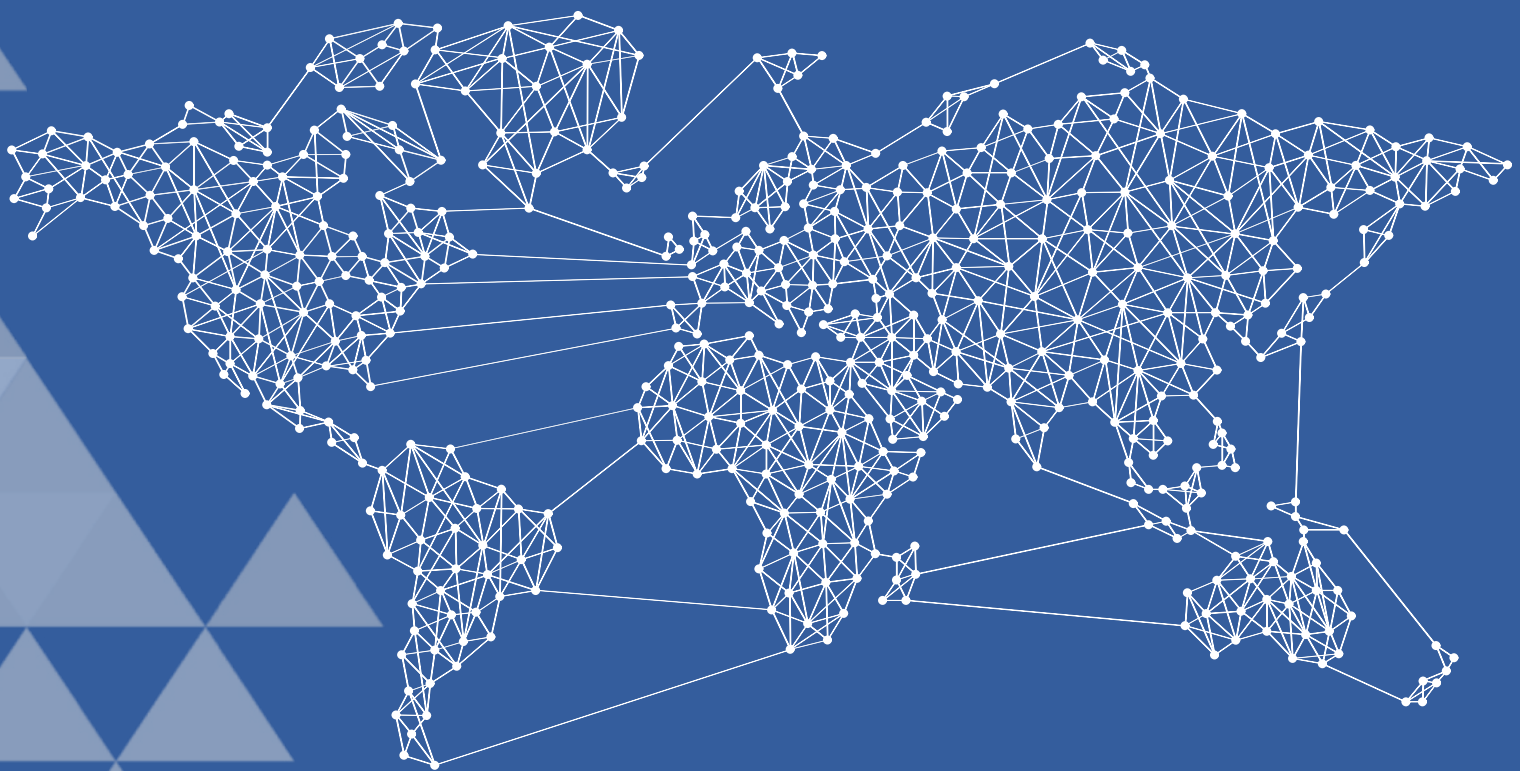


OneTrust DataGuidance Privacy Review Q3 2021



About the report

The third quarter of 2021 saw continual development across all areas of data protection and privacy. Legislative reform can be seen especially in the US and in the EU, with data protection authorities and other regulators alike focusing on international data transfers, cybersecurity, and cookies. In less established regions, such as the Middle East, APAC, and Latin America, jurisdictions also continued to introduce new legislation and guidelines, with China garnering much of the attention for its Personal Information Protection Law. Privacy Analysts at OneTrust DataGuidance survey the most significant developments in the third quarter and identify key areas to monitor in the coming months.

About the authors

OneTrust DataGuidance™

GLOBAL REGULATORY RESEARCH SOFTWARE TO HELP YOU BUILD AND MAINTAIN YOUR COMPLIANCE PROGRAM

OneTrust DataGuidance™ is the industry's most in-depth and up-to-date source of privacy and security research, powered by a contributor network of over 800 lawyers, 40 in-house legal researchers and 14 full-time in-house translators. OneTrust DataGuidance™ offers solutions for your research, planning, benchmarking and training.

OneTrust DataGuidance™ solutions are integrated directly into OneTrust products, enabling organizations to leverage OneTrust to drive compliance with hundreds of global privacy and security laws and frameworks. This approach provides the only solution that gives privacy departments the tools they need to efficiently monitor and manage the complex and changing world of privacy management.

For more information visit dataguidance.com

Contributors

OneTrust DataGuidance™

Angela Potter, Matteo Quartieri, Alexis Kateifides, Iana Gaytandjieva, Edidiong Udoh, Alahi Kazi, Karan Chao, Victoria Ashcroft, Robb Hiscock

Image production credits

Cover page: pop_jop / Signature collection / istockphoto.com

OneTrust DataGuidance Retention Schedules

STAY INFORMED ON CRITICAL RECORD RETENTION PERIODS



Sales & Marketing

Retain documentation on your organization's sales and marketing activities, including customer-related records



Company & Financial

Maintain internal executive information as well as your organization's accounting and tax records



Health & Safety

Know how long to keep audit reports, incident notifications, governmental inspection reports, and hazardous exposure records



Employment

Store records related to recruitment and selection, and know your obligations to the employees of your organizations

Global

Key takeaways:

- China's PIPL enacted
- Saudi Arabia passes data protection law
- Cookie enforcement and regulation
- Deadline to Whistleblowing Directive implementation looming

Saudi Arabia Data Protection Law

Saudi Arabia entered into a new era for data protection with the publication of the Personal Data Protection Law, implemented by Royal Decree M/19 of 17 September 2021 approving Resolution No. 98 dated 14 September 2021 ('PDPL'). In particular, the PDPL brings Saudi Arabia in closer alignment with its regional counterparts and aims to regulate the sharing and ensure the privacy of personal data, and prevent the abuse of the same. Covered entities will have roughly a year to come into compliance with entry into effect on 23 March 2022. However, this date will be delayed for a period of up to five years, and as determined by the Saudi Data & Artificial Intelligence Authority ('SDAIA'), for companies located outside the Kingdom that process the personal data of Saudi Arabian residents. In relation to supervision, the SDAIA will be the primary regulator for the first two years after which the role may be transferred to the National Data Management Office, the regulatory arm of the SDAIA. Some of the PDPL's key features include requirements to register with regulatory authorities, breach notification obligations, requirements to undertake Data Protection Impact Assessments ('DPIAS'), and the provision of data subject rights. Notably, the PDPL provides for stringent penalties for breaches, including imprisonment of up to two years and/or fines of up to SAR 5 million (approx. €1.1 million).

China Personal Information Protection Law

The data protection regime in China has seen a significant shift as the Personal Information Protection Law of the People's Republic of China ('PIPL') was adopted by the National People's Congress of the People's Republic of China ('NPC'). This came only a few months after the Data Security Law ('DSL') was passed and entered into effect on 1 September. Similar to the DSL, the PIPL has a short turn around period, entering into effect on 1 November 2021, only two months after being enacted. Notably, the PIPL was finalised after numerous changes were made from inception to the three drafts debated by the NPC which eventually landed on a law that draws many similarities with the EU's General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR'). More specifically, the PIPL sets out rules for lawful processing, the sharing and disclosure of personal information including sensitive personal information, as well as data controller obligations, data subject rights, and a strict enforcement regime. Although many of the concepts provided for in the PIPL were previously set out in several legal instruments in Chinese laws, the PIPL consolidates and supplements the data protection regime in China. Furthermore, with a short period between enactment and entry into force, organisations will be subject to significant changes specifically in relation to facilitating mechanisms for data subject rights and obligations in relation to data transfers and data localisation. More specifically, the PIPL sets out two categories of companies permitted to store personal information in China: critical information infrastructure operators and large processors. With entry into effect looming, organisations will be keeping a watchful eye on further guidance issued by enforcement and supervisory authorities in the region.

Cookies

Cookie enforcement and regulation continued to be a priority, particularly in Europe with many data protection authorities updating guidance and initiating enforcement proceedings for non-compliance. In particular, the Italian data protection authority ('Garante') published new cookies guidelines on 10 July and set out a six-month compliance deadline. For the most part, the focus of these and other guidelines is to ensure compliance with both the GDPR and Directive on Privacy and Electronic Communications (2002/58/EC) (as amended) ('ePrivacy Directive') especially in relation to what constitutes consent. Likewise, after public consultation, the Finnish Transport and Communications Agency ('TRAFICOM') published its revised cookie guidelines outlining, among other things, the general conditions for the storage and use of cookies, as well as again clarifying the rules regarding consent. In the Czech Republic, the Senate approved the transposition amendment to the Act No. 127/2005 Coll., on electronic communications and on Amendment of Certain Related Acts ('the Electronic Communications Act'), introducing active opt-in consent for the processing of data in relation to cookies and telemarketing. Reform continued in the UK with the Department for Digital, Culture, Media & Sport ('DCMS') announcing the launch of a public consultation on the country's data protection regime with specific changes in the use of cookies. More specifically, the reform would permit organisations to use analytics cookies and similar technologies without the user's consent and extend soft-opt in to permitted organisations in certain situations.

Furthermore, after questions were raised about the territorial application of the ePrivacy Directive, the European Data Protection Board ('EDPB') clarified that in the absence of a provision setting out the scope, the case law of the Court of Justice of the European Union on the territorial application of the repealed Data Protection Directive (Directive 95/46/EC) should give an indication of how the territorial application should be organised.

In enforcement, the EDPB announced that it had set up a task force to coordinate the efforts led by the non-profit group None of your business ('NYOB') in relation to complaints concerning cookies banners filed with several European supervisory authorities. Finally, data protection authorities in Spain and France announced enforcement actions for various cookie violations.

Whistleblowing

With less than three months until the December 2021 deadline, pressure is mounting on EU Member States to transpose the Directive on the Protection of Persons who Report Breaches of Union Law (Directive (EU) 2019/1937) ('the Whistleblowing Directive') into national law. The Network of European Integrity and Whistleblowing Authorities ('NEIWA'), a group of governmental organisations across the EU, adopted a statement in September, calling legislators to do so correctly and in a timely manner. Although there is increased attention on the Whistleblowing Directive, only a few Member States have made progress so far in this quarter. On 11 August 2021, the Ministry of Justice in Estonia launched a draft bill for public consultation, constituting the country's first consolidated whistleblowing law. Thereafter, on 21 September 2021, the Latvian Cabinet of Ministers also published a new draft law which is currently being considered by parliament and set to replace its previous whistleblowing law of 2018. Furthermore, while the Czech Republic was regarded as having made the most progress in this regard, the Committee on Constitutional and Legal Affairs failed to schedule discussions before the national elections, resulting in the jurisdiction unable to meet the transposition deadline.

Beyond the EU, the Dubai Financial Services Authority ('DFSA') released in July its consultation paper on whistleblowing, detailing measures applicable to DFSA-regulated entities, with the aim of achieving a more consistent approach to reporting misconduct. In Japan, the Consumer Affairs Agency ('CAA') also issued whistleblowing guidelines for business operators, particularly in relation to public interest notifications and internal reporting procedures for employees. Finally, the International Organization for Standardization ('ISO') finalised its long-awaited standard, ISO 37002, Whistleblowing management systems – Guidelines. Intended for public and privacy organisations of all sizes; the new standard provides sector-neutral guidance on management systems for whistleblowing.

What to look out for:

- Entry into effect for China's PIPL
- Increased cookie enforcement
- Deadline to transpose Whistleblowing Directive in December

Americas & Caribbean

Key takeaways:

- Colorado Privacy Act enacted
- Panama published data protection law
- CPPA published proposed rulemaking under CPRA
- Regulatory focus on anti-competitive practices
- LGPD enforcement provisions enter into effect

July

The quarter began with Senate Bill ('SB') 21-190 for an Act concerning additional protection of data relating to personal privacy being signed by the Colorado State Governor on 7 July 2021. With the Colorado Privacy Act, the state joins California and Virginia in passing a comprehensive private sector privacy law. Shortly thereafter, New York City Council bill 1170-2018 entered into effect which requires businesses to notify customers of the use of biometric identifier technology and prohibits the sale of the same. The introduction of state comprehensive privacy laws slowed down this quarter however, though Ohio introduced House Bill ('HB') 376 for the Ohio Personal Privacy Act which is still under review. In Wisconsin, the Office of the Commissioner of Insurance announced that the it joined 14 others in enacting the National Association of Insurance Commissioners' ('NAIC') Insurance Data Security Model Law.

Federal privacy legislation developments continued this quarter with Senators reintroducing a bill for the Setting an American Framework to Ensure Data Access, Transparency, and Accountability ('SAFE DATA') Act, although again these bills had no meaningful progression. However, SB 2047 for the Cyber Incident Notification Act of 2021 was introduced and if passed would require critical infrastructure organisations in the US to report security incidents to the Cybersecurity and Infrastructure Security Agency ('CISA') within 24 hours. In addition, an updated version of House Resolution ('HR') 4801 for Protecting the Information of our Vulnerable Children and Youth Act ('the Kids PRIVACY Act'), which would amend the Children's Online Privacy Protection Act of 1998 ('COPPA'), was introduced. Interestingly, the Kids PRIVACY Act takes many of the principles of the UK Information Commissioner's Office ('ICO') Age-Appropriate Design Code.

Notably, the National Conference of Commissioners of Uniform State Laws ('ULC') announced that it had approved the Uniform Personal Data Protection Act ('UPDPA'). The UPDPA could be a starting point for states without comprehensive privacy legislation, although it faced criticism from consumer trade groups like the American Bankers Association ('ABA') for not including exclusions for financial institutions already subject to federal financial privacy legislation.

One year after enforcement officially began under the California Consumer Protection Act of 2018 ('CCPA'), the California Attorney General ('AG') provided an update of its efforts noting that 75% of businesses acted to come into compliance within the 30-day statutory cure period, while the remaining 25% who received a notice of an alleged violation were either within the cure period or are currently being investigated.

Following on from the Supreme Court ruling in *AMG Capital Management v. FTC* last quarter that saw the court strike down one of the Federal Trade Commission's ('FTC') key enforcement tools, the FTC announced that it would rescind its 2015 policy that restrained some of its powers. Specifically, the 2015 anti-trust policy statement constrained the FTC's use of its authority under Section 5 of the FTC Act of 1914 to stop anti-competitive business tactics. This echoed the position of the White House which announced that the U.S. President had signed an Executive Order on Promoting Competition in the American Economy. Additionally, 36 State Attorneys General announced a multistate lawsuit against a company for anticompetitive practices in the smartphone application market. Moreover, legislation continues to be introduced that would expand and reinforce the enforcement powers of the FTC, including HR 2668 for the Consumer Protection and Recovery Act which amends the FTC's Section 13(b) authority, as well as HR 4447 for the 21st Century FTC Act which modifies the FTC's rulemaking authority and first offence civil penalty authority.

Negotiations on a new EU-US Privacy Shield framework were again silent for most of the quarter, however the Information Technology Industry Council ('ITI') published a set of priorities ahead of the US-EU Trade and Technology Council ('TTC') which included commitments to promote international regulatory compatibility.

Legislative reform continued across the region and in Canada, with the Government of Alberta seeking public comments to help identify opportunities to strengthen privacy protection in Alberta, particularly focusing on, among other laws, the Personal Information Protection Act. In Brazil, the Chamber of Deputies progressed with its artificial intelligence ('AI') bill which, among other things, establishes the positions of AI agents and principles, rights, and legal frameworks for the development of AI. Furthermore, as Mexico celebrated 11 years of its data protection law, the National Institute of Transparency, Access to Information and Protection of Personal Data ('INAI') emphasised that advances in technologies have necessitated an update to its legal framework. The INAI reiterated these sentiments in relation to the country's cybersecurity standards. Finally, the President of Panama approved the Executive Decree which regulates Law No. 81 on Personal Data Protection establishing several obligations in relation to the processing of personal data in the country.

Lastly, in enforcement, the FTC entered a \$100,000 settlement with a company for multiple violations of the Children's Online Privacy Protection Act Rule ('the COPPA Rule') and announced a \$1.6 million settlement with a company for illegal robocalls to customers listed on the FTC's Do Not Call Registry.

August

The month began with the entry into effect of the enforcement provisions under Law No. 13.709 of 14 August 2018, General Personal Data Protection Law (as amended by Law No. 13.853 of 8 July 2019) ('LGPD') on 1 August 2021. As such, the Brazilian data protection authority ('ANPD') published a series of frequently asked questions ('FAQs') addressing among other topics: sanctions, fines, or penalties; procedures for how fines will be calculated; and other administrative processes. Further, the Brazilian House of Representatives approved, in the second round, the text of the Constitutional Amendment Proposal PEC No. 17/2019, which

amends the Brazilian Federal Constitution to include the protection of personal data among the fundamental rights and guarantees, as well as to establish the exclusive federal competence to legislate on the protection and processing of personal data. Additionally, Uruguay announced that it had ratified the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data ('Convention 108+').

Cyber defence continued to be a priority at the federal level in the US with the National Institute of Standards and Technology ('NIST') announcing it would be seeking comments on a draft for the development of cyber-resilient systems. Likewise, CISA launched its Joint Cyber Defence Collaborative project in which it aims to lead efforts in the development of cyber-defence operation across the US. In addition, the Cyber Incident Notification Act continued to face legislative obstacles with the ABA and other trade groups raising concerns about the short 72-hour timeline, scope of the incidents, and mechanisms to notify respective agencies.

At the state level, New York's City Council enacted Bill Int 2311-2021 for a Local Law to amend the Administrative Code of the city of New York which outlines obligations for the processing of data on orders placed through third-party food delivery services. Minnesota's House File ('HF') 6 for the Insurance Data Security Act entered into effect on 1 August 2021.

As Canada's adequacy status is due for review every four years, the Office of the Privacy Commissioner of Canada ('OPC') announced that it had updated some of its guidance on its determination of 'sensitive data.' More specifically, the OPC highlighted that its updated guidance aims to better explain the concept of sensitive information under Personal Information Protection and Electronic Documents Act 2000 ('PIPEDA') so it can be evaluated more accurately against the GDPR. In addition, and with the increased risk of cyber attacks in the past year the Office of the Superintendent of Financial Institutions ('OSFI') updated its technology and cyber incident reporting guidance, which now recommends that incidents be reported to Lead Supervisors within 24 hours or sooner or risk increased oversight.

In enforcement in the US, the Financial Crimes Enforcement Network ('FinCEN') announced a \$100 million civil money penalty against a company for violations of the Bank Secrecy Act of 1970. In addition, the Federal Communications Commission ('FCC') proposed a \$5 million fine against a firm for unlawful robocalls without prior consent. In addition, the Securities and Exchange Commission ('SEC') announced fines against eight organisations for deficient cybersecurity procedures. Finally, the New Mexico AG also continued to prioritise children's privacy with the announcement of a lawsuit against a company for illegal collection of children's data.

September

Cyber incident reporting reform continued to be a priority in September in the US with a draft bill for the Cyber Incident Reporting for the Critical Infrastructure Act of 2021 being introduced that would direct certain organisations deemed as critical infrastructure owners and operators to report incidents no earlier than 72 hours to CISA and establish a new federal Cyber Incident Review Office within CISA. In addition, SB 2875 for the Cyber Incident Reporting Act of 2021 was also introduced in the US Congress establishing similar obligations.

Nominations have been finalised for two key privacy positions in the US, including Alvaro Bedoya as the Commissioner of the FTC and Lisa J. Pino as the Director of the Office for Civil Rights ('OCR'). Notably, the FTC has faced continued calls from US lawmakers to strengthen its powers of enforcement in relation to privacy protection and seems to have strong support as the U.S. House Committee on Energy and Commerce announced the approval of a \$1 billion fund to set up a privacy bureau within the FTC.

In terms of legislative reform, Brazil's House of Representatives announced that it had approved its bill for regulating AI, which will now be sent to the Senate for approval. Canada continues to prioritise legal reform both at the provincial and federal level. Particularly, the Yukon Information and Privacy Commissioner ('Yukon IPC') issued 18 recommendations to its health privacy law, which is currently under review. Then in Ontario, the Office of the Information Commissioner of Ontario ('Ontario IPC') published a response to the government's proposal for a private sector privacy law in which it also addressed some gaps in the federal Bill C-11 for the Digital Charter Implementation Act, which now requires reintroduction following the dissolution of Parliament. The Office of the Information and Privacy Commissioner for British Columbia ('OIPC') noted that it is continuing the statutory review of the Personal Information Protection Act, SBC 2003 c 63 ('PIPA'). Finally, Quebec's Bill 64 for An Act to modernise legislative provisions as regards the protection of personal information received royal assent, bringing with it wide sweeping changes to the data protection landscape in Quebec, including data breach reporting obligations, requirements for the appointment of a person responsible for implementing the personal information protection measures, and the requirement to conduct DPIAs.

At the US State law level, Texas' HB 3746 which amends the State's data breach notification law entered into law, establishing new disclosure requirements for organisations when sending breach notifications to affected residents. Generally, comprehensive privacy laws at the State level again slowed down, however Oklahoma introduced HB 2969 for the Oklahoma Computer Data Privacy Act 2022 that would establish a complete legislative framework for data protection within the State. Furthermore, an Appellate Court in Illinois clarified the limitation periods applicable to the State's Biometric Information Privacy Act ('BIPA') which is silent on the issue, noting that either a one or five year period is applicable dependent on the Section that has been violated.

Moreover, the California Privacy Protection Agency Board ('CPPA Board') invited preliminary comments on proposed rulemaking under the California Privacy Rights Act of 2020 ('CPRA'), which will cover topics including automated decision-making, audits, consumer rights matters, and high-risk processing.

The Court of Justice of the European Union's ('CJEU') judgment in *Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems* (C-311/18) ('the Schrems II Case') continued to have a global influence with the Uruguayan data protection authority ('URCDP') announcing that it has excluded the US from appropriate territories for data transfers and provided other mechanisms for such transfers which include contractual clauses and consent of interested parties. Negotiations on a renewed EU-US Privacy Shield did pick up slightly this quarter as preparation began for the inaugural meeting of the TTC, with both territories reaffirming their

willingness to coordinate on a number of issues including data governance and technology, transatlantic trade, and AI. EU and US counterparts also joined Australia in announcing a new security partnership with particular focus on collaboration on cyber capabilities and AI. From a US perspective, the Congressional Research Services released a report on the EU-US Privacy Shield and the status of transatlantic data flows, outlining its key principles for implementation of a new framework, guidance for organisations, as well as addressing the prospects for data flows between the two territories. Interestingly, the Office of the High Commissioner for Human Rights ('OHCHR') took a firm stance on the use of AI, calling for a moratorium on the sale and use of AI systems that pose a serious risk to human rights, until adequate safeguards are put in place.

In enforcement, the Cayman Islands Ombudsman announced that it had issued an enforcement order against a supermarket chain for failures to provide full access to data subject details following an access request. In addition, the Brazilian State of Minas Gerais' Public Prosecutor's Office ('MP/MG') announced that it had fined a telecommunication group BRL 10,702,464 (approx. €1,713,000) for non-compliance with a telemarketing block. Finally, the U.S. SEC announced a \$10 million settlement with an app company for engaging in deceptive practices about the collection of data.

What to look out for:

- Continued progress with US privacy bills on a state and federal level
- Public comments due on California CPPA Board call for comments on proposed rulemaking under CPRA
- Legislative activities in Latin America continue to progress such as Chile's data protection bill
- Proclamation awaited by the Governor-General of Barbados for the entry into force of some outstanding provisions of the new Act

APAC & the CIS

Key takeaways:

- China PIPL passed
- China DSL entered into force on 1 September
- Japan revised APPI guidelines published
- Hong Kong PDPO amendments passed

July

At the beginning of the month, it was confirmed that the Parliament of Mongolia was in the process of enacting comprehensive laws on personal data and cybersecurity, among others. Legislative reform progressed elsewhere across the region, particular in China, where the Shenzhen Municipal People's Congress ('MPC') released its draft AI Promotion Regulation for public consultation. Similarly, the Municipal Government of Hangzhou sought comments on its draft Social Credit Management Regulations.

After various industry and stakeholder responses, Hong Kong's Office of the Privacy Commissioner for Personal Data ('PDPC') announced that the Personal Data (Privacy) (Amendment) Bill 2021 amending the Personal Data (Privacy) Ordinance ('the PDPO Amendment Bill') had been gazetted and that deliberations would continue.

Cross-border partnerships continued with Singapore signing agreements with Japan and the UK in the field of information communication and financial cybersecurity. Furthermore, the Central Bank of Malaysia strengthened its policy on anti-money laundering and countering the financing of terrorism ('AML/CFT'), while the Australian Banking Association initiated a review into its Banking Code of Practice to enhance consumer protection.

At the same time, the Australian Department of Treasury announced amendments to its Consumer Data Right ('CDR') rules to promote open banking. Likewise, the New Zealand Government agreed to establish its first CDR framework, with the aim of introducing legislation by 2022. Macau joined these jurisdictions by adopting a consolidated consumer law, a new regime to protect consumer rights and interests.

Cybersecurity and data management reform remained a key focal point for regulators in the region, including in Australia, Pakistan, Japan, and China. Notably, the Australian Government proposed a number of reforms to strengthen cybersecurity. The Ministry of Information Technology and Telecommunication ('MOITT') in Pakistan also adopted its National Cybersecurity Policy 2021.

Echoing this focus, the Japanese Ministry of Economy, Trade and Industry ('METI') released its draft data management framework aimed at addressing risks during the data lifecycle. Likewise, the Cybersecurity Administration of China ('CAC') requested comments on its revised cybersecurity measures, in addition to introducing the Regulation on the Management of Network Product Security Vulnerabilities.

Elsewhere in China, the Standing Committee of the Shenzhen MPC finalised the Shenzhen Special Economic Zone Data Regulation, constituting the first comprehensive legislation on data protection in the country. At the national level, efforts by the NPC to enact the PIPL nevertheless continued.

Authorities and non-governmental groups in the region also paid closer attention to AI. The Data Security Council of India ('DCSI'), for example, developed a handbook on data protection and privacy for developers of AI. Meanwhile, South Korea's Personal Information Protection Committee ('PIPC') made available its guidance on AI and privacy, together with a checklist of recommended steps for the development and operation of AI services.

On 23 July 2021, the Indian Joint Parliamentary Committee ('JPC') filed a motion in parliament to extend the submission of its report on the Personal Data Protection Bill, 2019 to the first week of the winter session, having previously sought an extension in September 2020 and March 2021. Furthermore, the Russian Federal Service for the Supervision of Communications, Information Technology and Mass Communications ('Roskomnadzor') announced plans to establish dedicated commissions for data protection and for the protection of minors.

Privacy concerns were also shared by many regulators across multiple sectors. In Vietnam, stricter requirements for cross-border advertising services were implemented by the Ministry of Information and Communications ('MIC'). At the same time, the Philippine's National Privacy Commission ('NPC') issued an advisory addressing the privacy implications of data sharing between financial institutions. The Financial Markets Authority in New Zealand joined these authorities by issuing further guidance on cyber resilience for financial advice providers.

South Korea's PIPC continued to lead in enforcement actions. Notably, both the Reserve Bank of India and Roskomnadzor issued warnings to companies for their failure to comply with data localisation requirements. Finally, in landmark ruling, China's Supreme People's Court clarified and set limits to the use of facial recognition technology.

August

China became the latest country in the region to enact its first national data protection law, following the adoption of the Personal Information Protection Law ('PIPL') by the NPC on 20 August. Meanwhile, the Chinese State Council of the People's Republic of China announced that it had passed the Regulation on the Security Protection of Critical Information Infrastructure.

Issuing and updating guidelines remained a priority for authorities throughout the month of August. Notably, Japan's Personal Information Protection Commission ('PPC') launched a consultation on its revised guidelines on the Act on the Protection of Personal Information (Act No. 57 of 2003 as amended in 2015) ('APPI'), albeit not currently in force. South Korea's PIPC was particularly active in this regard, seeking opinions on its amended notice on pseudonymisation and amended security standards, in addition to publishing a revised

interpretation guide on the Personal Information Protection Act 2011 ('PIPA') and its 2020 amendments.

Likewise, the Philippine's National Privacy Commission ('NPC') continued to promote international standards in its advisories, prompting organisations to adopt those issued by the ISO. Hong Kong's PCPD also published new guidance on the ethical development and use of AI, while India's DSCI launched a privacy guide for the healthcare sector.

Discussions on Mongolia's Draft Law on the Protection of Personal Information progressed within the Parliament of Mongolia, which if passed, would enter into effect on 1 November 2021. Japan's PPC also announced a revised draft Law Enforcement Regulation on the Protection of Personal Information, setting enhanced breach notification requirements, among other things. The Legislative Council of Hong Kong ('LegCo') was especially proactive in advancing the proposed PDPO Amendment Bill, releasing a background brief, as well as supplementary papers and responses from key stakeholders.

August saw increased effort by financial regulators to tackle data protection issues in the financial sector. To address third-party risks, for example, countries such as India and Pakistan introduced frameworks and guidelines on adopting cloud services and outsourcing payment operations. Within the Commonwealth of Independent States, Russia's Roskomnadzor collaborated with the Bank of Russia to warn financial institutions against unlawfully processing personal data for purposes beyond the provision of services. Separately, the Bank of Russia developed security standards for customer authentication and a draft regulation on cyber resilience in banking activities. In a similar move, the National Bank of Ukraine announced its commitment to strengthen the protection and security of personal data in financial services.

Moreover, the Office of the Australian Information Commissioner ('OAIC') confirmed the reappointment of Angelene Falk as the Australian Information and Privacy Commissioner for an additional three-year term. For Thailand, the Ministry of Digital Economy and Society ('MDES') announced the launch of the National Cyber Security Agency ('NCSA') under the Office of the National Cyber Security Commission.

Data breaches and cybersecurity incidents across the region were increasingly reported on by organisations and authorities alike, including in Singapore and Japan. In response, the Delhi High Court in India called on the Government and the Indian Computer Emergency Response Team ('CERT-In') to investigate large-scale data breaches in the country.

In Russia, the Federal Antimonopoly Service ('FAS') developed draft principles to prevent unfair practices in digital markets and platforms. Pursuing a similar goal, the Chinese State Administration for Market Regulation ('SAMR') published draft regulations to prohibit unfair competition within the Internet. Further legislative reform continued in China, with the CAC introducing draft regulations on algorithm management and automobile data.

In terms of enforcement, the Russian FAS continued to impose fines for unlawful direct marketing. Enforcement action also intensified in South Korea, where two prominent media

companies faced respective fines of KRW 223.2 million (approx. €161,587) and KRW 6.44 billion (approx. €4,662,295) issued by the PIPC. Notably, the Taganksy District Court of Moscow also imposed fines totalling RUB 36 million (approx. €429,046) on three social media entities for non-compliance with data localisation requirements, following similar sanctions imposed in 2020.

September

The month of September began with China's DSL entering into effect on 1 September. Pakistan, Sri Lanka, and India were among the other countries in the region also advancing comprehensive data protection laws. Pakistan's MOITT, for example, published a revised consultation draft of the Personal Data Protection Bill. Furthermore, the Information and Communication Technology Agency of Sri Lanka ('ICTA') released another draft of the Act to Provide for the Regulation of Processing of Personal Data, which is expected to be published as an official bill in the coming months.

Notably, the JPC in India also recommenced its discussion of the Personal Data Protection Bill, 2019 after delays in July and August. In the Commonwealth of Independent States, the Parliament of the Republic of Tajikistan introduced a draft Information Code, which if passed would provide consolidated rules on data processing and data subject rights.

The PPC in Japan updated its guidelines and FAQs on the proper handling of specific personal information, while the OAIC in Australia launched its universal privacy principles targeted towards government and private businesses alike. Elsewhere, the Ukrainian Parliamentary Commissioner for Human Rights released recommendations for video surveillance systems, and the Office for Personal Data Protection ('GPDP') in Macau called on local organisations to comply with China's PIPL.

Singapore's Personal Data Protection Commission ('PDPC') made significant efforts in this regard, firstly by updating its guides on data protection management programmes and DPIAs, and secondly by announcing a new privacy guide and checklists for ICT systems.

In terms of technology and cybersecurity, the Cyber Security Agency of Singapore ('CSA') launched an industry consultation on a licensing framework for cybersecurity service providers. IndiaAI, a government-based initiative, also circulated a handbook on mitigating bias in AI, containing a formalised framework for start-ups on incorporate ethics and trust within AI development. In Japan, the National Center of Incident Readiness and Strategy for Cybersecurity ('NISC') also released its new cybersecurity strategy, outlining its approach towards digital transformation and sustainable development.

Within the financial sector, AML/CFT remained a point of concern for authorities across the region. In Kazakhstan, the Mazhilis of the Parliament of the Republic of Kazakhstan announced a proposed AML/CFT bill, with the METI in Japan also initiating a consultation on its revised AML/CFT guidelines specific to the credit card industry. Beyond that, the Central Bank of the Philippines ('BSP') urged for the passage a cybercrime bill aimed at strengthening electronic payments and financial stability.

Regulators in the region were also keen to address cross-border data transfers. For instance, Hong Kong's PCPD published FAQs regarding the use of the European Commission's Standard Contractual Clauses ('SCCs') and the applicability of the GDPR on Hong Kong organisations. Further progress was made with regards to the draft EU adequacy decision between South Korea and the European Commission, with the EDPB adopting a generally positive opinion in this regard.

Following further debate, Hong Kong's PCPD confirmed that LegCo had passed the PDPO Amendment Bill on 29 September, effectively incorporating new provisions to combat doxxing. Meanwhile, South Korea's PIPC submitted proposed amendments to PIPA at the National Assembly, with the view of clarifying data subject rights and consent mechanisms, as well as the interaction with the Act on Promotion of Information and Communications Network Utilization and Information Protection 2001 ('ICNA').

Finally, in yet another significant decision in South Korea, the PIPC fined a prominent software company KRW 12 million (approx. €8,693), while also establishing new standards for minor violations of PIPA. Other authorities across the region were also active in enforcement, including the New Zealand Office for the Privacy Commissioner ('OPC') which issued its first compliance notice to the Reserve Bank of New Zealand.

What to look out for:

- Entry into effect on China PIPL on 1 November
- Entry into effect of Belarus' Law on Personal Data on 15 November
- South Korea adequacy completion
- Movement on Pakistan's personal data protection bill, Sri Lanka's draft data protection bill, and India's Personal Data Protection Bill

EMEA

Key takeaways:

- New EDPB guidelines on codes of conduct, virtual voice assistants, and controller/processor concepts adopted
- UK post-Brexit plans and new proposed data regime announced
- South Africa's Information Regulator enforcement powers enter into effect
- Saudi Arabia publishes new data protection law
- UK Age Appropriate Design Code enters into force

July

After the South Africa Information Regulator's enforcement powers under the Protection of Personal Information Act, 2013 ('POPIA') entered into effect on 1 July 2021, it issued a number of guidance on, among other topics, processing of special personal information and processing personal data without consent.

In Togo, the National Assembly announced its ratification of the Cyber Security and Personal Data Protection ('the Malabo Convention') with the aim strengthen fight against cybercrime and the protection of personal data in Togo. Similarly, the Council of Europe ('CoE') confirmed the ratification of Convention 108+ in Italy.

Furthermore, regulators across multiple sectors and disciplines paid close attention to data protection and privacy-related issues. The Government of the Netherlands, for example, announced amendments to its telemarketing rules, which clarifies individuals' right to object. For financial services, the French data protection authority ('CNIL') introduced practical data protection guidance for the insurance sector. The Spanish data protection authority ('AEPD') also published a report, urging financial institutions to refrain from using facial recognition for compliance with AML/CFT obligations.

On an EU-level, proposals were also made by the European Commission to strengthen rules for AML/CFT. If adopted, the proposals would provide for a consolidated AML/CFT regulation at EU level, the establishment of a dedicated AML/CFT authority, a new AML/CFT directive, and specific rules for crypto-asset service providers.

Elsewhere, the Central Bank of the UAE ('CBUAE') Africa also issued guidance on AML/CFT for its licensed financial institutions on the implementation of Targeted Financial Sanctions. In particular, the guidance came into effect on 8 July 2021, and organisations were required to demonstrate compliance by 8 August 2021. In addition, the Abu Dhabi Global Market ('ADGM') issued new regulations for data protection fees and rules for fines. In addition, the DFSA in Dubai released its consultation paper on its whistleblowing proposal. In particular, the DFSA highlighted that the aim of the proposal is to standardise the approach to reporting and recording misconduct.

On 8 July, the EDPB held its 51st plenary session. The EDPB addressed several trending issues, including, among other things, coordinated enforcement actions against multi-jurisdictional entities. More importantly, the session culminated in the adoption of some crucial guidelines on codes of conduct, virtual voice assistants, and concepts of controller and processor under the GDPR.

Following this, the EDPB also initiated a public consultation on its code of conduct guidelines, which acknowledges that codes of conduct may be a suitable tool for cross-border data transfers to third countries. Indeed, cross-border transfers remained a key priority in July, which marked a year since the Schrems II Case. Notably, the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs published an independent study on the sharing of personal data after the Schrems II Case, in which it makes several recommendations to facilitate transfers to the US.

Legislative reform continued with many jurisdictions in Europe keen to modernise current frameworks in light of new technology. The President of the Government of Spain presented a new Digital Rights Charter which reaffirms several fundamental rights and principles. Likewise, the UK's DCMS launched its upcoming plan for digital regulation, highlighting a coordinated approach between different regulators and stakeholders. At the same time, the UK's ICO launched a beta version of its AI and data protection risk toolkit. In Germany, the Federal Office for Information Security ('BSI') also updated its minimum standard for external cloud services.

More generally, data protection authorities remained focused on health data and ongoing concerns stemming from COVID-19. Whereas the Belgian Data Protection Authority ('Belgian DPA') sought comments on its draft recommendations on the processing of biometric data, several countries such as Guernsey and Ireland also issued guidelines on vaccination passports and remote working.

Lastly, enforcement action significantly amplified in the month of July. Italy, Luxembourg, the Netherlands, France, Spain, and San Marino were among the jurisdictions issuing significant decisions against errant organisations, with the highest fine being €746 million imposed by the Luxembourg National Commission for Data Protection ('CNPD') for a company's targeted ad system.

August

The month of August began with the UK DCMS announcing an updated trust framework for the use of digital identities. In the updated version, the DCMS provides additional detail, including the process of certification and the different roles within data management.

Continuing this momentum, the ICO approved the first certification scheme criteria under the UK GDPR and the announcement of John Edwards, New Zealand's current privacy commissioner, as the preferred candidate for the next Information Commissioner. More importantly, weeks after obtaining EU adequacy, the DCMS revealed its post-Brexit plans for a UK data regime.

Among the proposed measures, the DCMS announced new guidance on international transfers and a new approach to assessing the adequacy of third countries. Accordingly, the ICO also requested comments on several tools and guidance for international transfers, including a draft international data transfer agreement and transfer risk assessments.

Furthermore, the Dubai International Financial Centre ('DIFC') continued its legislative reforms with the announcement that it had formally engaged with the UK's DCMS for an adequacy assessment of its data protection law. Likewise, the Qatar Financial Centre Authority ('QFCA') launched a public consultation on its data protection regulations and rules with a view to make the scope more consistent with the standards of international data protection laws. Also, the ADGM Office of Data Protection ('ODP') in Abu Dhabi released several guidance documents it provided clarity on its Data Protection Regulations 2021. Shortly thereafter, the ODP announced the adoption of new SCCs for data transfers outside the ADGM featuring new features that provide a more flexible approach and promote interoperability. Similar efforts were made in Switzerland where the Federal Data Protection and Information Commissioner ('FDPIC') confirmed the European Commission's new SCCs as a valid mechanism for data transfers to third countries, subject to Swiss law.

Separately, an internal document on the ePrivacy Directive, adopted by the European Data Protection Board ('EDPB') earlier in June, began to circulate in August. Notably, the document sets out the EDPB's position on the ePrivacy Directive's territorial application and the competency of national supervisory authorities.

In addition, authorities across the region tackled the topic of data sharing and compliance-related measures, among other things. The Gibraltar Regulatory Authority ('GRA'), for instance, launched its Data Sharing Code of Practice with a view of helping organisations develop compliant arrangements. The Dutch data protection authority ('AP'), on the other hand, granted licences to more than 160 financial institutions, permitting them to register and share personal information for fraud prevention purposes. Relatedly, the European Banking Authority ('EBA') issued draft guidelines on appointing compliance officers for AML/CFT. In addition, Israel's Privacy Protection Authority ('PPA') launched a public consultation on its DPIA guide which presents best practices for conducting DPIAs across all sectors of the economy. Notably, DPIAs are not required under Israel's data protection law.

August also marked an important month for cybersecurity developments. Most significantly, a new cybersecurity law entered into force in Italy on 5 August 2021. Shortly thereafter, a new decree was adopted in Italy to establish categories of ICT systems and services to be used in the Cybersecurity Perimeter, Italy's national system for protecting key communications infrastructure. In France, CNIL released guidance on preventing and responding to cyber attacks via email, while the Spanish National Cybersecurity Institute ('INCIBE') provided guidance on secure teleworking.

In terms of enforcement, the National Information Technology Development Agency ('NITDA') announced that it had fined an organisation NGN 10 million (approx. €20,700) for various

violations of the Nigeria Data Protection Regulation, 2019 ('NDPR') marking the first enforcement action issued under the NDPR. Israel's Privacy Protection Authority ('PPA') was particularly active this month fining organisations for, among other things, security vulnerabilities and failing to take adequate security measures. In Italy, the Garante issued a fine of €2.5 million to a company for violating principles of transparency in the use of its algorithms.

September

The Age Appropriate Design Code issued by the ICO entered into effect on 2 September, marking the end of a 12-month transition period. The code applies to providers of information society services that are likely accessible to children in the UK and requires them to incorporate a risk-based approach to designing online services.

Elsewhere, AI and new technologies dominated the conversation with the European Parliament commissioning a study on biometric identification and issuing corresponding amendments to the European Commission's Proposal for an AI Regulation. At the national level, the UK Government forged ahead with its national AI strategy, a 10-year plan towards an AI-enabled economy. Relatedly, Turkey's Personal Data Protection Authority ('KVKK') developed recommendations for stakeholders in the AI field, in addition to new guidance on processing biometric data. The Liechtensteiner data protection authority ('DSS') published its guidance on profiling and automated decision-making pursuant to the GDPR. Germany joined these countries with the release of decision-making guidelines on blockchain technology by the Federal Network Agency ('Bundesnetzagentur').

International cooperation continued in September. Data protection authorities from G7 countries held a meeting on 9 September to agree on key priorities for addressing digital markets, AI, and cookies, among other things. Separately, the CoE announced the launch of a global AI portal aimed at promoting global cooperation in the field. At the same time, the Office of the High Commissioner for Human Rights ('OHCHR') issued a report on the sale and use of AI systems, urging for a moratorium on the same.

Jurisdictions continued to reflect on international data flows and the impact of the Schrems II Case. Accordingly, the Norwegian data protection authority ('Datatilsynet') published update guidance, outlining additional measures that may be adopted to ensure sufficient protection of personal data.

In terms of EU adequacy, the EDPB adopted its opinion on the European Commission's draft adequacy decision for South Korea. Although the opinion was largely positive and recognised South Korea's PIPA as providing essentially equivalent protection, the EDPB asked the Commission to further clarify the decision's binding nature, among other things.

In addition to developments seen in previous months, legislative reform in the UK went ahead as the UK Government launched a public consultation on its plans to boost digital and economic growth. As part of its proposals, an overhaul of the UK data regime is expected, which would include reforms to the current frameworks for, among other things, accountability, cookies and electronic communications, the processing of sensitive data, and data transfers. At

the same time, the DCMS confirmed the appointment of John Edwards as the new Information Commissioner. UK Prime Minister, Boris Johnson, also announced the launch of a new security partnership between the UK, the US, and Australia.

Saudi Arabia's National Centre for Documents and Archives Royal Court published, on 24 September, the new PDPL, following its approval. Notably, the enforcement of the law will fall under the jurisdiction of the SDAIA for the first two years, after which it may be switched to the National Data Management Office. Legislative reform continued in Saudi Arabia with the National Cybersecurity Authority ('NCA') launching a public consultation on draft cybersecurity controls for operating systems. Similarly, the United Arab Emirates signalled that a new federal data law would be published soon. Finally, the DIFC launched a non-legislative data protection consultation on updated proposed DIFC data export and sharing materials which outline specific questions on, among other things, updated SCCs, adequacy decisions standards, and Binding Corporate Rules ('BCRs').

In Zimbabwe, the Media Institute of Southern Africa Zimbabwe ('MISA Zimbabwe'), took a firm stance on the cybersecurity and data protection bill which has now been sent to the President's office. More specifically, MISA Zimbabwe outlined that the bill has gone through significant changes from the one that was the subject of public hearings. In her 2021 State of Union Address, EU President Ursula von der Leyen alluded to the need for a new European Cyber Resilience Act. Also bolstering its cybersecurity regime, Kuwait's Communication & Information Technology Authority ('CITRA') published a new cloud computing regulatory regime with provisions for among other things, cybersecurity, data classification, and data privacy protection regulations.

Meanwhile, authorities remained active in issuing new resources. Key pieces of guidance issued in September include CNIL's data protection maturity self-assessment model and GDPR guide for recruitment sector. The Swedish Financial Supervisory Authority ('Finansinspektionen') released guidelines on consumer credit assessments, focusing on the collection of information from appropriate sources. Interactive Advertising Bureau ('IAB') Europe also published a new guide on data quality targeted towards digital advertising chains when accessing and storing personal data through online identifiers.

Finally, European authorities continued to lead in enforcement action. Ireland's Data Protection Commission ('DPC') initiated investigations into two companies, while also issuing a €225 million fine to a company as part of its obligations under a binding EPDB dispute resolution decision made in July.

What to look out for:

- Outcome of the UK consultations on data transfers and broader data protection reforms
- Follow-up on the Commission's consultation on AI Regulation proposal
- EDPB taskforce response to NOYB complaints on cookies, and further enforcement action from CNIL
- Finalised adequacy decision on South Korea from the Commission
- Finalisation of the UAE Federal Data Law

Further reading: Please note that there is further reading material on all the developments discussed in this review on the OneTrust DataGuidance platform.

Insights

- [International: Data transfers and online advertising technologies post-Schrems II](#)
- [EU: First transnational codes approved under the GDPR](#)
- [EU: The future of surveillance-based advertising](#)
- [EU-UK: Analysing the UK adequacy decision and what's next for UK data protection](#)
- [EU: EDPB and EDPS joint opinion - the Draft AI Regulation from a privacy perspective](#)
- [EU: Practical implications of the finalised EDPB guidelines on the concepts of controller and processor](#)
- [Ireland: Whistleblowing law amendments](#)
- [Turkey: Commitments on the transfer of data abroad](#)
- [Turkey: Provisions for the protection of children's data](#)
- [Turkey: The first national AI strategy](#)
- [UK: Dissecting post-Brexit plans for transfers, adequacy, and assessment manuals](#)
- [Italy: Garante's finalised guidelines on cookies and similar tracking technologies - key takeaways](#)
- [Gibraltar: The data sharing code and what organisations need to know](#)
- [Netherlands: Amendments made to the Dutch Telecommunication Act](#)
- [Finland: Key takeaways from the TRAFICOM revised guidelines on cookies and similar tracking technologies](#)
- [Russia: 2021 trends in data protection regulation](#)
- [Vietnam: Difficulties in creating a privacy program in Vietnam](#)
- [Kazakhstan: Amendments to privacy law](#)
- [China: Operationalising PIPL Part one: Data Subject Rights](#)
- [China: Operationalising PIPL Part two: Data transfers and localisation](#)
- [China: Data Security Law overview](#)
- [China: The PIPL - An act in three drafts](#)
- [Thailand: Data protection guidelines for Thai banks](#)
- [Taiwan: EU GDPR adequacy decision: The road ahead](#)
- [Saudi Arabia: New Personal Data Protection Law – What you need to know](#)
- [Bahrain: Overview of implementing orders](#)
- [Pakistan: A comparative analysis of 2020 and 2021 draft personal data protection bills](#)
- [QFC: Proposed changes to QFC's 2005 Data Protection Regulations and Rules](#)
- [Australia: New privacy legislation to address transparency by social media companies](#)
- [Australia: Trusted Digital Identity Framework and proposed expanded digital identity scheme](#)
- [California: The AG's first year enforcement update and online violation notification tool](#)
- [Colorado: Analysing the Colorado Privacy Act](#)
- [Colorado: Consumer rights under the Colorado Privacy Act](#)
- [Colorado: Analysing controller obligations under the Colorado Privacy Act](#)
- [Canada: Diversity and inclusion data](#)
- [Quebec: Quebec's privacy legislation is growing teeth - What businesses need to know before they get bitten](#)
- [El Salvador: Data privacy regulations overview](#)
- [Ecuador: Data subject rights under the new law](#)
- [Brazil: Cookies under the LGPD](#)

- [Mexico: The case for amending breach notification rules](#)
- [Brazil: Data protection in the energy sector](#)

Webinars

- [Canada Privacy: Breaking Down Quebec's Bill 64](#)
- [Canada Privacy: Updates on Laws & Regulatory Developments](#)
- [Colorado Joins US Privacy Landscape with New Law](#)
- [Understanding the Proposed New UK SCCs and Data Transfer Assessments](#)
- [ESG Compliance: EU and German Regulatory Updates](#)
- [Controller or Processor? EDPB Guidelines Unpacked](#)
- [AI Regulation: Implications for FinTech and FinTech M&A](#)
- [China PIPL: What You Need to Know](#)
- [China Regulatory Update: The Data Security Law](#)

Portals & Comparisons

- [Data Residency](#)
- [China's PIPL and DSL](#)

