DECODING KSA'S PRIVACY LAWS

tsaaro.™ consulting

KEY DEFINITIONS

CONTROLLER

Any Public Entity, natural person or private legal person that specifies the purpose and manner of Processing Personal Data.

PROCESSOR

Any Public Entity, natural person or private legal person that processes Personal Data for the benefit and on behalf of the Controller.

PERSONAL DATA

Any data that can directly or indirectly identify an individual, such as name, ID numbers, contact details, financial information, multimedia content featuring the individual, or any other data of a personal nature.

SENSITIVE DATA

Data revealing ethnicity, beliefs, criminal history, biometric or genetic identifiers, health information, or unknown parentage.

DATA SUBJECT

The individual to whom the Personal Data relates.

HEALTH DATA

Any Personal Data related to an individual's health condition, whether their physical, mental or psychological conditions, or related to Health Services received by that individual.

CREDIT DATA

Any Personal Data related to an individual's request for, or obtaining of, financing from a financing entity, whether for a personal or family purpose, including any data relating to that individual's ability to obtain and repay debts, and the credit history of that person.

PERSONAL DATA BREACH

Any incident that leads to the Disclosure, Destruction, or unauthorized access to Personal Data, whether intentional or accidental, and by any means, whether automated or manual

EXPLICIT CONSENT

Direct and explicit consent given by the Data Subject in any form that clearly indicates the Data Subject's acceptance of the Processing of their Personal Data in a manner that cannot be interpreted otherwise, and whose obtention can be proven.

APPLICABILITY & SCOPE

The law covers data processing within the Kingdom, including data related to residents processed from abroad. It also applies to data of deceased individuals if identification is possible.

ART **2** OF PDPL

The law doesn't apply to personal or family use of data, unless the individual discloses it publicly.

CORE PRINCIPLES

- PURPOSE LIMITATION
- DATA MINIMIZATION
- DATA ACCURACY
- TRANSPARENCY

DATA SUBJECTS RIGHTS

Right to be Informed (ART 4(1)of PDPL)

Right to Access (ART 4(2) of PDPL)

Right to Portability (ART 4(3) of PDPL)

Right to Request Correction (ART 4(4) of PDPL)

Right to Request Deletion (ART 4(5) of PDPL)

Right to Withdraw Consent (Art 5(2) of PDPL)

Right to submit a complaint to the Competent Authority **(Art 34 of PDPL)**

ENFORCEMENT AND FINES

Intentionally disclosing sensitive data risks up to **2 years** imprisonment and/or a fine up to **SAR 3M** (**approx. $7,99,241**). Violation of transfer requirements, imprisonment for one year or fine not exceeding **SAR 1M** (**approx. $2,66,413**) (**ART 35 of PDPL**)

Other violations may result in a warning or fine up to **SAR 5M** (approx. **$1,332,069**). (**ART 36 of PDPL**)

Fines can double for repeat offences, and courts may confiscate gains or require publicizing the judgement. (**ART 35(3) of PDPL**)

SAR 3,000,000 to SAR 5,000,000

CROSS BORDER TRANSFER

Under KSA PDPL and Regulation on Personal Data Transfer outside the Kingdom, Cross Border Data Transfer is permissible in case when the SDAIA determines a country as having an adequate level of data protection. (**ART 29(2) of PDPL**)

When there is no adequate protection level is not available, data transfer is permitted with these safeguards (**ART 5 of Regulation on Personal Data Transfer**):

- Binding Common Rules.
- Standard Contractual Clauses.
- Compliance Certifications.
- Approved Binding Codes of Conduct.

When there is no adequate protection level and appropriate safeguards is not available, Data transfer is permitted under the following conditions (**ART 6 of Regulation on Personal Data Transfer**):

- Contractual Necessity.
- National Security and Public Interest.
- Protection of Vital Interests.

OBLIGATIONS OF CONTROLLER

ARTICLE 12 OF PDPL

Controller must provide a privacy policy to Data Subjects before data collection.

ARTICLE 14 OF PDPL

Verify data accuracy, completeness, timeliness, and relevance before processing.

ARTICLE 19 OF PDPL

Implement organizational, administrative, and technical safeguards for data protection.

ARTICLE 20OF PDPL

Controller must notify the Competent Authority and inform the data subjects about data breaches.

ARTICLE 21 OF PDPL

Respond to the requests of the Data Subject. (Respond within a period not exceeding 30 days)

ARTICLE 22 OF PDPL

Conduct Data Protection Impact Assessment.

ARTICLE 23 OF PDPL

Extra controls for processing health data, including restricted access and minimal processing by staff.

ARTICLE 24 OF PDPL

Extra controls for credit data processing, including explicit consent.

ARTICLE 31 OF PDPL

Maintain Records of Processing Activities.

OBLIGATIONS OF PROCESSOR

ARTICLE 17(1) OF IR*

Process personal data based on the agreement with the Controller and provide sufficient guarantees to protect Personal Data

ARTICLE 17(2) OF IR

Comply with instructions of the Controller regarding the personal data processing.

ARTICLE 17(5) OF IR

Secure prior approval from Controller before entering into contracts with sub-Processors

ACHIEVING COMPLIANCE

- DATA INVENTORY & CLASSIFICATION
- TRANSPARENCY & PRIVACY NOTICE
- POLICY & CONSENT FRAMEWORK
- BREACH NOTIFICATION MECHANISMS
- CROSS-BORDER DATA MAPPING
- DATA SUBJECT REQUESTS
- ROPA COMPLIANCE
- SECURITY MEASURES
- RISK & VENDOR ASSESSMENTS
- DATA PROTECTION OFFICER

*'IR' means 'The Implementing Regulation of the Personal Data Protection Law'