryption of data packages
Policy Administration Team	Retrieve and correct policy data; action rectification requests in policy admin system; coordinate with reinsurers if needed
Medical Claims Team / TPA Liaison	Retrieve health data; coordinate with TPA for health record exports; update claim records per rectification requests; ADHICS audit trail
Customer Service / Call Centre	First point of contact; log requests; provide acknowledgement; escalate to Privacy Office; do NOT process DSRs independently
Legal / Compliance	Review refusal decisions; sign off on extension notices; review requests involving litigation or regulatory investigation
Marketing Team	Implement suppression / opt-out flags; update communication preferences; confirm consent withdrawal actioned
Branch Staff	Complete Form DSR-001 for walk-in requests; verify basic identity; route to Privacy Office; do NOT process independently
Finance Team	Retrieve financial/payment data for access requests; ensure PCI-DSS compliant data masking in all data exports

11. DSR REGISTER — MINIMUM FIELDS

The Privacy Office must maintain a DSR Register. Each entry must capture the following minimum fields:

Field	Description
DSR Reference Number	Unique identifier (DSR-YYYY-NNNNNN)
Date Received	Date the DSR was submitted by the Data Subject
Date Identity Verified	Date identity verification was confirmed
Request Type(s)	Access / Rectification / Erasure / Portability / Objection / Restriction / Consent Withdrawal
Data Category	Standard Personal Data / Special Category (Health) / Financial
Channel Received	Portal / Email / Phone / Branch / Letter
Assigned Handler	Privacy Officer name or ID
Systems Involved	List of all systems searched/actioned (Portal, CRM, TPA, Policy Admin, etc.)
Status	Received / In Progress / Pending Verification / Responded / Closed / Rejected / Abandoned
Response Date	Date formal response sent to Data Subject

Field	Description
Outcome	Fulfilled / Partially Fulfilled / Rejected / Abandoned / Extended
Legal Basis for Refusal (if applicable)	Specific law / regulation cited for any data withheld or request refused
Escalation Flags	DPO Escalated / Legal Review / ADHICS Health Flag / Minor / Third Party
Closure Date	Date case file was closed and audit log completed
Retention Expiry	Date the DSR case file may be purged (3 years from closure)

12. KEY PERFORMANCE INDICATORS (KPIs)

KPI	Target	Reporting Frequency
% of DSRs responded within 30 calendar days	>= 95%	Monthly
% of identity verifications completed within 3 days	>= 90%	Monthly
% of health data DSRs escalated to DPO on Day 1	100%	Monthly
Average DSR processing time (days)	< 20 days	Monthly
% of DSRs with complete audit trail	100%	Quarterly
Number of DSR-related regulatory complaints	0	Quarterly
% of DSR case files retained per policy (3 years)	100%	Annual

13. TRAINING & AWARENESS

- All staff who may receive a DSR (customer service, branch, underwriting, IT, marketing) must complete Orient Insurance Privacy & DSR Handling training annually
- New joiners must complete training within 30 days of start date before having access to any customer data system
- ADHICS-specific health data training is mandatory for all staff with access to medical claims systems
- DPO must complete at least 16 hours of continuing privacy education annually
- Training completion records must be maintained for audit purposes

14. DOCUMENT CONTROL & REVIEW

Version	Date	Author	Changes	Approved By
2.0	April 2026	Data Privacy Office	Initial release	DPO

This SOP must be reviewed at minimum annually or upon:

- Changes to UAE PDPL or implementing regulations
- Changes to ADHICS or DHA health data requirements
- Material changes to Orient Insurance systems, products, or data processing activities
- Following any DSR-related regulatory inquiry or significant complaint

15. REFERENCES & RELATED DOCUMENTS

- UAE Federal Decree-Law No. 45 of 2021 on Personal Data Protection (PDPL)
- UAE Federal Law No. 6 of 2007 on Insurance and its amendments
- Abu Dhabi Healthcare Information and Cyber Security Standard (ADHICS) v2
- Dubai Health Authority (DHA) Health Data Law
- Orient Insurance Confidentiality Statement (www.insuranceuae.com/confidentiality-statement)
- Orient Insurance Information Security Policy
- Orient Insurance Incident Response Policy
- ISO/IEC 27001:2022 Information Security Management Standard

APPROVALS & SIGN-OFF

Role	Name	Signature	Date
Data Protection Officer			
IT Head/VP Orient			

DISCLAIMER: This SOP has been drafted in alignment with UAE Federal Decree-Law No. 45/2021, ADHICS v2, DHA requirements Orient Insurance PJSC legal counsel should review this document before adoption to ensure alignment with any internal policies, insurance-sector specific regulatory guidance from the UAE Insurance Authority, and any group-level data governance frameworks not publicly disclosed. This is a compliance guidance document and does not constitute legal advice.