

Data Dictionary & ER Model

Digital ID Data Privacy and Access Monitoring System

ENTITY-RELATIONSHIP SUMMARY

Relationships:

- CITIZENS (1) ↔ (1) DIGITAL_IDS
- CITIZENS (1) ↔ (M) CONSENT_RECORDS
- CITIZENS (1) ↔ (M) ALERTS
- AUTHORIZED_ENTITIES (1) ↔ (M) ACCESS_REQUESTS
- DIGITAL_IDS (1) ↔ (M) ACCESS_REQUESTS
- ACCESS_REQUESTS (1) ↔ (1) ACCESS_LOGS
- ACCESS_REQUESTS (1) ↔ (0..1) VIOLATIONS
- DATA_CATEGORIES (1) ↔ (M) CONSENT_RECORDS

DETAILED DATA DICTIONARY

1. CITIZENS (Dimension Table)

Column	Data Type	Constraints	Purpose
CITIZEN_ID	NUMBER(10)	PK, NOT NULL	Unique citizen identifier
NATIONAL_ID	VARCHAR2(16)	UNIQUE, NOT NULL	Government-issued ID number
FIRST_NAME	VARCHAR2(50)	NOT NULL	Legal first name
LAST_NAME	VARCHAR2(50)	NOT NULL	Legal last name
DATE_OF_BIRTH	DATE	NOT NULL	Birth date
EMAIL	VARCHAR2(100)	UNIQUE, NOT NULL	Contact email

PHONE_NUMBER	VARCHAR2(15)	NOT NULL	Contact phone
ADDRESS	VARCHAR2(200)		Physical address
REGISTRATION_DATE	TIMESTAMP	DEFAULT SYSDATE	When registered
STATUS	VARCHAR2(20)	CHECK IN ('ACTIVE','SUSPENDED','INACTIVE'), DEFAULT 'ACTIVE'	Account status
CREATED_BY	VARCHAR2(50)		User who created record
CREATED_DATE	TIMESTAMP	DEFAULT SYSDATE	Creation timestamp
MODIFIED_BY	VARCHAR2(50)		Last modifier
MODIFIED_DATE	TIMESTAMP		Last modification time

Business Rules:

- Each citizen must have unique NATIONAL_ID
- Status can only be ACTIVE, SUSPENDED, or INACTIVE
- Email must be valid format (enforced via trigger)
- Age must be 18+ (enforced via CHECK or trigger)

2. DIGITAL_IDS (Fact Table)

Column	Data Type	Constraints	Purpose
DIGITAL_ID	NUMBER(10)	PK, NOT NULL	Unique digital ID
CITIZEN_ID	NUMBER(10)	FK → CITIZENS, NOT NULL	Owner of ID

ID_NUMBER	VARCHAR2(20)	UNIQUE, NOT NULL	Actual digital ID number
BIOMETRIC_HASH	VARCHAR2(256)	NOT NULL	Encrypted biometric data
ISSUE_DATE	DATE	NOT NULL	When ID was issued
EXPIRY_DATE	DATE	NOT NULL	When ID expires
ID_TYPE	VARCHAR2(30)	CHECK IN ('NATIONAL','PASSPORT','REFUGEE'), NOT NULL	Type of ID
SECURITY_LEVEL	NUMBER(1)	CHECK BETWEEN 1 AND 5, DEFAULT 3	Security clearance level
IS_ACTIVE	CHAR(1)	CHECK IN ('Y','N'), DEFAULT 'Y'	Active status
ENCRYPTION_KEY	VARCHAR2(128)	NOT NULL	Data encryption key
CREATED_DATE	TIMESTAMP	DEFAULT SYSDATE	Creation timestamp

Business Rules:

- Each citizen can have only ONE active digital ID
- EXPIRY_DATE must be > ISSUE_DATE
- BIOMETRIC_HASH must be encrypted (handled in application layer)
- Security level 5 = highest clearance

3. AUTHORIZED_ENTITIES (Dimension Table)

Column	Data Type	Constraints	Purpose
ENTITY_ID	NUMBER(10)	PK, NOT NULL	Unique entity identifier

ENTITY_NAME	VARCHAR2(100)	NOT NULL	Organization name
ENTITY_TYPE	VARCHAR2(30)	CHECK IN ('GOVERNMENT','BANK','HOSPITAL','INSURANCE','TELECOM','OTHER'), NOT NULL	Category
LICENSE_NUMBER	VARCHAR2(50)	UNIQUE, NOT NULL	Legal license/registration
CONTACT_PERSON	VARCHAR2(100)	NOT NULL	Responsible officer
CONTACT_EMAIL	VARCHAR2(100)	NOT NULL	Official email
CONTACT_PHONE	VARCHAR2(15)	NOT NULL	Official phone
AUTHORIZATION_LEVEL	NUMBER(1)	CHECK BETWEEN 1 AND 3, DEFAULT 1	Access privilege level
APPROVED_DATE	DATE		When authorization granted
EXPIRY_DATE	DATE		Authorization expiration
STATUS	VARCHAR2(20)	CHECK IN ('ACTIVE','SUSPENDED','REVOKED'), DEFAULT 'ACTIVE'	Current status
CREATED_DATE	TIMESTAMP	DEFAULT SYSDATE	Creation timestamp

Business Rules:

- Only ACTIVE entities can submit access requests
- Authorization expires and requires renewal
- Level 1 = basic access, Level 3 = full access

4. ACCESS_REQUESTS (Fact Table - Critical for Auditing)

Column	Data Type	Constraints	Purpose
--------	-----------	-------------	---------

REQUEST_ID	NUMBER(10)	PK, NOT NULL	Unique request ID
ENTITY_ID	NUMBER(10)	FK → AUTHORIZED_ENTITIES, NOT NULL	Who is requesting
DIGITAL_ID	NUMBER(10)	FK → DIGITAL_IDS, NOT NULL	Which ID is requested
REQUEST_DATE	TIMESTAMP	DEFAULT SYSDATE, NOT NULL	When request submitted
PURPOSE	VARCHAR2(500)	NOT NULL	Legal justification
DATA_CATEGORY	VARCHAR2(50)	NOT NULL	What data is needed
REQUEST_STATUSES	VARCHAR2(20)	CHECK IN ('PENDING','APPROVED','DENIED','EXPIRED'), DEFAULT 'PENDING'	Current status
APPROVED_BY	VARCHAR2(50)		DPO who approved
APPROVAL_DATE	TIMESTAMP		When approved/denied
ACCESS_START_TIME	TIMESTAMP		When access granted
ACCESS_END_TIME	TIMESTAMP		When access expires
IP_ADDRESS	VARCHAR2(45)		Requester IP
USER_AGENT	VARCHAR2(200)		Browser/system info
RISK_SCORE	NUMBER(3,2)	CHECK BETWEEN 0 AND 1	AI-calculated risk (0-1)
CREATED_BY	VARCHAR2(50)		System or user

Business Rules:

- ACCESS_END_TIME must be > ACCESS_START_TIME
 - Expired requests automatically change status
 - High risk_score (>0.7) triggers manual review
-

5. CONSENT_RECORDS (Bridge Table)

Column	Data Type	Constraints	Purpose
CONSENT_ID	NUMBER(10)	PK, NOT NULL	Unique consent record
CITIZEN_ID	NUMBER(10)	FK → CITIZENS, NOT NULL	Whose consent
DATA_CATEGORY_ID	NUMBER(10)	FK → DATA_CATEGORIES, NOT NULL	What data type
ENTITY_TYPE	VARCHAR2(30)		Which entity types allowed
CONSENT_STATUSES	VARCHAR2(20)	CHECK IN ('GRANTED','REVOKED','EXPIRED'), DEFAULT 'GRANTED'	Current status
GRANTED_DATE	TIMESTAMP	DEFAULT SYSDATE	When consent given
EXPIRY_DATE	DATE		When consent expires
REVOKED_DATE	TIMESTAMP		When revoked (if applicable)
CONSENT_LEVEL	VARCHAR2(20)	CHECK IN ('FULL','PARTIAL','RESTRICTED'), DEFAULT 'PARTIAL'	Level of access
CREATED_DATE	TIMESTAMP	DEFAULT SYSDATE	Creation timestamp

Business Rules:

- Citizen can revoke consent at any time
 - Expired consent = automatic DENIED for requests
 - FULL consent = all data, RESTRICTED = minimal fields only
-

6. ACCESS_LOGS (Audit Trail - Critical for Phase VII)

Column	Data Type	Constraints	Purpose
LOG_ID	NUMBER(10)	PK, NOT NULL	Unique log entry
REQUEST_ID	NUMBER(10)	FK → ACCESS_REQUESTS, NOT NULL	Related request
ACTION_TYPE	VARCHAR2(20)	CHECK IN ('VIEW','DOWNLOAD','MODIFY','DELETE'), NOT NULL	What action
ACTION_TIMESTAMP	TIMESTAMP	DEFAULT SYSDATE, NOT NULL	Exact time
ACTION_BY	VARCHAR2(50)	NOT NULL	User/system who acted
ACTION_RESULT	VARCHAR2(20)	CHECK IN ('SUCCESS','DENIED','ERROR'), NOT NULL	Outcome
DENIAL_REASON	VARCHAR2(200)		Why denied (if applicable)
DATA_ACCESSED	CLOB		What fields were viewed
SESSION_ID	VARCHAR2(50)		Session identifier
IP_ADDRESS	VARCHAR2(45)		Source IP
CREATED_DATE	TIMESTAMP	DEFAULT SYSDATE	Log creation time

Business Rules:

- ALL access attempts must be logged (even denials)
- Logs are IMMUTABLE (no updates/deletes allowed)
- Retained for 7 years for compliance

7. ALERTS (Dimension Table)

Column	Data Type	Constraints	Purpose
ALERT_ID	NUMBER(10)	PK, NOT NULL	Unique alert ID
CITIZEN_ID	NUMBER(10)	FK → CITIZENS	Affected citizen
REQUEST_ID	NUMBER(10)	FK → ACCESS_REQUESTS	Related request
ALERT_TYPE	VARCHAR2(30)	CHECK IN ('SUSPICIOUS_ACCESS','UNAUTHORIZED_ATTEMPT','CONSENT_VIOLATION','DATA_BREACH','UNUSUAL_PATTERN'), NOT NULL	Category
SEVERITY	VARCHAR2(10)	CHECK IN ('LOW','MEDIUM','HIGH','CRITICAL'), DEFAULT 'MEDIUM'	Priority
ALERT_MESSAGE	VARCHAR2(500)	NOT NULL	Description
ALERT_DATE	TIMESTAMP	DEFAULT SYSDATE	When generated
STATUS	VARCHAR2(20)	CHECK IN ('NEW','REVIEWED','RESOLVED','FALSE_POSITIVE'), DEFAULT 'NEW'	Current status
REVIEWED_BY	VARCHAR2(50)		DPO who reviewed
REVIEWED_DATE	TIMESTAMP		Review timestamp
RESOLUTION_NOTES	VARCHAR2(500)		What action taken

Business Rules:

- CRITICAL alerts notify DPO immediately

- Alerts expire after 30 days if unresolved
- Citizens receive notification for their alerts

8. DATA_CATEGORIES (Dimension Table)

Column	Data Type	Constraints	Purpose
CATEGORY_ID	NUMBER(10)	PK, NOT NULL	Unique category ID
CATEGORY_NAME	VARCHAR2(50)	UNIQUE, NOT NULL	Category name
DESCRIPTION	VARCHAR2(200)		Detailed description
SENSITIVITY_LEVEL	NUMBER(1)	CHECK BETWEEN 1 AND 5, NOT NULL	Privacy sensitivity (1-5)
REQUIRES_CONSENT	CHAR(1)	CHECK IN ('Y','N'), DEFAULT 'Y'	Needs explicit consent?
CREATED_DATE	TIMESTAMP	DEFAULT SYSDATE	Creation timestamp

Example Categories:

- PERSONAL_INFO (name, DOB, address) - Level 2
- BIOMETRIC_DATA (fingerprints, face scan) - Level 5
- FINANCIAL_INFO (bank accounts, income) - Level 4
- HEALTH_RECORDS (medical history) - Level 5
- CONTACT_DETAILS (email, phone) - Level 1

9. HOLIDAYS (For Phase VII Restriction Requirement)

Column	Data Type	Constraints	Purpose
HOLIDAY_ID	NUMBER(10)	PK, NOT NULL	Unique holiday ID
HOLIDAY_NAME	VARCHAR2(100)	NOT NULL	Holiday name

HOLIDAY_DATE	DATE	NOT NULL	Date of holiday
HOLIDAY_TYPE	VARCHAR2(20)	CHECK IN ('PUBLIC','RELIGIOUS','NATIONAL'), DEFAULT 'PUBLIC'	Category
IS_RECURRING	CHAR(1)	CHECK IN ('Y','N'), DEFAULT 'N'	Annual repeat?
CREATED_DATE	TIMESTAMP	DEFAULT SYSDATE	Creation timestamp

Business Rules:

- NO INSERT/UPDATE/DELETE operations allowed on weekdays (Mon-Fri)
- NO operations allowed on dates in HOLIDAYS table
- Only weekends (Sat-Sun) allow DML operations

10. VIOLATIONS (Fact Table)

Column	Data Type	Constraints	Purpose
VIOLATION_ID	NUMBER(10)	PK, NOT NULL	Unique violation ID
REQUEST_ID	NUMBER(10)	FK → ACCESS_REQUESTS	Related request
ENTITY_ID	NUMBER(10)	FK → AUTHORIZED_ENTITIES	Who violated
VIOLATION_TYPE	VARCHAR2(50)	CHECK IN ('UNAUTHORIZED_ACCESS','CONSENT_BREACH','TIME_VIOLATION','DATA_MISUSE','EXCESSIVE_ACCESS'), NOT NULL	Type
VIOLATION_DATE	TIMESTAMP	DEFAULT SYSDATE	When occurred
DESCRIPTION	VARCHAR2(500)	NOT NULL	Details
PENALTY_AMOUNT	NUMBER(10,2)		Fine imposed

REPORTED_TO_AUTHORITY	CHAR(1)	CHECK IN ('Y','N'), DEFAULT 'N'	Legal reporting
STATUS	VARCHAR2(20)	CHECK IN ('INVESTIGATING','CONFIRMED','DISMISSED'), DEFAULT 'INVESTIGATING'	Current status
CREATED_DATE	TIMESTAMP	DEFAULT SYSDATE	Creation timestamp

NORMALIZATION JUSTIFICATION

1st Normal Form (1NF):

- All tables have atomic values (no repeating groups)
- Each column contains single values
- Each table has a primary key

2nd Normal Form (2NF):

- All non-key attributes fully depend on primary key
- No partial dependencies exist
- Example: CONSENT_RECORDS depends fully on CONSENT_ID, not partially on CITIZEN_ID alone

3rd Normal Form (3NF):

- No transitive dependencies
- Example: ACCESS_REQUESTS.ENTITY_NAME removed (retrieved via FK to AUTHORIZED_ENTITIES)
- ALERTS.CITIZEN_NAME removed (retrieved via FK to CITIZENS)

Design Decisions:

- **Audit-First Design:** ACCESS_LOGS and ALERTS are immutable for compliance
- **Temporal Data:** Multiple timestamp fields track lifecycle of requests
- **Flexible Consent:** CONSENT_RECORDS allows granular control per data category
- **Risk Management:** RISK_SCORE enables AI-driven access decisions

BI CONSIDERATIONS

Fact Tables (Transaction Data):

- ACCESS_REQUESTS (primary fact table)
- ACCESS_LOGS (activity fact table)
- VIOLATIONS (compliance fact table)

Dimension Tables (Descriptive Data):

- CITIZENS (who)
- AUTHORIZED_ENTITIES (who)
- DATA_CATEGORIES (what)
- HOLIDAYS (when)
- ALERTS (events)

Slowly Changing Dimensions:

- **Type 1 (Overwrite):** CITIZENS.ADDRESS, CITIZENS.PHONE_NUMBER
- **Type 2 (Historical):** AUTHORIZED_ENTITIES.AUTHORIZATION_LEVEL (track changes)
- **Type 3 (Limited History):** Not used

Aggregation Levels:

- Daily access request counts
- Monthly compliance metrics
- Quarterly violation trends
- Entity-level access patterns

KEY ASSUMPTIONS

1. **Data Retention:** Audit logs kept for 7 years per GDPR-style regulations
2. **Encryption:** Biometric data encrypted at rest and in transit
3. **Weekday Restriction:** Phase VII requirement - no DML Mon-Fri or holidays
4. **Consent Expiry:** Default consent expires after 1 year unless renewed
5. **Entity Authorization:** Requires annual renewal by Data Protection Officer
6. **Risk Scoring:** AI model calculates risk based on access patterns (future implementation)
7. **Alert Thresholds:** >3 failed access attempts in 1 hour = HIGH severity alert
8. **Data Classification:** Follows ISO 27001 sensitivity levels (1-5 scale)

SAMPLE DATA VOLUMES (for Phase V)

Table	Minimum Rows	Recommended
CITIZENS	200	500

DIGITAL_IDS	200	500
AUTHORIZED_ENTITIES	50	100
ACCESS_REQUESTS	500	1000
CONSENT_RECORDS	400	1000
ACCESS_LOGS	1000	2000
ALERTS	100	300
DATA_CATEGORIES	10	15
HOLIDAYS	20	30
VIOLATIONS	50	100