paramount
@ssuring Value

KSA Personal Data Protection Law

Key Obligations and Articles

Data Subject Rights

Articles for reference:

Article 3: General Provisions of Data Subject Rights
Article 4: Right to be Informed
Article 5: Right of Access to Personal Data
Article 6: Right to Request Access to Personal Data
Article 7: Right to Request Correction of Personal Data
Article 8: Right to Request Destruction of Personal Data
Article 10: Means of Communication

Articles 3,4,5,6,7 & 8 primarily address the fundamental rights and protections granted to individuals with regard to their personal data. These articles outline the various aspects of data subject rights.

Know your Rights

- Right to be Informed
- Right of Access to Personal Data
- Right to Request Access to Personal Data
- Right to Request Correction of Personal Data
- Right to Request Destruction of Personal Data

Consent & Withdrawal

Articles for reference:

Article 11: Consent

Article 12: Consent withdrawal

1. **Consent:** Article 11 discusses the process of obtaining consent for data processing, emphasizing that it must be freely given, clear processing purposes, and consents shall be documented. It also states that consent shall be given by a person who has full legal capacity and independent consent shall be obtained for each processing purpose.

2. **Consent withdrawal:** Article 12 addresses consent withdrawal for personal data processing, emphasizing the right to withdraw, easy withdrawal procedures, and the impact on prior processing. It also mandates notifying recipients and requesting data destruction while acknowledging other legal bases for processing.

3. **Consent shall be explicit when processing involves :-**

   - Sensitive Data.
   - Credit Data.
   - Decisions are made solely based on automated processing of personal data.

Protecting Special Category Data

Articles for reference:

Article 9: Anonymization
Article 13: Legal Guardian
Article 26: Processing Health Data
Article 27: Processing Credit Data

1. **Anonymization:** Article 9 outlines the rules for anonymizing personal data. Controllers must ensure that re-identification of the data subject is impossible after anonymization, evaluate the risks of re-identification, and take measures to mitigate them. They should also assess the effectiveness of anonymization techniques and adjust as needed.

2. **Legal Guardian:** Article 13 states that for data subjects lacking full/partial legal capacity, their legal guardian must act in their best interests. The guardian can exercise the data subject's rights and consent to data processing. In such cases, the controller must verify the guardianship. When obtaining consent from the legal guardian, it should not harm the data subject's interests and should allow them to exercise their rights once they reach legal capacity.

2. **Health & Credit Data:** Articles 26 & 27 talk about processing Health and Credit data respectively and outline the appropriate organizational, technical and administrative measures a controller shall take to protect it.

Data Privacy Principles

Articles for reference:

Article 4 : Right to be Informed
Article 8 : Right to Request Destruction of Personal Data
Article 11 : Consent
Article 16 : Processing for Legitimate Interest
Article 19 : Data Minimisation
Article 22 : Correction of Personal Data
Article 31 : Photographing or Copying Official documents that reveal the identity of data subjects

1. **Data Minimisation:** Article 19 talks about the data minimisation principle of data privacy and states that the controller shall collect only the minimum amount of personal data necessary to achieve the purpose of processing.

2. **Accuracy:** Article 22 talks about the controller's responsibility of correcting data that is incorrect, completing data that is incomplete or updating data that is outdated and outlines the actions to be taken while fulfilling the responsibility.

3. **Integrity & Confidentiality:** Article 23 states that the Controller shall take the necessary organizational, administrative, and technical measures to ensure the security of Personal Data and the privacy of the Data Subjects.

4. **Fairness & Transparency:** Article 11 (a) & 11 (b) talks about the collection of consent freely without misleading methods and states that the processing purposes shall be clear, specific, and shall be explained and clarified to the data subject before or at the time of requesting consent.

5. **Purpose & Storage Limitation:** Article 4(6) states that the controller shall provide the data subject with necessary information when engaging in additional processing of personal data other than the one for which it was initially collected for before conducting the additional processing. Article 8(1.b) & and Article 31 say that if personal data is no longer necessary to achieve the purpose for which it was collected, the controller shall destroy the personal data.

6. **Lawfulness and Accountability:** Article 16 permits controllers (except in cases where the controller is a public entity) to process personal data for legitimate interests, with conditions including legal compliance, balancing rights, and assessing potential harm to the data subject's rights and interests. If issues arise, the controller must adjust the process or find another legal basis.

Controller Responsibilities

Articles for reference:

Article 17: Choosing the Processor
Article 23: Information Security
Article 24: Notification of Personal Data Breach
Article 25: Impact Assessment
Article 32: Data Protection Officer
Article 33: Records of Personal Data Processing Activities

1. **Notification of Personal Data Breach:** Article 24 outlines that in the event of an incident that potentially causes harm to the personal data, or to a data subject or conflicts with their rights or interests, the Controller shall notify the Competent Authority within a delay not exceeding (72) hours of becoming aware of the incident.
2. **Appointment of a Data Protection Officer:** Article 32 outlines the appointment and responsibilities of a Data Protection Officer (DPO).
3. **Records of Personal Data Processing Activities:** Article 33(1) states that the Controller shall retain the record of Personal Data Processing activities during the period of the Processing, in addition to five years starting from the date of completion of the Personal Data Processing activity.
4. **Impact Assessment:** Article 25 states that the Controller shall prepare a written and documented assessment of the potential impacts and risks that may affect the Data Subject as a result of Personal Data Processing and the cases where impact assessments shall be conducted.
5. **Choosing the Processor:** Article 17 focuses on the Controller's responsibility to select a processor that provides sufficient guarantees to protect personal data.
6. **Information Security:** Article 23 states that the Controller shall take the necessary organizational, administrative, and technical measures to ensure the security of Personal Data and the privacy of data subjects.

Personal Data Processing Practices

Articles for reference:

Article 14: Processing to Serve the Actual Interest of Data Subject

Article 15: Collecting Data from Third Parties

Article 16: Processing for Legitimate Interest

Article 18: Further Processing of Personal Data

Article 20: Disclosure of Personal Data

1. **Processing for Actual Interests:** Article 14 states that the controller shall retain evidence in case an Actual interest exists when processing the personal data of the Data Subject.
2. **Collecting Data from Third Parties**: Article 15 pertains to collecting personal data from third parties, emphasizing the need for legality when processing such data and compliance with specific regulations governing data collection from publicly available sources.
3. **Processing for Legitimate Interests:** Article 16 talks about allowing data processing for legitimate interests except in cases where the controller is a public entity while balancing rights, conducting assessments, and taking precautions.
4. **Personal Data Usage Beyond Original Purpose:** Article 18 talks about defining clear processing purposes, documenting procedures, and minimizing data collection for additional processing.
5. **Disclosure of Personal Data:** Article 20 addresses disclosure of data collected from publicly available sources, considering specific purposes, safeguarding privacy, and documenting disclosure operations.

Data Processing for Marketing and Research

Articles for reference:

Article 28: Processing Data for Advertising or Awareness Purposes

Article 29: Direct Marketing

Article 30: Collection and Processing of Data for Scientific, Research, or Statistical Purposes

1. **Advertising and Awareness Materials:** Article 28 discusses consent, sender information, and opt-out mechanisms for advertising and awareness materials.

2. **Direct Marketing:** Article 29 addresses consent, sender identification, and prompt cessation of marketing upon withdrawal of consent.

3. **Scientific, Research, or Statistical Purposes:** Article 30 pertains to data collection for research, emphasizing specific purposes, minimal data collection, and safeguarding data subject rights.

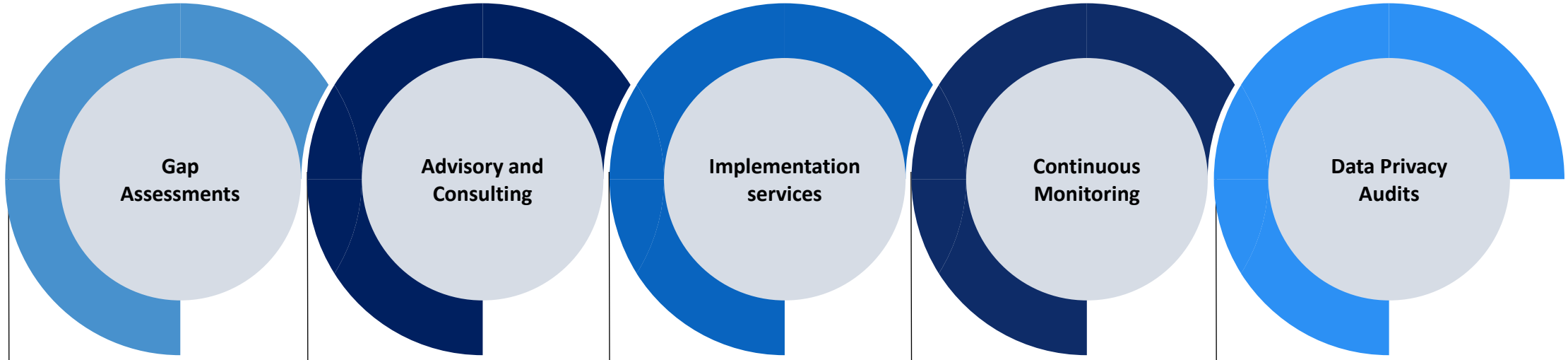
Cross-Border Data Processing

1. **Data Protection Evaluation:** Article 3 talks about evaluating data protection levels abroad based on criteria like existing laws, rule of law, and cooperation willingness, applicable to countries, sectors, or organizations by the competent authority.
2. **Evaluation Results:** Article 4 outlines the evaluation and reporting of the assessments by the competent authority outside the Kingdom to the Prime Minister including recommendations.
3. **Exemption cases:** Articles 5, 6 & 7 talk about the transfer based on appropriate safeguards for transferring personal data outside the Kingdom, its exceptions and cases where exemptions are not granted.
4. **Risk Assessment:** Article 8 talks about the cases where the Controller shall conduct a risk assessment of the Transfer of Personal Data outside the Kingdom or disclosure to a party outside the Kingdom.

Articles for reference:

Article 3: Evaluation of the Level of Protection for Personal Data
Article 4: Results of the Evaluation of the Personal Data Protection Level
Article 5: Transfer based on appropriate safeguards for transferring personal data outside the Kingdom
Article 6: Cases where the appropriate safeguards for Transfer of Personal Data outside the Kingdom are not required
Article 7: Cases where Exemptions are not Granted
Article 8: Risk Assessment of Transferring or Disclosing Personal Data outside the Kingdom

Our approach to help you achieve KSA PDPL Compliance



Assess existing data privacy gaps within the organization against applicable laws on the basis of a privacy control checklist and offer recommendations

Assist in organization -wide data privacy framework, governance structure and mitigate data privacy risks to meet regulatory requirements.

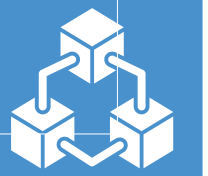
Drive data privacy processes through automation and provide support at each phase of data lifecycle.

Monitor privacy governance program through continuous risk assessments and provide training to employees.

Support in conducting internal data privacy audits followed by privacy roadmap.

Get the Paramount Advantage

Technology driven Privacy program implementation



Multi-regulatory coverage across Middle East

Qualified and experienced professionals (CIPP/E, CIPM, CIPT, FIP, etc.)

Contact Us

grcp@paramountassure.com

https://paramountassure.com/data-privacy/