COMPARISON BETWEEN GCC DATA PROTECTION LEGISLATION

A report by the Research Syndicate Group on the UK Gulf Women in Cybersecurity Fellowship programme.

2023

Foreign, Commonwealth & Development Office

plexal

PGI

1. INTRODUCTION

In today's rapidly advancing digital age, data privacy has become an increasingly important concern for individuals, organisations, and governments worldwide. With the growing dependency on digital platforms and the widespread collection, storage and use of personal data, the need for robust data privacy regulations has become paramount.
This report was conducted by the UK Gulf Women in Cybersecurity Fellowship Research Syndicate Group members, and aims to provide a comprehensive analysis of the data privacy policy regulations implemented in the six GCC countries. By examining the legal frameworks, regulatory bodies, key provisions and enforcement mechanisms, this report sheds light on the current state of data privacy in the GCC region.
Key findings:

1. **Legal frameworks:** All GCC countries have enacted data protection laws or regulations, either at the national or sector-specific level, to safeguard personal data. While some countries have comprehensive data protection frameworks, others are in the process of developing and implementing such legislation.
2. **Regulatory bodies:** Each GCC country has established a regulatory authority responsible for overseeing data privacy and protection. These bodies play a crucial role in enforcing data privacy regulations, ensuring compliance and handling complaints related to data breaches or privacy violations.
3. **Key provisions:** Common provisions found in the data privacy policies of GCC countries include consent requirements for data processing, rights of data subjects, data breach notification obligations, cross-border data transfer regulations and the establishment of lawful bases for data processing.
4. **Sector-specific regulations**: Several GCC countries have implemented sector-specific data privacy regulations to address unique

challenges and requirements of industries such as healthcare, telecommunications, finance and e-commerce. These regulations often supplement the overarching Data Protection Laws (DPLs).

5. **International alignment**: The GCC countries are making efforts to align their data privacy regulations with international frameworks, such as the General Data Protection Regulation (GDPR) implemented by the European Union. This alignment aims to facilitate international data transfers and enhance cooperation in data protection matters.
6. **Enforcement mechanisms**: The GCC countries employ various enforcement mechanisms to ensure compliance with data privacy regulations. These mechanisms include penalties, fines, audits, inspections and the establishment of data protection officers within organisations.
7. **Data localisation**: Some GCC countries have implemented data localisation requirements, mandating that certain categories of personal data be stored within the country's borders. These measures aim to enhance data security and protect national interests.

The findings of this report provide valuable insights into the data privacy policy regulations in the GCC countries, identifying trends, best practices and areas for improvement within the region. This analysis not only helps in evaluating the effectiveness of these policies in safeguarding individuals' privacy rights but also informs future research, policy development and international comparisons. By examining the experiences and lessons learned from the GCC countries' endeavours in data privacy, policymakers and stakeholders worldwide can gain valuable insights to strengthen their own data protection frameworks.

In conclusion, this report represents the collective effort of the UK Gulf Women in Cybersecurity Fellowship Research Syndicate Group's members to examine and evaluate the data privacy policy regulations in the GCC countries.

By delving into the legal frameworks, regulatory mechanisms, key provisions and enforcement practices, this report provides a comprehensive understanding of the data privacy landscape in the region.

The insights gained from this analysis contribute to the ongoing discourse on data privacy and facilitate informed discussions for the development of effective policies and practices to protect individuals' privacy rights in the digital age.

2. METHODOLOGY

The research is based on a descriptive research design to analyse and evaluate the data privacy policy regulations in GCC countries. The information was gathered by searching the official websites and public documentations of relevant governmental and regulatory bodies in each of the GCC countries [1-5, 7-9]. To have a comparative analysis between the GCC PDPLs, certain criteria were considered, including:

1. Definitions of personally identifiable data
2. Sharing of data between other countries
3. Enforcement
4. Breach notification
5. Online privacy
6. Timeline (how recent)
7. How closely it follows GDPR
8. Particularly sensitive data (for example, biometrics)
9. Scope
10. External auditor/s required
11. Child protection data
12. DPL published in English

All data collected from websites were publicly available and did not involve any personal or sensitive information. The analysis is based solely on publicly available information from official websites, which might not reflect the complete picture of data privacy in the GCC countries. The research is specifically focused on data privacy policy regulations in the

seven GCC countries. In this paper, the following sections cover the PDPL for each GCC country:

- Section 3: Bahrain
- Section 4: Kuwait
- Section 5: Oman
- Section 6: Qatar
- Section 7: KSA
- Section 8: UAE

Finally, the conclusion and recommendations are discussed in Section 9.

3. BAHRAIN

Bahrain, a small island country in the Arabian Gulf, has taken significant steps to safeguard the privacy and security of personal data through its data protection regulations. The primary legislation governing data protection in Bahrain is the Personal Data Protection Law (PDPL). The PDPL establishes a comprehensive framework for the collection, processing, storage and transfer of personal data, with the aim of ensuring individuals' rights and protecting their privacy. It sets out various principles and obligations for data controllers and processors, including requirements for obtaining consent, implementing security measures and facilitating individuals' rights to access and rectify their personal information.

The PDPL also empowers the Personal Data Protection Authority (PDPA) to oversee and enforce compliance with the law, promoting a culture of responsible data handling in Bahrain. Overall, Bahrain's data protection regulation reflects its commitment to safeguarding personal data and fostering a trustworthy digital environment.

3.1 Definitions of personally identifiable data

According to the PDPL, personal data encompasses all forms of information about an identifiable individual or someone who can be identified, either directly or indirectly. This includes their personal identification number, as well as any of their physical, physiological, intellectual, cultural, economic characteristics, or social identity.

3.2 Sharing of data between other countries

The transfer of personal data out of Bahrain is restricted, and it can only take place if the recipient country or region ensures an adequate level of protection for the personal data. This provision aims to safeguard the privacy and security of individuals' information during cross-border transfers.

3.3 Enforcement

Any individual who violates the law may face criminal consequences, including imprisonment for a maximum of one year and/or a fine ranging from BHD 1,000 to BHD 20,000.

3.4 Breach notification

According to the PDPL, there is no explicit requirement for data controllers to notify the Authority or the data subjects in the event of a personal data breach. However, there is a general requirement on the data protection officer to notify the Authority of any breach under the PDPL of which the data protection officer becomes aware.

3.5 Timeline

In 2018, Bahrain introduced Law No. 30 of 2018, known as the PDPL, which serves as the primary legislation governing data protection in the country. The PDPL became effective on 1 August 2019, and it takes precedence over any other laws that may conflict with its provisions.

3.6 How closely it follows GDPR

Both GDPR and PDPL apply to entities that collect and process personal data of individuals. The GDPR applies to entities handling personal data of

EU residents, while the PDPL applies to entities handling personal data of Bahrain residents.

Both regulations define personal data as any information that pertains to an identified or identifiable person. This means that any data that can directly or indirectly identify an individual falls under the scope of protection provided by both the GDPR and the PDPL.

3.7 Particularly sensitive data

Sensitive personal data is a category within the broader scope of personal data. It refers to information that, directly or indirectly, discloses an individual's race, ethnicity, political or philosophical opinions, religious beliefs, trade union membership, criminal record, or any data related to their health or sexual life. Due to the potentially sensitive nature of this information, data controllers are required to handle it with extra caution and adhere to more stringent data protection measures.

3.8 Scope

According to the PDPL, the Authority is empowered to conduct investigations into potential violations of the law independently, upon the request of the responsible minister, or in response to a complaint.

The Authority holds the mandate to issue orders aimed at ceasing any violations, which may include the issuance of emergency orders and the imposition of fines. In cases where people have suffered harm as a result of their personal data being processed unlawfully by a data controller or because of a violation of the PDPL by a business's data protection officer, civil compensation is allowed.

In summary, the PDPL grants the Authority the ability to investigate violations, take necessary measures to address them and impose penalties, while also providing avenues for people to seek compensation for damages when there is non-compliance.

3.9 External auditor/s required

There is no specific mandate for involving external auditors to enforce this law. However, the Board of Directors of Personal Data Protection Authority can receive and investigate full company audits where appropriate [10].

3.10 PL published in English

There is an English translation of Law No. 30 of 2018 with Respect to Personal Data Protection Law online [10].

4. KUWAIT

Kuwait, a small country to the north east of the Arabian Peninsula, doesn't have a formal personal data protection law but it has Data Protection Regulation (DPR). Previously, laws governing electronic records, signatures, documents, and payments, such as Kuwait Law No. 20 of 2014 on Electronic Transactions (the E-Commerce Law), governed privacy and data protection.

Meanwhile, the Cybercrime Law (Kuwait Law No. 63 of 2015 on Combating Cyber Crimes) prescribed severe penalties for the unauthorised alteration or acquisition of personal or official data or information. The Communications and Telecommunications Regulatory Authority (CITRA) introduced Decision No. 42 of 2021 on Data Privacy Protection Regulation (DPPR) (Data Protection Regulation (DPR), which imposed obligations in relation to data protection on Telecommunication Services Providers and related industry sectors that collect, process or store personal data, in whole or in part.

The DPR outlines the requirements for gathering and holding onto personal data, as well as the obligations of a service provider during or after they provide the service. Since there were no specific data protection laws or regulations, it was necessary to rely on the few applicable legal requirements found in other legislation(s), such as the E-Commerce Law and Cybercrime Law, so it was a major milestone when the DPR was introduced.

Regardless of whether data processing takes place inside Kuwait or outside, all service providers are subject to the DPR, which mandates that they disclose to customers how their data is gathered, used and kept [2].

4.1 Definitions of personally identifiable data

A person's positional affairs, personal status, health state, or elements of financial disclosures are regarded to be at least some of their personal data. Additionally, CITRA published the Data Classification Policy (DCP), which organisations working with vast amounts of data can use as a guide for data protection. Public data, private non sensitive data, private sensitive data and very sensitive data are all defined in the DCP [3,4].

4.2 Sharing of data between other countries

Similar to GDPR of the European Union, Kuwait's DPR mandates that service providers keep a record of processing activities which CITRA can request to inspect. Details like the transfer of personal data outside of Kuwait should be included in the records. Regardless of whether data processing takes place inside Kuwait or outside, all service providers are subject to the DPPR, which mandates that they disclose to customers how their data is gathered, used and kept.

4.3 Enforcement

To enforce the protection of data, penalties can be issued, such as a fine of KWD 500 to KWD 20,000, or a combination of both. Non-compliance could also result in a sentence of one to five years in jail. In addition, anyone who exposes personal information without appropriate authorisation or a court order faces a maximum sentence of three years in prison and fines of at

least KWD 5,000 (US$ 17,500). The E-Commerce Law also allows for the seizure of any software, hardware or other items used for illegal disclosure.

4.4 Breach notification

If there is a breach of personal data, the service provider must notify the owner of the personal data within 72 hours of becoming aware of the breach and include information about technical security precautions.

The Regulation mandates that Telecommunications Service Providers (TSPs) notify CITRA of any breach of personal data within 72 hours of becoming aware of it, or within 24 hours in the case of an erroneous disclosure to or access by a third party that could harm a significant number of users [4].

4.5 Online privacy

The DPR expands the definition of "service provider" to include anyone who:

- runs a website, smart application or cloud computing service
- collects or processes personal data
- instructs a third party to do so on its behalf, using information centres that they directly or indirectly own or use

This definition includes traditional TSPs.

4.6 Timeline

Private and public electronic records, signatures, documents and payments were subject to regulations governing privacy and data protection under laws such Kuwait Law No. 20 of 2014 on Electronic Transactions (the "E-Commerce Law"). The Cybercrime Law (Kuwait Law No. 63 of 2015 on Combating Cyber Crimes) prescribed severe penalties for the unauthorised alteration or acquisition of personal or official data or information.

CITRA introduced Decision No. 42 of 2021 on DPPR (DPR), which imposed obligations in relation to data protection on TSPs and related industry sectors who collect, process or store personal data, in whole or in part.

4.7 How closely it follows GDPR

Similar to the GDPR, Kuwait's DPPR is also seen as such a step forward when it comes to privacy legislation standards, although it is less developed than GDPR.

4.8 Particularly sensitive data

The DCP, which was released by CITRA, can be used as advice for data protection by organisations working with vast amounts of data. Public data, private non sensitive data, private sensitive data and very sensitive data are all defined in the DCP. Examples of private sensitive data include, but are not restricted to:

1. Meeting minutes and business strategies
2. Reports on internal projects
3. The court's rulings and orders, along with any associated papers, preliminary and final court orders, and litigation files
4. Legal office-issued notes and opinions
5. Health reports
6. Deoxyribonucleic acid (DNA) fingerprints from criminal activity.

4.9 Scope

The DPPR imposes legal requirements on Communications and Information Technology Service Providers and organisations that gather and use a natural person's personal data through a variety of channels, including as websites, applications, and other platforms. TSPs and allied industry sectors that collect, handle, or retain personal data, in whole or in part, are subject to requirements connected to data protection under the DPPR by CITRA. The DPR outlines the requirements for gathering and

holding onto personal data, as well as the obligations of a service provider while they provide the service or after it's been provided.

4.10 External auditor/s required

Kuwait's data protection legislation doesn't specifically mandate the involvement of external auditors for enforcement. The DPPR effectively gives CITRA unrestricted physical audit access to any data controller, processor and third party, both inside and outside Kuwait. Recommendations for CITRA to implement process safeguards have been made to enable companies to invest in Kuwait with confidence.

4.11 Child protection data

For children under the age of 18, service providers must get their guardian's express approval before collecting or processing the child's data. The law also requires CITRA to have a process in place to seek the approval of the child's guardian and service providers to make "acceptable efforts" and use "available technologies" to verify the age of the minor.

4.12 Data protection law published in English

The laws of the state of Kuwait have official English translations published by the Kuwaiti government.

5. OMAN

Oman, a country located on the south eastern coast of the Arabian Peninsula, has recognised the importance of protecting personal data and has implemented data protection regulations to safeguard people's privacy. The main legislation governing data protection in Oman is the Data Protection Law, which was enacted in 2022.

The law aims to regulate the processing of personal data and make sure people's rights are respected and their information handled securely. It sets out principles for data controllers and processors, such as the need to

obtain consent for data processing, implementing appropriate security measures and ensuring data accuracy.

The law also establishes the Information Technology Authority (ITA) as the regulatory authority responsible for enforcing compliance and overseeing data protection practices in Oman.

5.1 Definitions of personally identifiable data

Personally identifiable data is data that, whether directly or indirectly, allows someone to be identified based on one or multiple identifiers like their name, ID number, electronic information, location data or through factors related to genetics, physicality, mental state, psychology, social background, culture or economic status.

5.2 Sharing of data between other countries

The most significant fine for breaking data protection legislation is up to OMR 500,000 for the unlawful transfer of personal data outside of Oman [11]. The Oman PDPL applies to businesses registered in Oman or business that provide products and/or services to Omani residents. It broadly follows the same territorial principle as other data protection laws [12].

5.3 Enforcement

The Ministry of Transport, Communication and Information Technology (MTCIT) can punish individuals and entities with a fine from 500 OMR up to 200,000 OMR based on the violations committed under the law.

5.4 Breach notification

If there is a personal data breach resulting in the destruction, modification, disclosure, unauthorised access or unlawful processing of data, the responsible entity (controller) is required to notify both the Ministry and the data owner regarding the breach. This notification should adhere to the regulations and follow the established controls and procedures.

5.5 Online privacy

Processing of personal data should only take place within the principles of transparency, integrity, and respect for human dignity. Additionally,

explicit consent from the data owner is necessary before processing their personal data.

The request to process personal data must be provided in clearly and explicitly in writing, and in a way that's easily understood. The controller is responsible for providing evidence of written consent from the data owner as a prerequisite for processing their data.

Online identifiers are considered personal data [13].

5.6 Timeline

The ***Royal Decree 6/2022*** law was announced on 9 February 2022, and was effective on 9 February 2023.

5.7 How closely it follows GDPR

Oman's PDPL aligns to requirements prescribed by the EU's GDPR. For instance it is based on an opt-in principle. However, there are nuances between both sets of legislation.

5.8 Particularly sensitive data

Sensitive personal data refers to information concerning a natural person's ethnic origin, health status, physical or mental health conditions, religious beliefs, personal relationships or criminal history. These categories of information are regarded as sensitive because of their potential impact on people's privacy and rights.

5.9 Scope

This law applies to various aspects of handling personal data, including the receipt, collection, extraction and processing of such data. These activities can be carried out through traditional (conventional) or electronic methods.

5.10 External auditor/s required

As per the request of the MTCIT, both the controller and the processor have a duty to appoint an external auditor. Their role is to verify that the processing of personal data has been conducted in compliance with the regulations outlined in this law, as well as the procedures and controls specified by the controller in Article (13) of the law.

The regulations also define the specific controls and procedures for the selection and appointment of the external auditor.

5.11 Child protection data

According to Article (6) of the law, it's prohibited to process personal data of a child without the consent of their guardian, unless such processing is deemed to be in the best interest of the child. This processing must be carried out in accordance with the controls and procedures specified by the regulations.

This provision emphasises the importance of having the guardian's consent and prioritising the wellbeing and best interests of the child when processing their personal data.

5.12 Data protection law in English

The Personal Data Protection Law can be found in the English language.

6. QATAR

Qatar has put into effect Law No. (13) of 2016 Concerning Personal Data Protection (referred to as the Data Protection Law). Within the GCC, Qatar was an early implementer of a widely applicable data protection law.

The National Cyber Governance and Assurance Affairs (NCGAA) of the National Cyber Security Agency has developed a set of regulatory guidelines to augment the Data Protection Law. The recommendations aim to clarify requirements under the Data Protection Law and solve issues that are not covered by it by using concepts from EU privacy regulatory frameworks.

When personal information is any of the following, the Data Protection Law applies to data that is processed in one of these ways: electronically; obtained, collected, or extracted in any other way in advance of being processed electronically; and processed by fusing electronic and

conventional processing. According to the Data Protection Law, everyone has the right to the privacy of their personal information. Such data may only be processed in line with the terms of the Data Protection Law, in a way that is open, truthful, and respectful of human dignity [5].

6.1 Definitions of personally identifiable data

Personal data is information about somebody whose identity can be determined or can fairly be determined from the information, either alone or when combined with additional information. Additionally, Qatar has outlined what constitutes as critical personal data.

6.2 Sharing of data between other countries

The responsible authority may decide to process some personal data without adhering to the requirements of Articles (4), (9), (15), and (17) of this legislation if it means protecting the state's international relations, according to Chapter 5: Exemptions, Article 18. 6.3 Enforcement

The NCGAA has the authority to punish individuals and entities with a fine of up to US$1.4m for breaking the Data Protection Law.

6.4 Breach notification

The data controller should notify the NCGAA and the data subject as soon as feasible after becoming aware of the breach, but no later than 72 hours after that.

6.5 Online privacy

Data controllers must make sure they have a privacy notice in place to inform data subjects that they’re processing personal data with regard to online privacy. The handling of children's personal information online is expressly governed by the Data Protection Law.

6.6 Timeline

Law No. (13) of 2016 Concerning the Protection of Personal Data (often known as the Data Protection Law) is in effect in Qatar. Qatar issued a

widely applicable data protection law with the adoption of its Data Protection Law in 2016.

6.8 Particularly sensitive data

Personal information about a natural person's ethnic origin, health, physical or mental health or condition, religious beliefs, relationships, and criminal history is considered sensitive personal data.

6.9 Scope

In 2016, Qatar took a significant step in data protection by implementing its Data Protection Law.

To complement the Data Protection Law, the NCGAA of the National Cyber Security Agency issued a set of regulatory guidelines. These guidelines draw on concepts from the European Union's privacy regulatory frameworks and serve two main purposes. Firstly, they aim to provide clarity on the obligations outlined in the Data Protection Law. Secondly, they address specific matters that might not have been covered in detail within the main legislation.

By introducing these guidelines, the Qatari government offers a mechanism for individuals and entities subject to the Data Protection Law to better understand their responsibilities under the law.

The Data Protection Law is applicable to personal data under the following circumstances:

1. When the data is subjected to electronic processing.
2. When the data is obtained, collected, or extracted in any other manner with the intention of electronic processing.
3. When the data undergoes processing involving a combination of electronic and traditional methods.

According to the Data Protection Law, everyone has the right to privacy when it comes to their personal data. The processing of such data is only allowed within a framework that upholds principles of transparency, honesty, respect for human dignity, and strict adherence to the provisions set forth in the Data Protection Law.

6.10 External auditor/s required

N/A

6.11 Child protection data

The handling of children's personal information online is expressly governed by the Data Protection Law.

6.12 Data Protection laq published in English

The laws of the State of Qatar are not published in official English translations by the Qatari government.

7. KINGDOM OF SAUDI ARABIA

The Personal Data Protection Law (PDPL) is Saudi Arabia’s first comprehensive data protection law that aims to protect people’s privacy by regulating the collection, processing, disclosure and retention of personal data. PDPL was implemented by Royal Decree M/19 of 16 September 2021 and came into force on 23rd of March 2022.

7.1 Definitions of personally identifiable data

Any information, regardless of its form, that can be used to directly or indirectly identify a living or deceased person. This includes the person's name, identification number, contact information, photographs and video recordings. Personal data also includes digital identifiers like IP addresses, usernames and location data such as GPS coordinates [7].

7.2 Sharing of data between other countries

Personal data must be stored and processed within the geographical borders of the Kingdom to preserve national sovereignty and protect data subjects' privacy. Data may only be transferred outside the Kingdom under certain circumstances, such as if the external processor is located in a

country on the accreditation list or if an adequate level of protection is guaranteed.
If adequate protection isn't available, appropriate guarantees must be put in place to protect data subjects' rights. In exceptional cases, a statutory exception may be relied on for data transfer [8].

7.3 Enforcement

The Saudi Data & Artificial Intelligence Authority (SDAIA) will supervise the implementation of the new legislation for the first two years, following which a transfer of supervision to the National Data Management Office (NDMO) will be considered [6].

7.4 Breach notification

The Data Controller must notify both the Competent Authority and the Data Subject in accordance with the Regulations. The Competent Authority must be informed as soon as the Controller becomes aware of any breach, damage, or illegal access to personal data.
The Data Subject must also be informed if the breach, damage, or illegal access to their personal data could cause damage to their data or prejudice their rights and interests [7].

7.5 Timeline

The Personal Data Protection Law (PDPL) aims to protect people's privacy by regulating the collection, processing, disclosure, and retention of personal data. PDPL was implemented by Royal Decree M/19 of 16 September 2021 and came into force on 23 March 2022 [6].

7.7 How closely it follows GDPR

Compared to other similar laws, the PDPL (Personal Data Protection Law) implements a more rigorous approach to data sovereignty. This means that controllers are prohibited from transferring personal data outside of Saudi Arabia, unless it's necessary to comply with an agreement in which the Kingdom is involved.

• The PDPL also covers the data of deceased individuals, which is not a common feature in other international data protection laws. If the data can lead to the specific identification of the deceased person or their family, it falls under the PDPL's jurisdiction.

• The breach notification provisions of the PDPL are more stringent than many international laws. Companies are required to notify authorities immediately in the event of a breach, rather than being allowed a specified period of time to do so.

7.8 Particularly sensitive data

Some personal data is considered sensitive, as it could cause harm to the individual if leaked or misused. Under the Saudi PDPL, personal data is classified as sensitive if it relates to:

- Ethnic or tribal origin
- Criminal and Security data
- Genetic and health data
- Biometric data
- Religious, intellectual or political beliefs
- Credit data
- Location data
- Any data that indicates an individual’s parents are unknown

7.9 Scope

The Personal Data Protection Law (PDPL) aims to protect personal data. This refers to any information, regardless of its form, that can be used to directly or indirectly identify a living or deceased individual. This includes the person's name, identification number, contact information, photographs and video recordings. Personal data also includes digital identifiers like IP addresses, usernames, and location data such as GPS coordinates [7].

7.10 External auditor/s required

According to PDPL, licences to audit or check Personal Data Processing activities related to the Controller's activity may be granted by the Competent Authority to entities. The Competent Authority has the responsibility to establish the conditions and criteria for granting such licences, as well as the rules that regulate them [7].

7.11 Child protection data

The Personal Data Protection Policy issued by NDMO entitles children and incompetent individuals to all the rights of a data subject. However, these rights will be exercised by their guardian. Additionally, minors have the right to request the destruction of their personal data once they reach the age of majority or when their guardianship expires, if their personal data was collected and processed with their guardian's consent [9].

7.12 Data protection law published in English

The Saudi government issued the official PDPL documentations in both English and Arabic and they're publicly available in the Unified National Platform and on SDAIA's public archive [6,7].

8. UNITED ARAB EMIRATES

The United Arab Emirates (UAE) is a country in West Asia, in the Middle East. Its capital is Abu Dhabi and Dubai is an international hub and its most population-dense city.

8.1 Definitions of personally identifiable data

Personal data is defined as any data relating to an identified natural person, or one who can be identified directly or indirectly by way of linking data. It includes sensitive personal data and biometric data.

8.2 Sharing of data between other countries

The PDPL applies to each controller or processor inside the UAE and for those located outside the UAE who carry out processing activities of data subjects inside the UAE.

8.3 Enforcement

The enforcement of privacy laws in the UAE can be carried out through various methods:

1. Breach of the penal code: If an unauthorised disclosure of personal data leads to a breach of the penal code, the case may be transferred to the Criminal Courts of First Instance. The data subject can attach a civil claim to the criminal proceedings. Penalties can include fines and imprisonment.
2. Breach of the New Cyber Crime Law: Breaches are handled by specialised cybercrime units within the police in each Emirate. Jurisdiction is determined based on where the offender lives or where the disclosure took place. The cybercrime unit investigates the case and may refer it to the Public Prosecutor. Penalties under the Cyber Crime Law may involve imprisonment and fines.
3. A breach of the Central Bank's Consumer Protection Regulation or SVF Regulation: The Central Bank can impose administrative penalties, such as fines or restrictions on the powers of Senior Management or Members of the Board, against licensed financial institutions and SVF licensees.
4. A breach of telecoms law and policies: The Telecoms Regulatory Authority (TDRA) oversees the enforcement of the Telecoms Law. If there is a breach, the TDRA may collaborate with the police and Public Prosecutor in the Emirate where the breach took place or where the offender lives. Subscribers or data subjects generally need to file a complaint with the service provider, and within three months. They can submit a complaint to the TDRA, which may direct the service provider to take appropriate remedies to address the complaint

These are the potential methods of enforcement for privacy breaches under UAE law, each with its own specific jurisdiction and penalties.

8.4 Breach notification

Article 9 of the PDPL mandates that controllers must promptly report any infringement or breach of personal data that jeopardises the privacy, confidentiality and security of data. The report should include the details of the breach and the findings of the investigation. The specific timeframe, procedures, and conditions for reporting will be determined by the executive regulations, which have not been published as of now.

8.5 Online privacy

The UAE's Personal Data Protection Law (PDPL) doesn't specifically address online privacy, but it does apply to the processing of personal data online. While the UAE Criminal Law doesn't have explicit provisions related to the internet, its broad provisions on privacy can potentially apply to online matters.

As mentioned in the section on collection and processing, online privacy can be protected through various provisions of the Cyber Crime Law, such as Articles 2, 3, 4, 6, 7, 8, and 45. These laws address unlawful access to financial information, such as credit cards and bank accounts, without permission through the internet or electronic devices. The TDRA's Consumer Protection Regulation also plays a role in safeguarding online privacy.

In summary, while there may not be specific legislation solely dedicated to online privacy in the UAE, the PDPL, Cyber Crime Law, and Consumer Protection Regulation offer some level of protection and address certain aspects of privacy in the online realm.

8.6 Timeline

Protection of Personal Data Protection (PDPL), which was issued on 26 September 2021 and came into effect on 2nd January 2022.

8.7 Particularly sensitive data

Sensitive personal data is defined as any data that directly or indirectly reveals a person's family, racial origin, political or philosophical opinions, religious beliefs, criminal records, biometric data and health status related data.

8.8 Scope

The law applies to the processing or sharing of personal data, in full or part through electronic systems, inside or outside the country. It defines controls to secure and maintain data confidentiality and privacy and gives the owner of the data the rights to consent, correct and retract data.

8.10 Child protection data

Article 29 of Federal Law No. 3 of 2016 Concerning Child Rights, also known as Wadeema's Law, is responsible for Protection of children's data online Law No. 26 of 2015 on the Organization of Dubai Data Publication and Sharing, aims to protect the data and privacy of individuals, including children.

8.11 Data protection law published in English

9. Conclusion and recommendations

In this paper a comparative analysis of privacy legislations across the GCC countries reveals slight variations in key aspects such as definitions of personally identifiable data, sharing of data between other countries, enforcement mechanisms, breach notification requirements, online privacy regulations and timelines of implementation.

GCC countries have been working towards harmonising their privacy regulations and aligning them with international standards to make it easier for businesses and individuals operating in the region to stay compliant.

7. References

[1] https://www.dlapiperdataprotection.com/index.html?t=law&c=BH&c2=

[2] https://www.dlapiperdataprotection.com/index.html?t=law&c=KW

[3] https://citra.gov.kw/sites/en/LegalReferences/Data_Classification.pdf

[4] https://www.citra.gov.kw/sites/en/LegalReferences/Data_Privacy_Protection _Regulation.pdf

[5] https://www.dlapiperdataprotection.com/index.html?t=law&c=QA

[6] The Artificial Intelligence Act (https://artificialintelligenceact.eu/)

[7] Saudi Arabia's Privacy and Data Protection Law on GOV.SA https://www.my.gov.sa/wps/portal/snp/content/dataprotection

[8] Saudi Arabia's National Data Governance Policies: Transfer of Personal Data outside the Geographical Borders of the Kingdom https://sdaia.gov.sa/ar/SDAIA/about/Documents/General%20Rules%20for%20the%20Transfer%20of%20Personal%20Data%20outside%20the%20Geographical%20Borders%20of%20the%20Kingdom.pdf

[9] Saudi Arabia's National Data Governance Policies: Children and Incompetents' Data Protection Policy https://sdaia.gov.sa/ar/SDAIA/about/Documents/Children%20and%20Incompetents'%20Data%20Protection%20Policy.pdf

[10] http://www.pdp.gov.bh/en/assets/pdf/regulations.pdf

[11] https://www.addleshawgoddard.com/en/insights/insights-briefings/2022/data-protection/oman-data-protection-law-2022/#:~:text=There%20are%20various%20fines%20set,personal%20data%20outside%20of%20Oman.

[12] https://secureprivacy.ai/blog/oman-data-protection-law#:~:text=The%20Oman%20Personal%20Data%20Protection,there%20is%20another%20legal%20basis.

[13] https://www.pwc.com/m1/en/services/consulting/documents/oman-data-privacy-handbook.pdf

The UK-Gulf Women in Cybersecurity Fellowship programme is being delivered by Plexal and Protection Group International (PGI) for the Foreign, Commonwealth & Development Office (FCDO) for cyber security professionals throughout the Gulf Cooperation Council (GCC).

The Fellowship empowers women by giving them networking opportunities and access to guest speakers from the UK and the GCC to help them build their careers, grow in confidence and learn about the latest trends, challenges and technologies affecting the sector. Breaking up into project groups, the fellows practice hands-on skills and create solutions to the big challenges facing cyber. This report is the output of one of these groups.

Learn more about the programme
https://www.plexal.com/our-work/ukgulfwic/

Foreign, Commonwealth & Development Office

plexal

PGI

#UKGULFWIC