PERSPECTIVES

APRIL 2020

MANAGING PRIVACY RISKS:

An overview of the new
Bahrain Personal Data Protection Law

Author:
Anestis Dimopoulos
Risk Manager, Information Security & Privacy, Trust Re.

Contents

Introduction

Protecting personal data and the right to privacy are topics which are ever more present in the news, raising multiple questions on how to share and collect personal data and process it securely. Almost all types of organisations are increasingly digitised, thus increasing the focus on how personal data is collected electronically. Without collecting this data, a number of business activities cannot be completed (e.g. employee recruitment, customised user experience in mobile apps).

Globally, there is a trend towards increased regulation for the secure processing of personal data, in multiple jurisdictions. The introduction of the European Union's General Data Protection Regulation (EU GDPR) almost two years ago has been a major game changer for organisations across the world (although relevant EU directives and laws were in place before). Similar regulations have been introduced in many countries in Africa and Asia, as well as the USA.

On 1st August 2018, Bahrain's new relevant law (Personal Data Protection Law [PDPL] No.30 of 2018) came into force, making it one of the first laws in the Gulf Cooperation Council (GCC) region to address protection of personal data.

In light of these developments, Trust Re is pleased to publish this article which discusses key data protection concepts and the global regulatory landscape, Bahrain's new PDPL requirements, an overview of data privacy risks, as well as risk mitigation measures.

Key Concepts: Privacy or Data Protection?

The terms data protection or data privacy are usually utilised globally to refer to the protection of personal data.

Privacy

- Defined as the right to respect for a person's private and family life, his/her home and correspondence.
- Described by the IAPP glossary[1] as a philosophical, legal, social and technological concept which means different things to different observers.
- In an influential 1890 Harvard Law Review article, Samuel Warren and Louis Brandeis, who later became a Supreme Court Judge, famously defined privacy as "a right to be let alone."

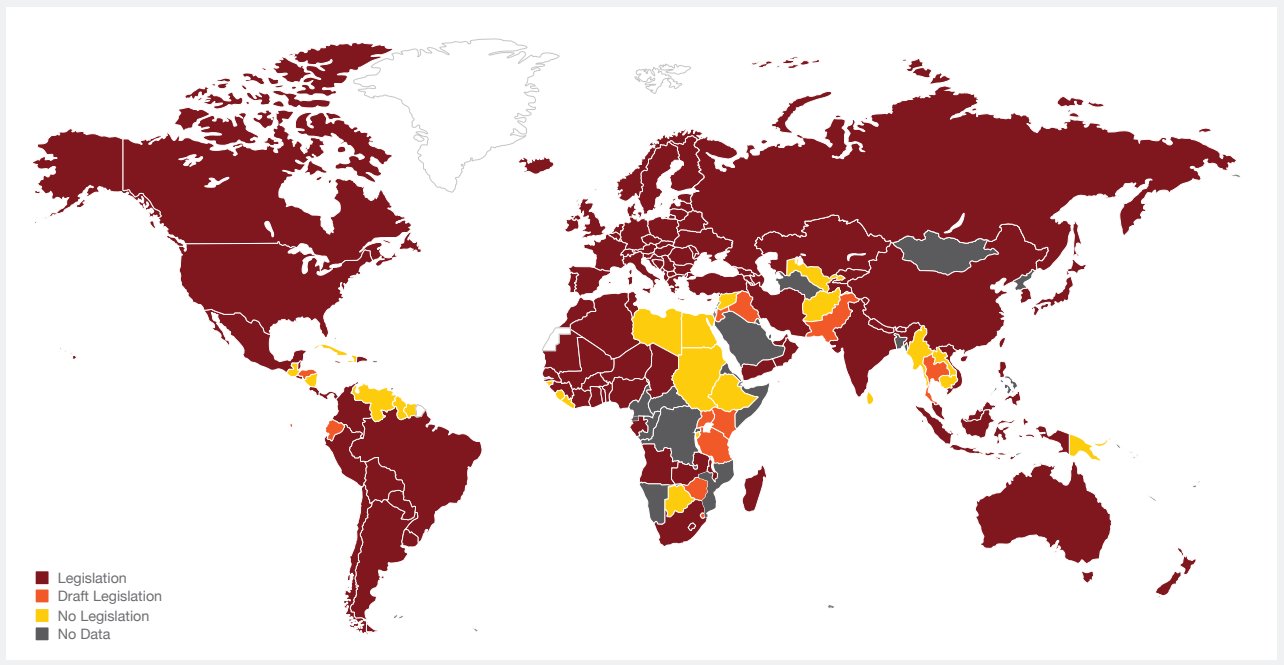
Data Protection

- Defined as the rules and safeguards applying under various laws and regulations to personal data about individuals that organisations collect, store, use and disclose.
- "Data protection" is the professional term used in the EU, whereas in the USA the concept is generally referred to as "information privacy."
- Data protection is different from data security, since it extends beyond securing information to devising and implementing policies for its fair use.

[1] International Association of Privacy Professionals (IAPP) Glossary (https://iapp.org/resources/glossary/)

The Global Landscape

Personal data protection laws and regulations are either present or are currently being drafted in many countries across the globe.



Data Protection and Privacy Legislation Worldwide (Source: UNCTAD,18/02/2020)

Europe

References to privacy were included in the Universal Declaration of Human Rights (UHDR, 1948), and a first effort for the protection of privacy was published from OECD in 1980. Further to that, the EU introduced its relevant Data Protection Directive in 1995, which evolved to the EU GDPR and came into effect on 25th May 2018.

Its objective is to harmonise and enhance the data protection regulatory framework across the EU.

GDPR Key Areas	Penalties For Breach
New consent requirements	Maximum fine of up to €20 million, or 4% of annual global turnover, whichever is higher. *applies regardless of the location of the company processing the data, whether in the EU or not.
Right to access	
The right to be forgotten	
Data portability	
Transfer of data to third countries	
Mandatory breach notifications	
Privacy by design	

[2] United Nations Conference on Trade and Development, Data Protection and Privacy Legislation Worldwide, 18/02/2020) (https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx)

Asia

In Asia, the APEC Cross-Border Privacy Rules ("APEC CBPR") system was endorsed in 2011 as a development of the APEC Privacy Framework having an aim of alleviating these concerns. It is a voluntary, principles-based privacy code of conduct for data controllers in participating APEC member economies, based on the nine APEC Privacy Principles developed in the APEC Privacy Framework.

China	PRC Cybersecurity Law came into effect in 2017. It was the first national-level law to address cybersecurity and data privacy protection.
India	Personal Data Protection Bill was formulated in 2019, further to Information Technology Act of 2000, which included provisions for the protection of personal data.
Singapore	Enacted the Personal Data Protection Act in 2012.
Taiwan	The Personal Data Protection Law became effective in 2012 and was further amended in 2016.
Thailand	On 28th May 2019, the Personal Data Protection Act ("PDPA") became law with a one-year grace period for implementation.

Africa

In Africa, a number of countries have launched personal data protection laws and regulations including:

Morocco	Data Protection Law of 2009
South Africa	Protection of Personal Information Act 4 of 2013
Madagascar	Law No. 2014-038
Uganda	Data Protection and Privacy Act, 2019

Americas

USA	USA has a number of industry-specific (e.g. financial services, telecommunications) and topic-specific laws (e.g. personal health information, information about children, direct marketing) at a national level. The most recent one is the California Consumer Privacy Act of 2018 (CCPA), effective 1st January 2020.
Latin America	• Brazil (General Data Protection Law 2018) • Chile • Colombia.
Canada	• Personal Information Protection and Electronic Documents Act (PIPEDA).

Overall, the developments in the international legal and regulatory environment indicate a trend for more regulation and alignment, which will facilitate cross-border exchange of data, support the digital economy and protect the rights of the personal data subjects.

Overview of Bahrain PDPL key requirements

PDPL 2018 of the Kingdom of Bahrain was introduced as part of the country's continued efforts to enhance its investment ecosystem, together with other relevant laws, such as the Cloud Computing Services to Foreign Parties Law, and Competition Law. The Law was published on 19th July 2018, and came into effect on 1st August 2019. Its objective is to support the development of the digital economy, promote efficient and secure processing of big data and provide guidelines for the effective transfer of data across borders.

Defining Personal Data

PDPL uses a personal data definition very close to EU GDPR. It defines Personal Data as any information of any form related to an identifiable individual, or an individual who can be identified, directly or indirectly, particularly through his/her personal ID number, or one or more of his/her physical, physiological, intellectual, cultural or economic characteristics or social identity. Examples include name, CPR number, passport number, date of birth, address, phone number, etc.

Sensitive Personal Data

In addition, it defines Sensitive Personal Data as any personal information that reveals, directly or indirectly, the individual's race, ethnicity, political or philosophical views, religious beliefs, union affiliation, criminal record or any data related to his/her health or sexual life.

Furthermore, processing of personal data is defined with a wide scope, including any activity of the data lifecycle - any operation or set of operations carried out on personal data by automated or non-automated means, such as collecting, recording, organising, classifying in groups, storing, modifying, amending, retrieving, using or revealing such data by broadcasting, publishing, transmitting, making them available to others, integrating, blocking, deleting or destroying them.

The Law describes a number of data protection principles that need to be adhered to throughout the processing activities of personal data, including:

- Processing shall be fair and legitimate
- Collected for a legitimate, specific and clear purpose and no subsequent processing shall be carried out thereto in a way that is inconsistent with the purpose of collection
- Sufficient, relevant and not excessive for the purpose of collection
- Correct and accurate, and subject to updates whenever necessary
- Shall not remain in a form allowing the identification of the Data Owner after meeting the purpose of collection thereof or the purpose for which subsequent processing is carried out

For the processing of personal data to be legitimate, the consent of the owner is required, with specific exceptions (e.g. implementation of a contract, implementation of an obligation prescribed by the law, protection of the vital interests of the data owner). Especially for sensitive personal data, this needs to be previously authorised by the Data Protection Authority, which as of today, is pending establishment (currently the Ministry of Justice, Islamic Affairs and Awqaf assume the responsibility of the duties and powers for the Authority).

This new law provides new rights to individuals and introduces a number of obligations for organisations in Bahrain that process personal data.

Rights of Individuals
Receive adequate information upon provision of personal data
Inquire whether a business is processing his/her personal data
Right to Object to Direct Marketing
The Right to Object to Processing
The Right to Object to Decisions Made Based on Automated Processing
The Right to Demand Rectification, Blocking or Erasure
Submit a complaint to the Data Protection Authority

Obligations for Organisations
Obtain the consent of the data owner for processing their personal data
Implement technical and organisational measures capable of protecting the data against unintentional or unauthorised destruction, accidental loss, unauthorised alteration, disclosure or access, or any other form of processing
Prohibited from disclosing any personal data except with approval from the Data Owner
Do not transfer personal data outside the Kingdom, unless it is an approved country or there is authorisation from the Authority
Ensure that sensitive personal data, biometric, genetic and visual recording are processed only after obtaining authorisation from the Authority
Notify the Authority and the data owner in case of a data breach

Challenges and risks

Implementing PDPL obliges organisations to take a number of actions and record them. Depending on the nature of the activities of the organisation, its size, as well as the level of international business and transactions, the effort and the skills required may vary significantly. Companies usually form multidisciplinary teams during their compliance journey, including employees from IT, Legal, Compliance, Risk Management, HR, as well as from functions dealing with sensitive personal data. The challenges of such projects include:

- **Change of culture** – as PDPL introduces a relatively new concept in data management activities in the Kingdom, it requires a change in mindset, practices, behaviours and readiness. Awareness and training activities are usually a crucial part of such programmes.
- **Identifying personal data** – depending on the size of the organisation, this may require significant effort to identify such data, understand data flows and conduct data mapping, and implement the necessary measures for data protection (both for electronic and physical records).
- **Privacy Notices and Consent** – At the points of collection of personal data, relevant privacy notices and consent forms need to be designed and implemented. This requires a certain legal approach, but also adequate information about exactly what data is collected and its purpose.
- **International transfers** – Companies need to analyse potential international transfers of personal data, inbound and outbound, and implement the measures required by the Law. An important challenge relates also to which personal data law to apply, i.e. if an online customer is buying services from a provider in Bahrain, what legal provisions should be followed, GDPR or PDPL?
- **Legal / contractual obligations** – a significant part of such data protection programmes is the review and update of legal agreements or relevant formal documentation (e.g. Master Agreements, SLAs, etc.) The duties and responsibilities of each party needs to be clearly defined.

Processing personal data inherently poses a number of risks for the organisation, which need to be managed effectively, such as:

- **Regulatory Compliance** – risk of non-compliance with the requirements of the law or any further implementation guidelines, which may lead to fines, even potential imprisonment, experience loss of revenue, and high litigation and remediation costs.
- **Reputation** – risk of non-compliance with the Law could result in brand damage, loss of consumer trust, loss of employee trust, and customer erosion.
- **Operational** – risk of data owners imposing data processing restrictions, which may result in restricted operations and process complexity.
- **Data exposure** – risk of a security breach which will expose personal data, leading to reputational risks and potential fines.

Managing privacy risks

In order to effectively manage these privacy risks, organisations need to implement a number of risk responses, customised to their size, type of business, risk profile and applicable regulatory environment. Indicatively, the following measures are usually suggested as a good practice to prevent, mitigate or transfer privacy related risks:

- **Proactive and informed risk management** – Ensure a proven risk management framework is in place to support effective and timely identification and management of risks. The NIST Privacy Framework[3] is recently published, integrating Data Privacy with Cybersecurity, as part of an effective Enterprise Risk Management programme.
- **Cybersecurity** – Ensure personal data, as well as other business data, are properly secured based on their classification and protection requirements, from cyber threats. Personal data breach may lead to significant impact in terms of reputation, regulatory fines, and loss of customer trust. Encryption is a key measure, as well as identity and access management, security monitoring and incident response mechanism.
- **Governance** – Proper governance structures will support the initial implementation and the continuous monitoring and improvement of the data privacy programme, including defined roles and responsibilities, policies and procedures, as well as reporting structures and escalation paths.
- **Awareness** – A training and awareness programme will support the change of culture in the organisation, as well as the effective implementation of a data privacy programme.
- **Cyber insurance** – Although an organisation may take significant proactive measures to protect personal data, the current security paradigm is not whether systems will be breached or not, but rather when this will happen. In such cases, a cyber insurance policy may provide multiple options to effectively mitigate or transfer the impact of such a breach, including:
  - **Data breach incident response costs**, a specialist data breach response team, ready to assist
  - **Data restoration**, including costs to engage a service provider to attempt to restore your electronic data following a network security breach
  - **Network security**, privacy and data breach liability, including damages and legal costs associated with investigation and defence of third party claims
  - **Regulatory liability**, covering legal fees or fines and penalties
  - **Business interruption**, such as lost profits, continuing normal operating expenses
  - **Cyber extortion**, including e.g. in case of a ransomware attack, the cost of the expenses charged by professionals to deal/negotiate with attacker, money paid to meet extortion demands, the cost of hiring computer security experts, and to prevent future extortion attempt
  - **Technology liability**, including Legal fees incurred in the investigation or defence of a claim, or damages that a company becomes liable for, due to a negligent act, error, or omission
  - **Media Liability**, covering for wrongful acts when releasing content on website and social media
  - **Social engineering**, covering financial loss or goods, following social engineering fraud

[3] NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management, NIST January 16, 2020 (https://www.nist.gov/system/files/documents/2020/01/16/NIST%20Privacy%20Framework_V1.0.pdf)

Conclusion

As we have seen in this article, our increasingly digitised world has led to the need to protect personal data. As digitisation expands further still, so will the need for greater risk awareness and mitigation. With proper measures in place, businesses and organisations are more likely to gain the trust of consumers and avoid paying harsh penalties handed out for breaching regulations, such as Bahrain's PDPL.

At the same time, even if organisations are compliant with regulatory laws governing the processing of personal data, cyber incidents can occur. This is where cyber insurance can help mitigate against the potential for loss. Insurance and reinsurance companies which can keep up to date with technology developments and propose solutions that meet the needs of increasingly digitised and connected customers, are set to thrive.

Title: Managing Privacy Risks: An overview of the new Bahrain Personal Data Protection Law
Author: Anestis Dimopoulos, Risk Manager, Information Security & Privacy, Trust Re
Editor: Sally Meikle, Communication Specialist, Trust Re.