KARM

صندوق النقد العربي
ARAB MONETARY FUND

مجلس محافظي المصارف المركزية ومؤسسات النقد العربية
COUNCIL OF ARAB CENTRAL BANKS AND MONETARY AUTHORITIES GOVERNORS

Comparison of Data Protection Regimes: EU, Australia, KSA & ADGM

Arab Regional Fintech WG Sixth Meeting
24-25 November 2021

EU GDPR, KSA Personal Data Protection Law and ADGM Data Protection Regulations – lay separate obligations for controllers and processors

Australia Privacy Act – lays obligations for all APP entities – carrying out collection, use or disclosure

Agenda

- **Providing a brief comparison of laws governing data protection in EU, Australia, KSA and ADGM.**
- **Developing an understanding of the key concepts in the data protection laws of aforesaid jurisdictions.**
- **Underscoring key differences between the data protection regimes of the aforesaid jurisdictions.**

JURISDICTIONS	APPLICABLE LAWS
EU	General Data Protection Regulations, 2018
Australia	The Privacy Act, 1988
KSA	Personal Data Protection Law, 2021
ADGM	Data Protection Regulations, 2021

	Territorial		Personal	Material		
	Companies established within the jurisdiction	Companies not established within the jurisdiction- but are linked to data subjects within the jurisdiction		Means of collection		Definition of personal data/ information
				Automated	Manual	
EU	✓	✓	All natural Persons residing in EU (explicitly excludes deceased persons)	✓	✓	Related to a directly or indirectly identified or identifiable data subject
Australia	✓	✓ (only companies that have an Australian Link i.e. it has a legal presence in Australia, as a citizen, partnership, body corporate, unincorporated association or it carries on business in Australia or an external territory or it collected or held personal information in the same)	All natural Persons	✓	✓	Information/ opinion about an identified individual, or an individual who is reasonably identifiable
KSA	✓ (only if they collect personal data of individuals residing within KSA)	✓	All natural Persons residing in KSA (explicitly includes deceased persons)	✓	✓	Whatever source or form that would lead to the identification of the individual specifically
ADGM	✓		All natural Persons irrespective of their residence	✓	✓ (only where it is intended to form part of filing system)	

	Personal/household activities	Non-business capacity	Small businesses	Activities related to the criminal judicial system	Anonymized data
EU	✓			✓	✓
Australia	✓	✓ Activities carried out for employment purposes, political act and practices, or by organisations acting under Commonwealth or State contracts or journalism purposes	✓ under the AUD 3 million (approx. €1.8 million) turnover threshold and not otherwise subject to the Privacy Act/APPs		✓
KSA	✓				
ADGM	✓			✓	

	Differentiates between data controllers and processors	Definition of Controllers	Definition of Processors
EU	✓	Article 4(7)- alone or jointly with others, determines the purposes and means of the processing of personal data	Article 4(8)- processes personal data on behalf of the controller
Australia	No Applies to all private sector entities with the exceptions provided in Section 6D		
KSA	✓	Article 1(18)- that specifies the purpose and manner of processing personal data, whether they process the data by themselves or by a processing entity.	Article 1(19)- processes personal data for the benefit of, and on behalf of, the controlling entity.
ADGM	✓	Article 60- determines the purposes and means of the Processing of Personal Data	Article 60- processes personal data on behalf of the Controller

	Relevant Provisions	Definition of Sensitive Data	Prohibition on processing	Exceptions
EU	Article 9	Racial or ethnic origin Political opinions Religious or philosophical beliefs Trade union membership Genetic data Biometric data Health data Sexuality Sexual orientation	✓	Consent; Authorized by law; Public domain; Judicial activity ; Necessary for public interest, public health, scientific and historic research.
Australia	No separate provision- included in the provisions permitting processing	In addition to the definition provided in EU GDPR, includes Criminal Record data	General obligation are applied more rigorously	
KSA	Article 26	In addition to the definition provided in EU GDPR, includes Criminal Record, security, location and credit data	✓ No separate provision except for prohibition on use for marketing, scientific and research purposes, and on cross border transfer of sensitive data	Processing for scientific, research or statistical purposes can be carried out with consent.
ADGM	Article 7	In addition to the definition provided in EU GDPR, includes Criminal Record and security data	✓	Consent; legal obligations; vital for data subject incapable of giving consent; public health; public interest; judicial activity.

LAWFULNESS, FAIRNESS AND TRANSPARENCY

PURPOSE LIMITATION

DATA MINIMIZATION

ACCURACY

STORAGE LIMITATION

INTEGRITY AND CONFIDENTIALITY

ACCOUNTABILITY

صندوق النقد العربي
ARAB MONETARY FUND

	Governing Provisions	Consent based	Additional grounds where consent is not required	
			Common Grounds	Additional Grounds
EU	Articles 6, 7, 8, 11	Informed consent	Processing for performance of contract Processing to Carry out legal obligations Processing where consent cannot be obtained, but is necessary to protect vital interests Public interest	Processing that does not require identification
Australia	Schedule 1, Part 2, Clause 3	Informed consent		
KSA	Articles 5, 6, 10, 27	Informed consent		
ADGM	Sections 5, 6,	Informed consent		To protect legitimate interests of controllers that supersede interests of data subjects

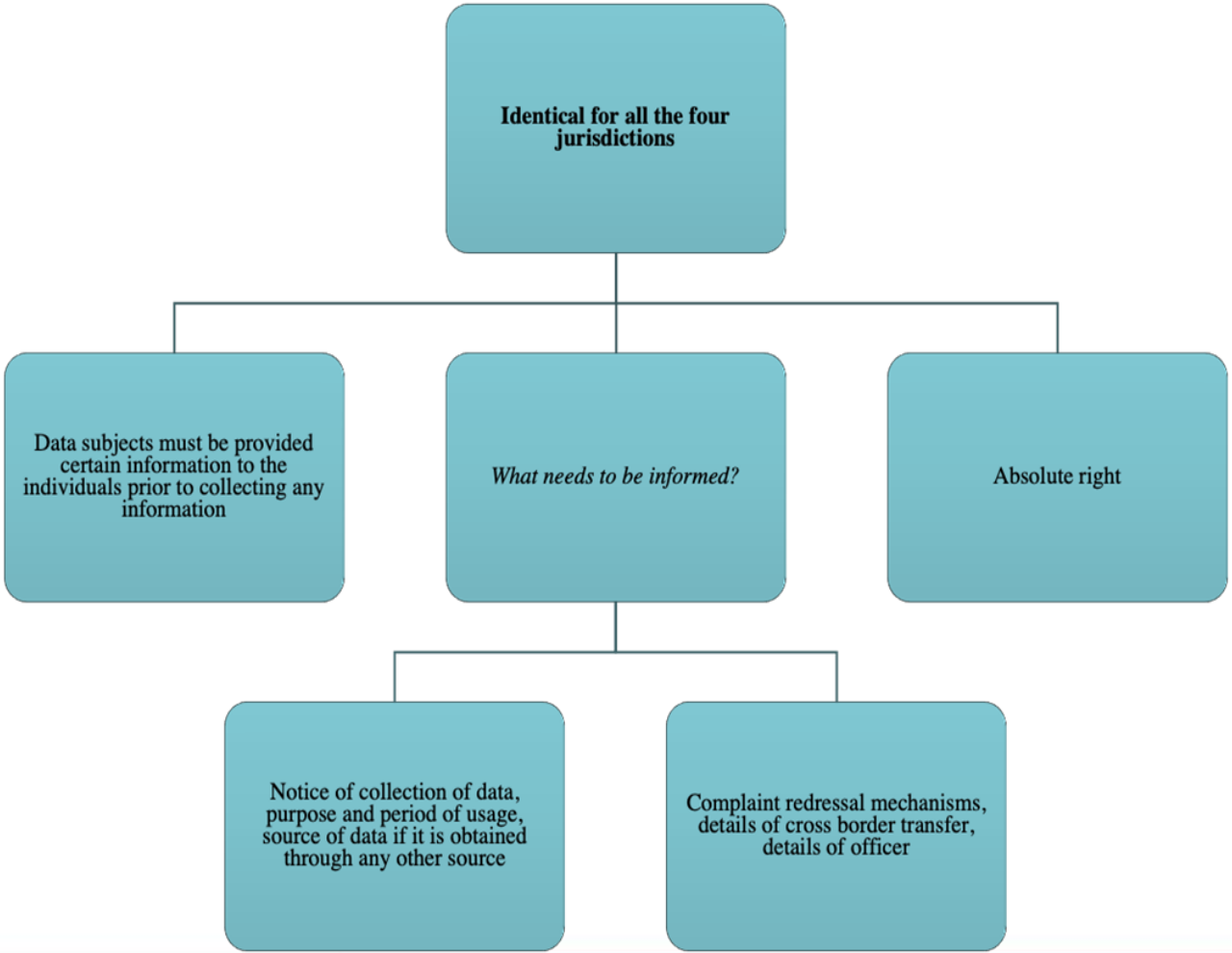
RIGHTS OF DATA SUBJECT/ OWNER

01	02	03	04	05	06	07
Right to erasure/ deletion	Right to correction/ rectification	Right to be informed	Right to opt-out/ withdraw	Right to access	Right to data portability	Right to not identify one-self

Allows individuals to request the deletion or correction of their personal information

Not an absolute right- subject to exceptions

	Governing provisions	Grounds	Exceptions	Entity Responsible
EU	Article 16, 17, Recital 65	Withdrawal of consent; unlawful processing; objection to processing; legal compliance (for deletion only)	Freedom of Speech and Expression; to fulfil a legal obligation; public interest, scientific or historic research; establishment, exercise or defence of legal claims (for deletion only)	Controllers
Australia	Not provided. However, certain aspects of this right are covered under Australia Privacy Principles 11 and 13 providing for de-identification of information once purpose for collection is fulfilled and rectification of personal information			
KSA	Article 4(4), (3)	Retention of data no longer needed		Controllers
ADGM	Article 14, 15	Retention of data no longer needed; consent is withdrawn; objection to processing; legal obligation.	Legal obligations; public health; archiving and research purposes; establishment, exercise or defence of legal claims.	Controllers


Identical for all the four jurisdictions
Data subjects must be provided certain information to the individuals prior to collecting any information
What needs to be informed?
Absolute right
Notice of collection of data, purpose and period of usage, source of data if it is obtained through any other source
Complaint redressal mechanisms, details of cross border transfer, details of officer

RIGHT TO OBJECT/OPT-OUT/WITHDRAW CONSENT

	Allows data subjects the option to withdraw consent or object to the processing of their data at any time	Absolute Right
EU	✓	No
Australia	No Australia only provides for a right to opt out from direct marketing or usage of information used for direct marketing in Australia Privacy Principles Article 7.6	No
KSA	✓	No
ADGM	✓ ADGM provides for a right to restriction of processing under Section 16 during the pendency of a claim raised by the data subject, in addition to the right to opt-out.	No

How is right to data portability different from right to access?

While both allow users to access personal data, right to data portability allows access in a machine-readable format and is applicable specifically to processing of data by automated means.

	Allows data subjects to access and receive a confirmation on the data and its nature which is being processed	Right to Data Portability
EU	✓	Provided for separately from right to access
Australia	✓	Not provided for separately. However, can be covered under right to access.
KSA	✓	Not provided for separately. However, can be covered under right to access.
ADGM	✓	Provided for separately from right to access

Australia	Data subjects under APP 2 can deal with an entity anonymously unless required by law or impractical.
EU, KSA, ADGM	Not recognized

EU GDPR, KSA Personal Data Protection Law and ADGM Data Protection Regulations – lay separate obligations for controllers and processors

Australia Privacy Act – lays obligations for all APP entities – carrying out collection, use or disclosure

Note: these obligations are in addition to the ones corresponding to the rights of data subjects

OVERVIEW: OBLIGATIONS OF CONTROLLERS AND PROCESSORS

		Data privacy by default	Maintain records	Security measures	Notification to authority and data subject upon data breach	Risk/ impact assessment	Data protection/ compliance officer	Contract for processing on behalf of other entity	Other
EU	Controllers	✓ Integrate data protection concerns into every aspect of their processing activities.	✓ Are required to maintain a record of their processing activities, covering areas such as processing purposes, data sharing and retention.	✓	✓ Report certain types of personal data breach to the relevant supervisory authority (within 72 hours of becoming aware of the breach, where feasible)	✓ Carry out Data Protection Impact Assessment if processing operation is 'likely to result in high risks to the rights and freedoms of natural persons.	✓		Representatives if not established within the EU
	Processors			✓	✓ Notify controller		✓	✓ Processing shall be governed by a contract or other legal act under Union or Member State law	Representatives if not established within the EU
Australia	Unlike European law, there is no concept of data 'controller' or 'processor' under Australian privacy law. The APP entity is considered as the controller.			✓ Require APP entities delete or de-identify all personal information once all legal requirements have passed	✓	✓ Only mandated at the direction of Information Commissioner	Not mandated but is recommended by Privacy Commissioner	As there is no separation between controllers and processors, same obligations apply- no requirement for contract	

OVERVIEW: OBLIGATIONS OF CONTROLLERS AND PROCESSORS

		Data privacy by default	Maintain records	Security measures	Notification to authority and data subject upon data breach	Risk/ impact assessment	Data protection/ compliance officer	Contract for processing on behalf of other entity	Other
KSA	Controllers	✓	✓ Maintain a record of processing for a period that will be prescribed by the executive regulations	✓ Controlling to notify competent authority as soon as it becomes aware of a leakage or damage of personal data	✓	✓ Conduct an evaluation of the consequences of processing personal data for any product or service provided to the public according to the nature of the activity practiced by the controlling entity.	✓		
	Processors	✓		✓				✓	Confidentiality even after contract termination
ADGM	Controllers	✓	✓	✓ Must implement appropriate measures to ensure a level of security appropriate to the risk	✓	✓	✓		Pay data protection fee
	Processors				✓ To the controller		✓	✓	

	Relevant Provision	Role of Data Protection/ Compliance Officer
EU	**Article 39**	Inform the entities of compliances, monitor entities, advise based on outcome of data protection impact assessment, cooperate with supervisory authority.
Australia		A data protection officer is not mandated by law in Australia but it is recommended by the Privacy Commissioner to comply with APP 1.2.
KSA	**Article 30**	Implementation of the Law by controlling entities, cooperate with supervisory authority.
ADGM	**Article 37**	Inform and advise on law, monitor compliance, advise based on outcome of data protection impact assessment, cooperate with supervisory authority.

	Conditions	Permissions	Safeguards
EU	- The European Commission provides a list of the third country/ organization/ specified sectors that ensure adequate level of protection to which data can be transferred to. - A Cross-Border Data Transfer may take place on the basis of an approved Code of Conduct, together with binding and enforceable commitments to provide appropriate safeguards. - Binding corporate rules. - To develop international cooperation mechanisms for effective enforcement of data protection legislation.	None	- Enforceability of rights and remedies - Binding corporate rules
	Exceptions: Article 49 states grounds for cross border transfer of data in the absence of adequacy decision, these are: -Data subject has given consent -Necessary for the performance of a contract -to protect vital interests of other persons or public interest -establishment or defence of legal claims		
Australia	-APP entity must ensure the overseas entity will handle the data in accordance with the APPs. APP will be responsible in case of any mishandling. -Reasonable steps to prevent breach.	None	Follow the Australian Privacy Principles
	Exceptions: APP 8.2 provides exceptions including comparable protection in the overseas jurisdiction. APP can share information where: -APP entity reasonably believes that the overseas recipient is subject to a law or binding scheme that has the effect of protecting the information in a way that is substantially similar to the APPs		

	Conditions	Permissions	Safeguards
KSA	Prohibited Exception: extreme necessity to preserve the life of the data owner outside KSA or his vital interests or to prevent, examine or treat an infection	Yes	- Does not prejudice national security or the vital interests - Guarantee of confidentiality
ADGM	- The Commissioner of Data Protection has decided that the third country/ organization/ specified sectors within ensure adequate level of protection. - Data can be transferred to a third country or an international organization if the controller or processor has provided appropriate safeguard. - Binding corporate rules. Exception: Section 42 Transfers subject to appropriate safeguards Section 44 Derogations in specific situations, such as: -Data subject has given consent -Necessary for the performance of a contract -to protect vital interests of other persons or public interest -establishment or defence of legal claims	None	- The safeguards are only mandated if the adequacy decision is spending - Includes binding corporate rules

Jurisdiction	Supervisory Authority
EU	-Article 51- each member state shall appoint an independent supervisory authority. -European Data Protection Board- head of one supervisory authority of each Member State and of the European Data Protection Supervisor, or their respective representatives.
Australia	-Office of Australian Information Commissioner -Australia Information Commissioner -Privacy Commissioner (currently the Australian Information Commissioner)
KSA	-First 2 years- The Saudi Authority for Data and Artificial Intelligence. -Later to National Data Management Office, based on the results
ADGM	-Office of Data Protection. -The Board of Directors of ADGM can appoint a Commissioner of Data Protection

	Provisions	Penalty
EU	Each member state may lay down rules for penalties under Article 84 in addition to administrative fines under Article 83.	Can range from €10 million, or 2% of the firm's worldwide annual revenue from the preceding financial year to €20 million, or 4% of the firm's worldwide annual revenue from the preceding financial year, whichever amount is higher.
Australia	Part VIB Section 80U provides for the civil penalty provisions.	Maximum penalty for a corporation for serious and repeated interferences of privacy is currently AUD 2, 220,000 although the government is planning to increase the maximum penalties to the greater of: (a) AUD 10 million, (b) three times the benefit obtained through misuse of personal information; and (c) 10% of the company's annual domestic turnover.
KSA	Article 35 prescribes for imprisonment and civil penalties.	Unlawfully transferring data out of KSA can result in imprisonment of up to 1 year and/or a fine of up to SAR 1 million. Disclosing sensitive data unlawfully can result in imprisonment up to 2 years and/or a fine of up to SAR 3 million.
ADGM	Part VII, Section 54-56 prescribes administrative fines.	The regulator can issue fines of up to $28 million for serious breaches of the regulations.

Thank you

صندوق النقد العربي
ARAB MONETARY FUND