Freshfields Bruckhaus Deringer

Performing a Check-Up on Your Global Privacy Compliance Program: Overview of Global Trends and Developments in Privacy Laws
(February 2022)

Companies operating globally need a privacy compliance program that spans the jurisdictions where they operate, providing a centralized governance structure built to accommodate common elements of data protection laws and the flexibility to adapt locally as needed. Below, we provide an overview of global trends and developments in privacy laws across four regions—the Americas, Asia Pacific, the Middle East, and Africa—reflecting key areas requiring attention in global privacy compliance programs.

The Americas

1. Regional Overview

We have examined a sampling of thirteen jurisdictions in the region: Argentina, Bermuda, the Bahamas, Bolivia, Canada, Colombia, Costa Rica, the Dominican Republic, Ecuador, Mexico, Panama, Trinidad & Tobago and Uruguay. In recent years, these jurisdictions have developed comprehensive privacy laws. As a general trend, various recent and upcoming legislative changes are bringing these data protection regimes closer to the EU's strict GDPR standards.

Opt-in consent. All of these jurisdictions require opt-in consent in at least some cases to use personal data (e.g. for direct marketing).

Restrictions on sending personal data abroad. These jurisdictions typically have some level of restriction on international transfer. This generally entails that transfer is permitted to a foreign jurisdiction provided that the foreign jurisdiction is deemed to provide an adequate level of personal data protection. Where this is not the case, any transfer must generally be approved by the relevant regulator or requires appropriate contractual safeguards to be implemented.

Mandatory data breach notification requirements. These jurisdictions vary with respect to mandatory data breach notification requirements to either the regulator and/or individuals affected. The timing of the notification, as well as the threshold at which a notification is required also vary. This means that the approach to data breach notifications is not consistent in the region.

"Sensitive" data. The majority of these jurisdictions have stricter rules for "sensitive" data (e.g. health data). These jurisdictions with stricter rules in place generally require that sensitive data is only processed when particular requirements are met.

Fines. The jurisdictions vary with respect to the level of fines. Some of the jurisdictions have material fines that may be in excess of $100,000, whereas others do not. A number of the jurisdictions define the cap on the fines with reference to the minimum wage. Where the minimum wage changes, this may therefore lead to a corresponding material change in the cap on fines.

Regulator. The jurisdictions generally have active data protection authorities, with the notable exceptions being Ecuador, where the sanctions regime will come into force in 2023, and Bolivia, which does not have a data protection authority.

Restrictions on profiling and / or automated decisions for personal data. Some of the jurisdictions have a right to not be subject to decisions made on the basis of automated processing. The majority of the regions do not have this right.

2. Recently enacted privacy laws

Across Latin America there has been a move towards implementing more comprehensive data protection regimes, and, in more recent years, an effort to move closer to the measures implemented in the European Union's General Data Protection Regulation (GDPR). There have been new significant data protection regimes, most notably in Brazil (the Brazilian General Data Protection Law (LGPD), and Ecuador (the Organic Law on Data Protection) which aim to bring the data protection regimes broadly into line with the GDPR.

Asia Pacific

1. Regional Overview

We have examined a sampling of 14 jurisdictions in the region: Australia, Indonesia, Japan, Kazakhstan, Kygyzstan, Macao, Malaysia, New Zealand, Pakistan, Singapore, South Korea, Thailand, Turkmenistan, and Uzbekistan. While the data protection legislation in these jurisdictions shares core principles, each jurisdiction has specific rules that differ from each other and those in other regions.

Opt-in consent. Each of these jurisdictions requires opt-in consent in certain cases to use personal data (e.g. for direct marketing).

Restrictions on sending personal data abroad. Each of these jurisdictions has restrictions on sending personal data abroad. The legal bases for cross-border transfers range from requiring an adequate level of protection for personal data, obtaining consent, or satisfying other specific conditions. These other conditions may include obtaining written consent from the data subject or approval from the designated governmental body.

Mandatory data breach notification requirements. Australia, Indonesia, New Zealand, Pakistan, Singapore, South Korea, Thailand and Turkmenistan all have mandatory data breach notification requirements, either to the regulator and/or to individuals affected.

"Sensitive" data. Most of these jurisdictions have stricter rules for "sensitive" data (e.g. health data), such as requiring explicit consent for processing.

Fines. The severity of fines for breach of data protection law varies significantly between jurisdictions. Eight jurisdictions provide for the possibility of fines over $100,000. New Zealand's maximum fine issued to date is currently approximately $80,500. The remaining jurisdictions (Kazakhstan, Kyrgyzstan, Pakistan, Turkmenistan and Uzbekistan) have lower limits for fines (if any).

Regulator. There is evidence of regulators enforcing the local law in a number of these jurisdictions. In addition, Thailand's regulator, the Personal Data Protection Commission, was established on 18 January 2022.

Restrictions on profiling and / or automated decisions for personal data. Macao, Pakistan and Uzbekistan have explicit restrictions on profiling. These jurisdictions provide data subjects with a right not to be subject to a decision based solely on automated processing. In addition, South Korea requires notification where automated profiling or decisions are used. In Australia, there are actions available under other legislation if the automated decision-making results in discrimination.

Rules on localisation for personal data. Pakistan and Uzbekistan have data localisation requirements in place. Pakistan has a requirement that critical personal data shall only be processed on a server or data centre located in Pakistan. Similarly, in Uzbekistan where processing of personal data involves the information of Uzbek citizens, the data must be collected, systematised, and stored using technical means physically located on the territory of Uzbekistan.

2. Recently enacted privacy laws

Japan. The amendment to the Act on the Protection of Personal Information (***APPI***) was enacted on 12 June 2020 and will be in effect on 1 April 2022. The amendment, amongst other things, enhances the rights of data subjects, imposes an obligation to report any personal data leak incident that falls into certain categories, strengthens penalties and imposes a new obligation on international transfer.

Kazakhstan. The Law on Amendments and Additions to Some Legislative Acts of the Republic of Kazakhstan on the Regulation of Digital Technologies was introduced in July 2020. This significantly extended the data protection obligations for organisations. It introduces, among other things, further requirements for data collection and processing, obligations for data operators (similar to data processors), and further establishes the competency of the data protection authority including its powers and role.

New Zealand. The key legislation in New Zealand relating to data protection is the Privacy Act 2020. Certain aspects of this act came into force on 1 July 2020, with most operative provisions commencing from 1 December 2020. The 2020 Act retains the 'principle' based approach from the previous legislation, in contrast to a trend set by the GDPR for more prescriptive data protection requirements.

Pakistan. Whilst Pakistan does not have any extensive data protection legislation in place, there are a number of recently enacted laws which provide a legal framework in this respect. For example, the Removal and Blocking of Unlawful Online Content (Procedure, Oversight and Safeguard) Rules 2020 provide that the Pakistan Telecommunication Authority will have the power to remove, block, or issue directions for the removal or blocking of access to information through any information system if it considers it necessary in relation to, inter alia, incitement of any offence under the Prevention of Electronic Crimes Act 2016.

3. New laws expected in 2022 and beyond

Australia. The Australian Government's Attorney-General's Department is currently undertaking a review of the Privacy Act. The discussion paper was released on 25 October 2021 and the proposals include: (i) redrafting of the definition of "personal information" to include online identifiers and technical data; (ii) an intention to reduce reliance on the "notice and consent" self-management model of privacy regulation; (iii) tightening legal tests for what constitutes a valid

consent; (iv) abolishing the existing rule on direct marketing in favour of applying the same standards as for other activities; and (v) broadening the idea of sensitive information to include restricted acts. Submissions on the discussion paper are due in January 2022.

Indonesia. In January 2020, the Indonesian government introduced a data privacy bill in Parliament which was expected to pass by the end of the year. However, due to the pandemic, this is still being discussed. It is expected that the bill should be passed in the next few months. If enacted in its current form, the proposed law would, among other things, require controllers to process personal data on the basis of consent or on another legal basis, to implement stricter controls for sensitive personal data, to notify individuals and the data protection authority within 72 hours after a data breach occurs, and to provide individuals with access, correction, deletion, and data portability rights. In addition, the proposed law imposes limits on cross border transfers and prohibits the buying and selling of personal data for money.

Malaysia. In February 2020, the Malaysian Department of Personal Data Protection held a public consultation on proposed changes to the Personal Data Protection Act 2010 (the ***PDPA***). The consultation paper sought views and comments from the public on a total of 22 issues including imposition of direct obligation on data processors, right to data portability, reporting of data breach incidents, privacy by design, and processing personal data in cloud computing.

Pakistan. The Ministry of Information Technology and Telecommunications has introduced the Personal Data Protection Bill 2021, which is yet to be promulgated into law. Once enacted, this bill will be the main legislation regulating controllers and processors of personal data in Pakistan and will apply to any person who processes, has control over, or authorises the processing of any personal data, provided that the data subject, data controller or data processor (either local or foreign) is located in Pakistan.

Thailand. The Personal Data Protection Act (***PDPA***) was supposed to be enforced on 27 May 2021. However, due to the Covid-19 pandemic, this has been postponed to 1 June 2022. The PDPA is based on the same lines as the GDPR and aims to protect Thai data owners from illegally collecting, using, and sharing their personal information. The regulator under the PDPA, the Personal Data Protection Commission, was established on 18 January 2022.

Middle East

1. Regional Overview

We have examined five jurisdictions in the region: the Abu Dhabi Global Market, the Dubai IFC, Israel, Morocco, and the Qatar FC. In recent years, these jurisdictions have developed comprehensive privacy laws. As a general trend, various recent and upcoming legislative changes are bringing these data protection regimes closer to the EU's strict GDPR standards.

Opt-in consent. All of the jurisdictions at hand require opt-in consent in certain cases to use personal data (e.g. for direct marketing). In other cases, such as under the Israeli data protection regime, data subject consent may be implied.

Restrictions on sending personal data abroad. These jurisdictions typically have restrictions on sending personal data abroad. These jurisdictions generally allow for the transfer to a recipient in a jurisdiction designated as providing an adequate level of protection for personal data. However,

if this is not the case, personal data may only be transferred outside the jurisdiction on the basis of specific conditions. These may include obtaining written consent from the data subject or obtaining a permit.

Mandatory data breach notification requirements. The Abu Dhabi Global Market, the Dubai IFC and Israel all have mandatory data breach notification requirements, either to the regulator, or to individuals affected. However, the thresholds for notification vary between the jurisdictions, with Israel only requiring notification in case of a "*severe security event*".

"Sensitive" data. All jurisdictions have stricter rules for "sensitive" data (e.g. health data). Most of the jurisdictions prohibit the processing of such data unless certain special conditions are met. For example, whilst Morocco has a specific authorisation procedure for sensitive data, Israel has a general higher standard of security, and requires mandatory registration of databases.

Fines. The severity of fines for breach of data protection law varies significantly between jurisdictions. Two jurisdictions (Abu Dhabi Global Market, and Dubai IFC) have fines over $100,000. Israel's maximum fine is currently $70,000, but legislators are in the process of drafting a significantly higher limit. The remaining jurisdictions (Morocco and Qatar FC) have lower limits for fines (if any).

Regulator. There is evidence of regulators enforcing the local law in most of the jurisdictions at hand. However, the regulator in Morocco tends not to be as active in relation to enforcement.

Restrictions on profiling and / or automated decisions for personal data. Abu Dhabi Global Market and Morocco both have explicit restrictions on profiling. These jurisdictions provide data subjects with a right not to be subject to a decision based solely on automated processing, and in some cases, a right to know the logic behind such a decision.

2. New laws expected in 2022 and beyond

Abu Dhabi Global Market. The Data Protection Regulations 2021 provide for a twelve-month transition period for current establishments, as well as a six-month transition period for new establishments, being enforceable from 14 February 2022 and 14 August 2021 respectively. Up until these dates, the Data Protection Regulations 2015 will continue to apply.

Qatar FC. The Qatar Financial Centre issued on 21 December 2021 the new QFC Data Protection Rules, along with the new Data Protection Regulations 2021. In particular, this legislation adds to controllers' transparency obligations towards data subjects.

Africa – Data Protection Summary

1. Summary

We have examined 24 jurisdictions in the region.[1] The level of data protection in Africa varies significantly from country to country. While some countries have already enacted comprehensive laws, others still lack such laws. In recent years, more and more countries have adopted

[1] The 24 jurisdictions surveyed are Angola, Benin, Burkina Faso, Cape Verde, Chad, Congo, Cote d´Ivoire, Egypt, Equatorial Guinea, Gabon, Ghana, Kenya, Lesotho, Madagascar, Mali, Mauritius, Morocco, Nigeria, Sao Tomé and Príncipe, Senegal, South Africa, Togo, Tunisia, and Uganda.

comprehensive data protection laws. Africa has a rapidly evolving data protection landscape and is region to watch.

Opt-in consent. These jurisdictions typically require opt-in consent to use some or all personal data (e.g., for direct marketing).

Restrictions on sending personal data abroad. These jurisdictions tend to have restrictions on sending personal data abroad. This generally entails that transfer is permitted to a foreign jurisdiction provided that the foreign jurisdiction is deemed to provide an adequate level of data protection. Where this is not the case, the transfer must generally be approved by the relevant regulator or requires additional appropriate contractual safeguards to be put in place.

Mandatory data breach notification requirements. These jurisdictions vary with respect to mandatory data breach notification requirements to either the regulator and/or individuals affected. Just over half of these jurisdictions require some form of mandatory data breach notification. The timing of the notification, and the threshold at which the notification requirement is triggered also vary, which show that the approach to data breach notifications is not consistent in the region. It is striking that nearly half jurisdictions examined have no notification requirement at all.

"Sensitive" data. Most of these jurisdictions have stricter regulations for data classified as "sensitive" (e.g., health data). In most of these jurisdictions, sensitive data can only be processed if additional conditions are met. These conditions range from requiring consent to getting specific authorisations.

Fines. These jurisdictions differ, sometimes significantly, in the severity of fines that can be levied for violations of data protection laws. In most countries, fines are generally limited to under USD 100,000. Several of these countries allow fines above USD 100,000. In several countries, the upper limit of fines that can be imposed is a percentage of the company's turnover.

Regulator. Many countries have a data protection authority that is enforcing local data protection laws. However, nearly half of these jurisdictions do not have a data protection authority, or if they do, the regulator is not yet active.[2]

Restrictions on profiling and / or automated decisions for personal data. In many of these jurisdictions, there are restrictions on profiling and automated decision processes using personal data.

Rules on localisation for personal data. The examined jurisdictions have no express rules on data localisation except for Kenya. Kenya stipulates that health data should not be stored outside Kenyan territory.

2. Recently enacted privacy laws

Angola. Two laws have been published in 2021 that establish the fees to be paid to the Data Protection Authority (APD). Angola has also enacted Law 11/20 of 23 April 2020 on the

[2] Note in the following countries there is no competent authority or at least one is not active: Chad, Kongo, Equatorial Guinea, Kenya, Lesotho, Madagascar, Nigeria, Togo, Tunisia.

identification and location of cell phones and electronic surveillance by police authorities, and Law 2/20 of 22 January 2020 on video surveillance.

Botswana. The Data Protection Act (Act No. 32 of 2018) came into effect on 15 October 2021. There is a 12 month transition period, which will automatically end on 15 October 2022 by which data controllers must comply with the Act.

Burkina Faso. Law No. 001-2021/AN of March 30, 2021 ("the 2021 Law"), repealed and replaced the previous data protection law, which dates back to 2004. The main novelties are the strengthening of the protection of the privacy of individuals, inter alia, by extending the geographical scope to controllers abroad processing data from Burkina Faso (regardless of whether they use local data processing systems), by monitoring cross-border transfers, and by introducing a broader right to information. The 2021 law also tightens security requirements by requiring that when data is transferred to a third country, the data recipient must enter into a contract that includes a data return clause and must encrypt the data.

Congo. Law No. 017/2020 repeals Law No. 013/2002 and regulates the areas of telecommunications and information communication technology. The Law makes reference throughout to the protection of personal data and includes provisions on consent and the processing of sensitive data.

Egypt. Egypt recently introduced the Personal Data Protection Law ("Data Protection Law"), which was issued pursuant to Resolution No. 151 of 2020 on July 13, 2020. The Data Protection Law mirrors the European General Data Protection Regulation (Regulation (EU) 2016/679) ("GDPR"), as it aims to establish various standards and rules that protect the rights of individuals in Egypt with respect to their personal data.

Rwanda. Law NO. 058/2021 Relating to the Protection of Personal Data and Privacy came into effect on 15 October 2021 upon being published in the Rwanda Official Gazette. Data controllers that are already in operation have a two-year transition period to comply with the Act.

Zambia. Zambia has enacted two comprehensive data protection laws. The Data Protection Act No. 3 of 2021 was enacted on 23 March 2021, and the Cyber Security and Cyber Crimes Act No. 2 of 2021 was enacted on 24 March 2021.

Zimbabwe. Zimbabwe has enacted the Data Protection Act No. 05/2021 on 3 December 2021, which is its first comprehensive data protection regime. The act includes provisions on data protection, cybersecurity and cybercrimes. The enactment of the new law follows amendments made to its Cybersecurity and Data Protection Bill.