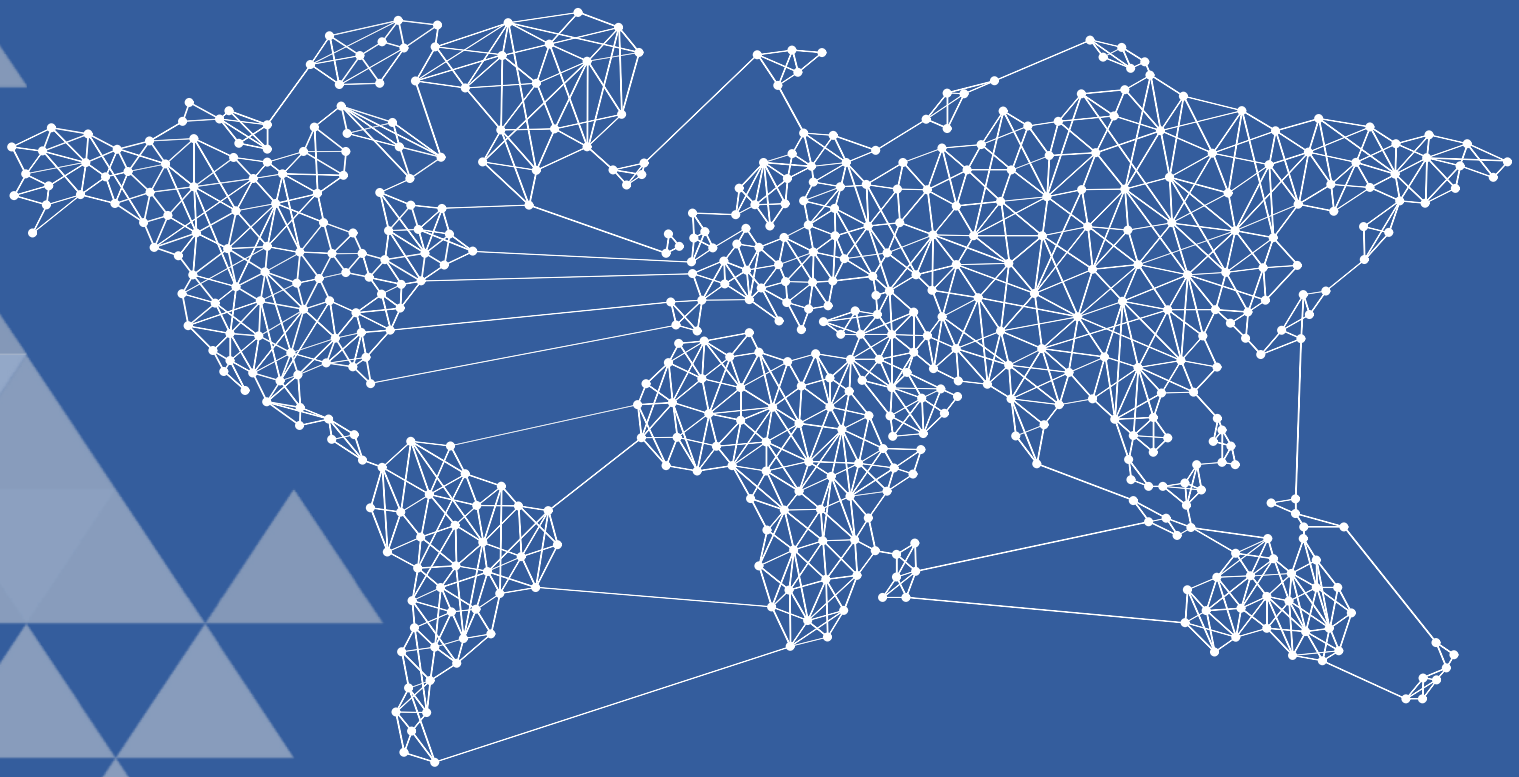
OneTrust DataGuidance Privacy Review

Q1 2021



OneTrust DataGuidance™
REGULATORY RESEARCH SOFTWARE

About the report

Quarter 1 of 2021 continued to be a very active one. Virginia became the next US state to pass comprehensive privacy legislation following on from California. Legal reform was a priority for US States with 21 states introducing comprehensive privacy legislation. Negotiations continued on a reformed EU-US Privacy Shield and regulators globally continued to prioritise mechanisms to facilitate cross-border data flows. Organisations also await the final EDPB recommendations on data transfers post Schrems II, as well the EU Commission's revised set of SCCs. Just months after the UK formally withdrew from the EU, the European Commission published a draft UK adequacy decision and also began the process of adequacy for South Korea. COVID-19 vaccine rollout began, raising privacy concerns in terms of consent, processing of vaccine information, and employer obligations.

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

OneTrust DataGuidance™
REGULATORY RESEARCH SOFTWARE

Global

Key takeaways:

- UK and South Korea adequacy decisions advance
- A number of US states introduced comprehensive privacy bills
- Council of the EU agrees on draft ePrivacy Regulation
- COVID-19 vaccinations' privacy and data protection implications ongoing
- Continued developments and regulatory action in the ad tech ecosystem

COVID-19 vaccinations and privacy

The COVID-19 pandemic continued to have lingering impact on the privacy world specifically in regards to the large amounts of processing of sensitive personal data globally. Authorities in Switzerland, Kenya, and South Korea issued guidance addressing, among other topics, data protection requirements for private companies when collecting health data, access to personal data, as well as personal information protection measures to combat the COVID-19 pandemic. Privacy considerations only intensified as vaccine development and deployment began. In particular, questions arose as to the efficacy of vaccine passports and the obligations and privacy considerations for employers in relation to employee vaccination information. Specifically, countries including Denmark, Hungary, Estonia, and Greece are considering vaccine passports or similar technologies linking an individual's vaccination information to a digital identification. Israel's Green Pass is already well under way and the European Commission recently released its proposal for a regulation on a framework for Digital Green Certificates which would facilitate free movement during the COVID-19 pandemic. Authorities in Germany, Latvia, and Belgium have issued guidance on the processing of personal data regarding vaccinations, highlighting the necessary consent requirements for sharing such information under the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR'). In addition, in the context of employer privacy obligations in relation to COVID-19 vaccinations, authorities in Australia, Italy, and the Czech Republic published guidance on, among other things, requirements to vaccinate employees, data retention periods for vaccination data, and consent requirements for the processing of personal information.

Ad tech and cookies

As a result of announcements by regulators and private companies, the digital advertising industry continues to make its way through a transformative period. To this end, in January, the UK's Information Commissioner's Office ('ICO') announced the resumption of its investigation into real-team bidding and the ad tech industry.

Moreover, the beginning of the year saw the Council of the European Union announcing that its Member States had agreed on a negotiating mandate for the proposed Regulation concerning the Respect for Private Life and the Protection of Personal Data in Electronic Communications and Repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) ('the Draft ePrivacy Regulation'). The Draft ePrivacy Regulation, once adopted, will provide harmonised standards across the EU on areas such as cookies and similar technologies, direct marketing practices, metadata processing, and security within the Internet of Things. A number of investigations were initiated in the industry with specific attention to digital advertising as it pertains to children's data including the illegal processing of children's data, age controls, and unfair, misleading or deceptive marketing practices. Furthermore, authorities including France's data protection authority ('CNIL') and the Interactive Advertising Bureau ('IAB') Europe, as well as USA's IAB Tech Lab, published guidance including studies on online targeted advertising, navigating the post-third-party era, and standards for responsible addressability and predictable privacy. CNIL's updated version of its frequently-asked-questions ('FAQs') on its guidelines and recommendations on cookies and other trackers, which entered into force on 1 April 2021, cover general questions regarding the commencement of CNIL compliance audits, scope of application, audience measurement cookies, conditions for obtaining valid consent from users for the use of cookies, and the manner in which users should be able to opt-out from the use of cookies and other trackers.

Finally, None of Your Business ('NOYB') announced that an appeal by Max Schrems and a social media company against a judgment in a court in Vienna had reached the Austrian Supreme Court. More specifically, the case involved the social media company's alleged circumvention of the consent rules under the GDPR in respect to its personalised advertising.

US State privacy bills

The year began with a flurry of comprehensive data protection bills being introduced at the state level. This included a number of bills that had previously been introduced. Currently, 21 states have introduced comprehensive privacy bills so far, most notably Virginia's House Bill 2307 for the Consumer Data Protection Act ('CDPA') and its companion Senate Bill 1392 were signed into law, on 2 March 2021, by the Virginia State Governor. For the most part, the CDPA follows on from previously enacted state privacy legislation like the California Consumer Privacy Act of 2018 ('CCPA') and also takes inspiration from the GDPR. Similarities include definitions of personal information, sensitive/special categories of information, scope, data subject rights, and data security provisions. The CDPA departs from the CCPA in that, among other things, the authority is given to the Attorney General and not a centralised supervisory authority, there is no private right of action, and processing as it relates to a child is explicitly defined under sensitive personal data.

Elsewhere, bills in Mississippi, North Dakota, and Utah have already failed to pass. However, with many legislative sessions closing, there is a strong possibility for others to result in final approval. Interestingly, while most bills currently being discussed follow industry standards and take provisions from the CCPA, discrepancies exist, namely the inclusion of a private right of action, the opt-in requirement age, and the personal scope of application. Athough it remains to be seen which state will follow Virginia, many experts believe that Florida's Senate Bill ('SB') 1734 for an Act Relating to Consumer Data Privacy and its companion bill SB 1734 could follow soon.

Cross-border data transfers

Almost a year on from the decision in *Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems* (C-311/18) ('the Schrems II') and international data transfers continues to be a major talking point. From an EU perspective, organisations await the European Data Protection Board's ('EDPB') finalised Recommendations on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data. An updated version of the European Commission's Standard Contractual Clauses ('SCCs') is also due to be released, with the EDPB and the European Data Protection Supervisor ('EDPS') providing their opinion on the same and calling for several amendments to raise the clarity of the instrument's text, always

taking into account the consequences of the Schrems II decision. In terms of EU-US negotiations, EU Commissioner of Justice, Didier Reynders, alongside the U.S. Secretary of Commerce, Gina Raimondo, issued, on 25 March 2021, a joint statement noting that the US Government and the European Commission have decided to intensify negotiations on an enhanced EU-US Privacy Shield framework. Privacy groups and regulators continue to weigh in on trade negotiations for the EU and US with the Information Technology Industry Council ('ITI') issuing recommendations for the functioning of the proposed EU-US Trade and Technology Council with ITI recommending key policy areas including artificial intelligence ('AI'), data governance, and data sharing.

In the APAC region, the ministers of the Association of South East Asian Nations ('ASEAN') published their Data Management Framework ('DMF') and Model Contractual Clauses for Cross Border Data Flows ('MCCs'), which aim to harmonise national laws, while also facilitating business and the digital competitiveness of the region. Notably, the DMF provides organisations with best practices to manage the risks associated with data-dependent operations, while the MCCs set out concise contractual terms and conditions to be used in legal agreements between business in the course of cross-border data flows.

After a draft agreement was reached for cross-border data flows between the UK and the EU temporarily until July 2021, the European Commission published a draft of its adequacy decision for the UK and began the formal process. Additionally, after recent changes to its data protection laws, the European Commission announced the conclusion of its adequacy findings for South Korea who will now also begin the process towards adequacy.

What to look out for:

- Ongoing developments for a revised EU-US Privacy Shield negotiations
- State privacy laws passing
- Continued discussions on a US federal privacy law
- Finalisation of UK and South Korea adequacy process
- Finalised EDPB recommendations for data transfers post Schrems II and revised EU Commission's SCCs

Americas & Caribbean

Key takeaways:

- Multiple comprehensive privacy bills introduced
- Virginia CDPA enacted
- California Privacy Protection Agency established
- Continued Privacy Shield Negotiations
- Panama data protection law enters into effect
- Comprehensive privacy law being discussed in Ecuador
- Bermuda validates APEC CBPR for data transfers

January

The start of 2021 saw a significant increase in activity in the US at both the federal and state level. In particular, with a change in administration and privacy prioritised at the legislative level many bills were introduced and reintroduced in January. At the federal level, US Senators and Representatives reintroduced the Public Health Emergency Privacy Act which aims to set strong and enforceable privacy and data security rights for health information at a federal level. At the state level, a number of states introduced both targeted and comprehensive privacy bills. Oklahoma's House of Representatives introduced a bill on online business data transparency ('HB 1130'), whilst New York's state legislature introduced bills on biometric privacy, regulating the sale of consumer personal information to third parties, online consumer protection, and COVID-19 data collection. In terms of comprehensive privacy bills, Virginia, New York, Minnesota, and Washington all introduced versions of previously drafted bills, including the Virginia Consumer Data Protection Act ('SB 1392'), the Minnesota Consumer Data Privacy Act ('HS 36'), the Washington Privacy Act ('SB 5062'), and the New York Privacy Act ('AB A680'). Privacy advocates were notably hopeful about the 2021 round of privacy bill proposals in light of positive remarks from state Governors.

Enforcement activity also increased in the US in January. The U.S. Department of Justice ('DoJ') issued a $150 million fine against a company for selling personal information as part of a fraudulent scheme. In addition, the Financial Crimes Enforcement Network ('FinCEN') announced a $390 million civil penalty against a bank for violations of the Bank Secrecy Act. Furthermore, the U.S. Department of Health & Human Services' Office for Civil Rights ('OCR') continued its enforcement under its right of access initiative and reached a $200,000 settlement with a company for Health Insurance Portability and Accountability Act of 1996 ('HIPAA') Privacy Rule violations. In Latin America, the Colombian data protection authority ('SIC') continued to issue fines. In particular, two organisations were fined COP 109,023,120 (approx. €25,718) and COP 172,619,940 (approx. €40,721) for failing to facilitate data subject rights.

In sectoral developments, the U.S. Chamber of Commerce's ('CoC') Center for Capital Markets Competitiveness published a report detailing a number of recommendations on digital assets including technology neutral regulation, regulatory responsiveness, central

bank digital currency research and development, and the establishment of a White House Task Force. Subsequently, the Computer Security Resource Center ('CSRC') of the National Institute of Standards and Technology ('NIST') solicited comments on a draft publication on the security of information exchanges and the risks associated with their management. Furthermore, New York introduced a bill in relation to the collection and use of information during the COVID-19 pandemic.

After the Canadian Government tabled Bill C-11 for An Act to enact the Consumer Privacy Protection Act and the Personal Information and Data Protection Tribunal Act and to make consequential and related amendments to other Acts (also known as the Digital Charter Implementation Act, 2020), there has been calls by privacy advocate groups and provincial regulators for reform Canada's public sector privacy law. The Canadian Department of Justice announced, on 5 January 2021, that the public consultation period for modernising Canada's Privacy Act 1985 had been extended until 14 February 2021. Elsewhere, Brazil's data protection authority ('ANPD') issued its Biannual Regulatory Agenda for 2021-2022 which included a differentiated regulation for small businesses, editing of regulations and procedures on personal data protection and data protection impact assessments ('DPIA'), launching of a resolution to determine the term required for reporting a security incident, and guidelines on international transfers of personal data.

February

In February, US state privacy legislation showed no signs of slowing down. Comprehensive privacy bills were introduced in Illinois ('HB 3910'), Minnesota ('HB 1492'), Massachusetts ('SD 1726'), Vermont ('HB 075'), Alabama ('HB 216'), Utah ('SB 200'), Florida ('HB 969'), Oklahoma ('HB 1602'), and Washington ('HB 1433'). For the most part, the bills introduced contain obligations for data controllers and processors including data security and breach requirements, data subject rights, privacy policy requirements, prohibitions on processing, as well as enforcement powers by the State Attorney General.

Virginia was the first state to move forward with their comprehensive privacy bill for the CDPA which passed both the State Senate and State House of Delegates by 18 February 2021. In addition, a bill which seeks to amend the Illinois Biometric Information Privacy Act ('BIPA') was introduced on 2 February 2021, including provisions requiring written privacy policies when processing biometric information. State legislatures also took action on a number of bills ranging from topics on genetic information and biometric technology to data brokers. Furthermore, both Idaho and Rhode Island became the next two states to implement the National Association of Insurance Commissioner's ('NAIC') Cybersecurity Act into their state legislation in an important step to harmonising insurance data security laws across states.

In enforcement news, the Financial Industry Regulatory Authority ('FINRA') issued a proposed $125,000 settlement against a company for improper disclosure of personal information without consent. The OCR continued its work under the HIPAA Right of Access Initiative and settled its 17th investigation. In addition, significant investigations were finalised by both the Federal Trade Commission ('FTC'), which reached a settlement

with a company over security and privacy practices, and the New York Department of Financial Services ('NYFDS'), which released an investigative report on an organisation's privacy practices. Moreover, the NYFDS issued, on 4 February 2021, its Cyber Insurance Risk Framework which stipulates recommendations and best practices for the industry to manage cyber insurance risk. Financial trade groups have continued to show support for the advanced notice of proposed rulemaking ('ANPR') issued by the Consumer Financial Protection Bureau ('CFPB') which seeks to modernise the consumer access and data sharing rules under Section 1033 of the Dodd-Frank Act. Data sharing was also a focus for privacy advocate groups such as the Electronic Frontier Foundation ('EFF') who released, on 12 February 2021, a white paper outlining the importance of the interoperability regime and highlighting the benefits, which they argue, outweigh the privacy and data security issues associated with it.

February marked the conclusion of one of the most significant investigations by the Office of the Privacy Commissioner of Canada ('OPC') in conjunction with the privacy commissioner of Alberta, British Columbia, and Quebec. In particular, the OPC issued a number of recommendations for an organisation which was accused of processing and collecting sensitive biometric information without consent. However, the OPC noted that as the organisation disagreed with its findings it would, along with the four authorities mentioned, pursue other actions available under their respective laws. In anticipation of privacy reform in Canada, the Interactive Advertising Bureau Canada ('IAB Canada') released its draft policies for the Canadian Transparency and Consent Framework ('the TCF') for public comment. Specifically, the TCF consists of a set of technical specifications and polices to which publishers, advertisers, technology providers, and others may voluntarily adhere to. In consideration of the federal privacy sector reform in Canada, the Office of the Information and Privacy Commissioner of British Columbia ('OIPC') released a supplementary submission to the Special Committee to Review the Personal Information Protection Act 2003 ('PIPA') following its submission in September 2020. Particularly, the submission underscores the importance of harmonisation between the federal law and PIPA. In addition, the British Columbia Financial Services Authority ('BCFSA') released for public comment, two draft guidelines which focus on information security and outsourcing in the financial sector.

After announcing small business regulations as regulatory priority in January, the ANPD launched a public consultation on the applicability of the 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') for small businesses, as well as start-ups and individuals who process personal data for economic purposes. Moreover, a significant data breach in Brazil prompted members of the Chambers of Deputies of the National Congress to request that the ANPD provide information in response to the breach and outlined measures, including guidance, in response to the same. Additionally, the ANPD launched a public consultation on the notification of security incidents pursuant to Article 48 of the LGPD. Notably, two competing bills were introduced to the Chamber of Deputies which would either make LGPD enforcement immediate or extend the current enforcement date of 1 August 2021 to 1 January 2022. Interestingly, the COVID-19 pandemic was used to justify both bills. Finally, in Costa Rica Bill No. 22.388 to Reform the Law on the Protection of Persons Regarding

the Processing of their Personal Data No. 8968 of 2011 ('Bill No. 22.388') was published, on 12 February 2021, in the Official Gazette. In particular, Bill No. 22.388 aims to improve the current data protection framework in Costa Rica by clarifying definitions, developing principles governing the processing of personal data, improving data subject rights, and strengthening the powers of the Costa Rican data protection authority ('PRODHAB').

March

March saw Virginia become the next state with a comprehensive privacy law with the CDPA signed by Virginia Governor, Ralph Northam, on 2 March 2021. In particular, the CDPA, which will enter into force on 1 January 2023, provides consumer with rights to opt-out, confirm, amend, delete, and share their data. Furthermore, the CDPA contains several obligations for data controllers, such as the provision of a privacy notice, data security requirements, and outlines rules governing contracts with data processors. States across the US continued to follow suit in introducing comprehensive bills, including Colorado ('SB 21-190') and Arizona ('HB 2685'). Both Iowa and Minnesota introduced bills for insurance data security laws following the NAIC legislation closely. At the state level bills were also introduced on topics including student data security, health data, and cybersecurity.

At the federal level a bill for the Information Transparency and Personal Data Control Act was reintroduced, on 10 March 2021, and aims to create a national data privacy standard and establish a uniform set of rules for businesses when handling personal information including data relating to finance, health, genetics, biometrics, and geolocation. A bill for the Data Care Act was also reintroduced which seeks to establish a framework for a duty of care obligations for businesses to protect user data.

In California, the long-awaited announcement of the appointment of the newly established California Privacy Protection Agency ('CPPA') came on 17 March 2021 when the California Attorney General ('the California AG') appointed its inaugural five-member board as outlined under the California Privacy Rights Act of 2020 ('CPRA'). In particular, the CPPA will have full administrative power, authority, and jurisdiction to implement and enforce the CCPA and CPRA. The California AG also announced approval of additional regulations under the CCPA which focus on unfair consumer procedures like 'dark patterns,' confusing language or unnecessary steps, or presenting reasons why consumers should not opt-out.

Moreover, the USA IAB Tech Lab released standards for responsible addressability and predictable privacy for public comment which would be designed to provide a foundation on which to build solutions that prioritise consumer privacy and accountability. In addition, Utah and New York introduced bills addressing online advertising. Discussions on a reworked EU-US Privacy Shield are ongoing and the US Congressional Research Service released, on 17 March 2021, a report on the EU data transfer requirements and US intelligence laws examining the impact of the Schrems II judgment. The report outlines a number of considerations for Congress, including an executive action addressing the concerns raised in the Schrems II judgement, negotiating a diplomatic solution to replace Privacy Shield, or adopting statutory requirements which properly address concerns raised in the judgement. In Bermuda, the Office of the Privacy Commissioner ('PrivCom') announced that they would recognise the Asia Pacific Economic Cooperation ('APEC') Cross Border Privacy Rules ('CBPR') system as a certification mechanism that can be utilised for overseas data transfers under Section 15(4) of the Personal Information Act ('PIPA').

Ecuador could be the next Latin American country with a comprehensive privacy law after the National Assembly announced, on 10 March 2021, that the Commission on Sovereignty and International Relations held two hearing on the framework of the draft Organic Law on the Protection of Personal Data. In addition, Panama's Law No. 81 on Personal Data Protection entered into effect on 29 March 2021 after its enactment two years prior. Authorities in Brazil were active in March as the Central Bank of Brazil ('BACEN') issued Resolution No. 4,893 on the Cybersecurity Policy and the Requirements for Contracting Data Processing Storage and Cloud Computing Services to be Complied with by Financial and Other Institutions, authorised to operate by BACEN which sets out polices for security incidents, disclosures, and data retention requirements for the financial sector. Finally, in Brazil the ANPD and the Brazilian Federal Department of Consumer Protection of the National Consumer Secretariat ('SENACON') signed a technical cooperation agreement in order to promote joint actions on issues involving personal data and consumer protection.

What to look out for:

- Introduction of more general privacy bills in the US States
- Canada's reform of PIPEDA as well as provincial reforms of privacy legislation in Canada, notably Quebec and British Columbia
- Legal reform in Chile, Costa Rica, and Ecuador

APAC & the CIS

Key takeaways:

- Draft regulations in payments sector in Asia
- Cybersecurity guidance issued
- Singapore PDPA amendments enter into force
- South Korea publishes PIPA amendments
- Conclusion of South Korea adequacy negotiations

January

In Pakistan, the Ministry of Information Technology and Telecommunications ('MOITT') announced that the long-awaited Personal Data Protection Bill 2020 would shortly be presented to the concerned department for legislative approval. South Korea's Personal Information Protection Committee ('PIPC') published the final draft of the amendments to the Personal Information Protection Act 2011 ('PIPA') for public consultation which include, among other things, the introduction of data portability rights and increased requirements for data transfers outside of South Korea. Australia continues to prioritise competition in the marketplace, and the Senate Standing Committee on Economic held a public hearing on discussion on the proposed code that aims to address the bargaining power imbalances between Australian news media business and big tech digital platforms.

The Malaysian Ministry of Communications and Multimedia reaffirmed its support in implementing the initiatives under the ASEAN Digital Governance Framework to enable safe cross-border data flows. Bank Indonesia ('BI') announced a new regulation on consumer protection applicable to payment system operators and money market businesses, in addition to a more general regulation on payment systems. In Pakistan, the MOITT published its draft National Cybersecurity Policy 2021 for public consultation which aims to address the increased risk of cybersecurity incidents and financial risks to consumers. Many jurisdictions have faced increased data breaches and security incidents with the Office of the Australian Information Commissioner ('OAIC') reporting a 5% increase in the second half of 2020 of notifiable breaches. Cybersecurity incidents also took place at the Australian Securities and Investments Commission, Health Research Council of New Zealand, and the Reserve Bank of New Zealand as the number of government cyber-attacks intensified. The Australian Cyber Security Centre ('ACSC') released two guidance in relation to identifying and managing cyber supply chain risks and domain system security. In response to recent data breaches, authorities in Singapore, China, and India published guidance on emerging cyber threats in blockchain and IoT security and provided mitigation tips including periodic security passements and anonymisation measures. Furthermore, authorities in the region, including South Korea, Indonesia, Australia, and New Zealand PIPC continued to issue guidance on the impact of the COVID-19 pandemic and the protection of personal information, data management for vaccine programs, and contact tracing.

In enforcement action, the Australian Communications and Media Authority ('ACMA') issued a remedial direction to a company for publishing the personal information for unlisted phone numbers. Additionally, the ACMA fined an organisation AUD 310,800 (approx. €198,240) for breaches of the Spam Act 2003 (Cth). Moreover, the High Court of Delhi issued a preliminary decision to suspend a INR 9.3 million (approx. €108,600) fine imposed on a payment services company for AML violations, pending further clarifications from financial authorities. China's Ministry of Industry and Information Technology released its first batch of notifications to apps on violations of user rights in 2021. Furthermore, South Korea's PIPC took action on seven companies for violations of its data protection law and imposed several fines for data breaches and data security violations of the data protection law, as well as processing notification failures.

Belarus continued its administrative reform with the National Information Centre publishing amendments to the Code of Administrative Offences of the Republic of Belarus. Specifically, the amendments outline sanction for personal data processing violation including the intentional unlawful collection, storage, or provision of personal data and the intentional illegal distribution of personal data. Furthermore, the National Information Centre also announced that the draft law on personal data, which had already been approved by the Council of Europe, would be ready for adoption at its second reading during the spring parliamentary session. The Belarus Council of Ministers also passed a decree governing the use of digital banking technologies. Finally, in Uzbekistan, amendments to the personal data law introduced data localisation requirements for the processing of personal data of Uzbek citizens. The localisation requirements will enter into force on 16 April 2021.

February

In Singapore, the month began with amendments to the Personal Data Protection Act (No. 26 of 2012) ('PDPA') entering into effect on 1 February 2021. In particular, the amendments include, among others, mandatory data breach notification requirements, new consent obligations, and increased powers for the Singapore Personal Data Protection Commission ('PDPC'). Legislative reform continued across the Asia region with Vietnam's Ministry of Public Security publishing a draft decree on personal data protection and inviting comments on the same. Equally, Thailand's PDPC announced hearings for subordinate regulations under the PDPA.

Fiji announced the enactment of its Cybercrime Act 2021 which was introduced by the Government in February 2020. In particular, the Cybercrime Act regulates the processing and handling of computer data and computer systems, provides law enforcement officials powers authority to collect and intercept data, and empowers the Minister of Communications to issues regulations prescribing penalties of a maximum of FJD 200,000 (approx. €81,260) for legal entities. Moreover, the Fiji Parliament passed the National Payment System Act 2021 which aims to implement a framework to regulate payment service providers operating wholly or partly in Fiji and establish the Reserve Bank as regulator to, among other things, issue directives, establish retention requirements, and take administrative action in cases of non-compliance.

Just months after the enactment of the Privacy Act 2020, the New Zealand Office of the Privacy Commissioner ('OPC') issued a briefing to the Minister of Justice recommending further key reforms to be implemented including the introduction of, among other things,

the right to be forgotten and data portability, provisions addressing automated decision-making and the processing of de-identified data, and increased powers to the OPC. Furthermore, the OPC announced that it had created an interactive tool to aid organisations when transferring personal information in compliance with Information Privacy Principle 12.

Following debates in the Australian Parliament, the Treasury Laws Amendment (News Media and Digital Platforms Mandatory Bargaining Code) Bill 2021 passed, on 25 February 2021. In particular, the Code provides a framework for dispute resolution between parties and includes provisions ensuring that an environment of mutuality is fostered. A further code of conduct was released by the ACMA in relation to disinformation and misinformation, and signatories have until May 2021 to sign up to its commitments. Cybersecurity authorities continued efforts to bolster incident response with the ACSC in Australia publishing two guidance documents including a report on key cybersecurity threats in the health sector and a small business cybersecurity guide, and the Indonesia National Cyber and Encryption Agency establishing an incident response team in addition to issuing guidance on cyber risk profiles for the banking sector. Furthermore, authorities in Singapore issued guidance on the security of cloud services and data sharing agreements. In addition, the OAIC launched a public consultation on its guide to securing personal information. Data protection supervisors in the Philippines and Japan also issued guidelines on data sharing, data subject rights, cybersecurity, and cloud services. Regulatory reform in the financial sector continued with the Reserve Bank of India issuing a direction on digital payment security controls and announcing plans to issue guidelines on outsourcing in the payments industry.

Legislators in Russia were focused on strengthening enforcement powers. In particular, Bill No. 1061159-7 was signed into law on 17 February, increasing fines for processing personal data in cases not provided for by Russian law. Fines for organisations have been increased from RUB 75,000 to RUB 100,000 (approx. €840 to €1,110). Legislators in the region were also active in reform with the Ukraine Ministry of Finance announcing a bill to bring Ukraine legislation into closer alignment with European requirements for electronic identification and electronic trust services. In addition, the Parliament of Ukraine ('Verkhovna Rada') announced that they had adopted a resolution to amend the rules for ensuring the protection of information in telecommunication systems. Finally, the Bank of Russia announced a public consultation for a roadmap to modernise the data model for banking reports.

March

The Legal Draftsman's Department of Sri Lanka released the final version of the draft data protection bill which underwent a number of amendments following a public consultation with various stakeholders and government bodies. In Japan, the Personal Information Protection Commission announced that the amendments to the Protection of Personal Information (Act No. 57 of 2003 as amended in 2015) ('APPI'), which mostly focus on data security procedures, will enter into effect on 1 April 2022. India's data protection bill continues to face delays with a motion in Parliament to extend the submission of its report on the bill. The New Zealand Parliament announced that a bill which would expand the scope of the Harmful Digital Communications Act 2015 is being considered by the Justice Committee. Additionally, the whistleblower bill to amend the Protected Disclosures Act 2000 is also being considered in Parliament.

Authorities in China, Indonesia, South Korea, and Singapore focused on issuing guidance on cybersecurity standards in information technology, the financial sector, as well as supply chain management. In enforcement action, the Ukrainian Parliamentary Commissioner for Human Rights ('the Commissioner') released the results of an inspection into a university for failures to make adequate plans for unauthorised access to data. Furthermore, the Commissioner took action against a bank's illegal processing of personal data. Additionally, authorities in China, Macau, Singapore, and South Korea levied fines against organisations for inadequate security measures, illegal data processing, AML/CFT failures, and illegal telemarketing activities.

Significant legal reform began in the region in March with the Russian State Parliament ('Duma') announcing the amendments to Russia's Law on Personal Data entering into effect on 1 March 2021. The amendments provide additional protection for personal data and expand the conditions for consent. Then, on 27 March 2021, the law which amends the administrative offences law in Russia, entered into effect introducing increased maximum fines for legal entities when processing personal data. Similarly, in Belarus, the National Information Centre announced that the amendments to the Code of Administrative Offences entered into effect, which included new sanctions for personal data violations. In addition, European Commissioner for Justice Didier Reynders and South Korea's Personal Information Protection Commission Chairperson Yoon Jong announced the conclusion of adequacy talks with a decision to be reached in the coming months.

After publishing amendments to the personal data law in Uzbekistan, the State Center for Personalisation under the Cabinet of Ministers clarified the impact of the data localisation requirements for social media platforms, noting that the rule applies only to information such as names, phone numbers, and passport information used by citizens to register on the network, not including any database containing posts, comments, and uploaded multimedia. Lastly, the Federal Market Committee of the Duma urged the adoption of a bill which would amend the Russian payment system law, enabling operators to simplify the identification process for customers. In their recommendation, the Federal Market Committee highlighted that the bill would help individuals to manage funds without increasing the risks associated with money laundering and terrorist financing.

What to look out for:

- Opinion from the EDPB on South Korea's adequacy decision
- Movement in relation to India's personal data protection bill and China's draft law
- CAC regulation in China on necessary scope of personal information on mobile internet apps enters into effect on 1 May 2021
- Australia's review of the privacy act – AG set to release a discussion paper
- Supplementary guidance from MDES in Thailand before enactment of PDPA on 27 May 2021

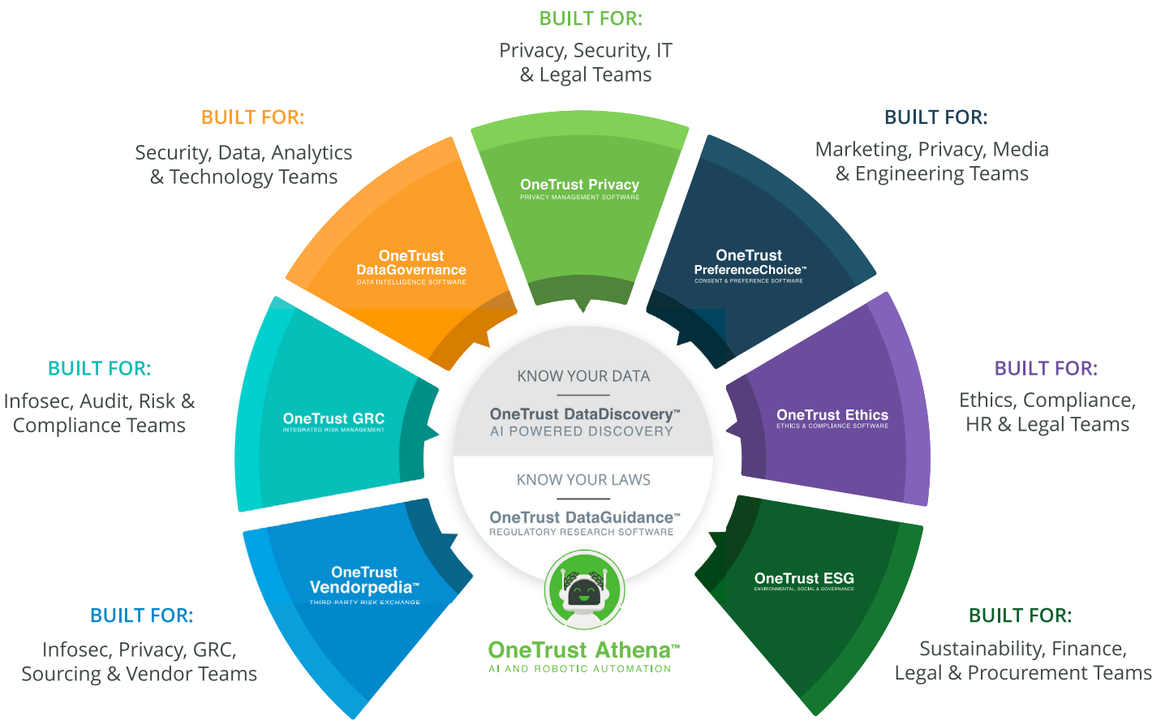
OneTrust

PRIVACY, SECURITY & GOVERNANCE

Make Trust a Competitive Advantage

The #1 Most Widely Used Platform to Operationalize

Privacy, Security & Data Governance



Trusted by 8,000 Customers, Both Big and Small

aetna™ Allianz Akamai Marketo ORACLE vevo Steelcase randstad

Interested in what OneTrust can do for your business?

REQUEST A DEMO

EMEA

Key takeaways:

- EDPB and EDPS publish opinions on draft SCCs
- Agreement on negotiating mandate on draft ePrivacy Regulation
- Increase in data breach reporting
- Legislative reform in ADGM, DIFC, and Zambia
- Draft UK adequacy decision

January

The European Data Protection Board ('EDPB'), together with the European Data Protection Supervisor ('EDPS'), published its joint opinions on the two sets of the European Commission's draft Standard Contractual Clauses ('SCCs'), which include one opinion on draft SCCs between controllers and processors ('the Controller-Processor SCCs Opinion') and one on the draft SCCs for the transfer of personal data to third countries ('the Third Country Transfer SCCs Opinion'). In particular, the Controller-Processor SCCs Opinion provides, with respect to the clause referring to data subject rights, further clarifications on, among other things, the title of the clause and the fact that the responses to data subjects shall be made in accordance with the controller's instructions. Moreover, the Third Country Transfer SCCs Opinion outlines and explains the main clauses addressed in the SCCs on, among other things, transparency, controller to controller transfers, the security of processing as well as documentation and compliance.

After the EU-UK Trade and Cooperation Agreement ('TCA') provisionally came into force, pending ratification by the European Parliament and the Council of the European Union, on 1 January 2021, a number of data protection authorities ('DPAs') across Europe published statements and opinions on the impact the same, for the most part, echoing sentiments outlined by the UK Information Commissioner's Office ('ICO'). Further, the ICO cautioned businesses to take sensible precautions for any eventuality and that any new UK adequacy regulations, SCCs, or ICO approvals of international transfer mechanisms must be put before the EU-UK Partnership Council.

As the impact of the COVID-19 pandemic continued to linger, DPAs in Europe increased regulatory scrutiny of the measures and legislation adopted in response. More specifically, in a second opinion on France's data processing operations in response to the COVID-19 pandemic, the French data protection authority ('CNIL') found deficiencies relating to, among other things, user authentication, the transition of data to unauthorised parties, as well as data security and management. Similar COVID-related investigations and reports were carried out in Ireland in response to a telecommunications company's use of geolocation data and in Denmark in relation to a sharing of personal information via a messaging application. In addition, with the vaccine rollout began in Europe, the Government in Greece set up research groups to investigate the creation of a digital vaccine passport. Ministers in Sweden and Denmark have also signalled similar efforts would be made by the summer of 2021. At the EU level the European Commission released its proposal

for a regulation on a framework for Digital Green Certificates which would facilitate free movement during the COVID-19 pandemic.

The Presidency of the Council of the European Union released, on 5 January 2020, its revised text of the proposed Draft ePrivacy Regulation. In particular, the Draft ePrivacy Regulation introduced modification to further align itself to the GDPR for consistency and legal certainty for users and businesses. Of note, the Draft ePrivacy Regulation introduces the possibility to process electronic communications metadata and to use processing and storage capabilities of terminal equipment and the collection of information from end-user's terminal for further compatible processing, in accordance with Articles 5(1)(b) and 6(4) of the GDPR. Furthermore, the ICO announced that it had resumed its investigation into the practices of the ad tech industry and specifically into how much sensitive personal data is collected without the consent of data subjects.

In other legislative reform, Spain's decree amending the Directive on Security Network and Information Systems (Directive (EU) 2016/1148) ('the NIS Directive') was published in its Official Gazette on 26 January 2021. Furthermore, Germany's amended unfair competition act entered into force on 19 January 2021.

Research into the uses and manipulation of artifical intelligence ('AI') tools continued to be a priority for regulators with the Spanish data protection authority ('AEPD') publishing guidance for managers who audit AI-related processing. Specifically, the guidance focused on, among other things, documenting the audited AI component and clear identification of responsibilities, in order to comply with the principle of proactive responsibility. Corresponding with its 40th anniversary, the Committee of Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ('Convention 108') adopted guidelines on facial recognition setting out reference measures for stakeholders when using facial recognition.

In Israel, the Privacy Protection Authority ('PPA') launched a public consultation alongside the Consumer Protection and Fair Trade Authority and the Competition Authority on a joint policy paper discussing the right to data portability. In particular, the paper recommends that a right to data portability should be provided for data subjects and outlines the benefits of the right and the procedures that can be put in place under the current Israeli privacy framework to ensure its facilitation. The PPA was also active in enforcement actions and announced the completion of its supervision procedures of the mental health clinics sector in Israel and the outsourcing and personal data management practices.

Data security became an increasingly important issue for regulators with both the Egyptian Ministry of Communications and Information Technology ('MCIT') and South African Information Regulator ('the Regulator') announcing a sharp increase in cybersecurity incidents. Specifically, Egypt's MCIT cited a 32% increase in incidents and in South Africa, the Regulator highlighted that it had seen an unprecedented number of data breaches in 2020. Zambia took an important step towards possibly becoming the next African nation with a comprehensive privacy law. The Data Protection Bill 2020 and the Electronic Communications and Transactions Bill 2020 were submitted to the National Assembly of Zambia and are currently being discussed. If passed, the Data Protection Bill will introduce responsibilities for data auditors and establish rules and exceptions for personal data processing.

February

Cross-border data transfers continued to be a priority with the European Commission addressing the topic in its trade strategy and highlighting that an open but assertive approach is needed. In particular, in assessing the TCA, the EDPS noted that the agreement failed to take account and incorporate the horizontal EU provision regarding cross-border data flows and personal data protection in the context of digital trade thereby creating uncertainty about the position of the EU in relation to data protection in trade. The long-awaited process, whereby the UK is declared an adequate country for data transfers began on 19 February 2021, when the European Commission published its draft UK adequacy decision. Data flows in the EEA and the UK remained safeguarded under the conditional interim regime of the TCA until 30 June 2021. In addition, the Council of the European Union announced that its Member States had agreed on a negotiating mandate for the ePrivacy Regulation. The Regulation, once adopted, will provide harmonised standards across the EU on areas such as cookies and similar technologies, direct marketing practices, metadata processing, and security within the Internet of Things. Furthermore, IAB Europe released its update guide on the post-third-party cookie era, which addresses, among other things, the impact of the depletion of third-party cookies on stakeholders and on digital advertising, the solutions that could replace the use of third-party cookies, and the suitability of said solutions for different businesses.

In enforcement, authorities in Poland, Denmark, Sweden, and Italy issued penalties for data breach notification failures, data security violations, and processing of personal data without consent. Notably, the Luxembourg CNPD outlined a shift in enforcement objectives towards motivating organisation to change culture as opposed to the current status of large GDPR fines as a deterrence for future violations.

Legislative reform took priority across the Middle East with the Dubai International Financial Centre ('DIFC') announcing the launch of a public consultation on the proposed amendments to the Data Protection Law No. 5 of 2020. The amendments focus on, among other things, procedural requirements for data controllers when handling data subject access requests and rules for when the Data Protection Commissioner is required to pay court fees for proceedings initiated by its office. The Abu Dhabi Global Market ('ADGM') announced the enactment of the Data Protection Regulations 2021, following a public consultation back in November 2020. Further to this, the ADGM Board also announced the appointment of Mr Sami Mohammed as the ADGM Commissioner of Data Protection to head the newly established Office of Data Protection for a term of four years. The ADGM highlighted that the regulations propose a 12-month transition period for current establishments and six months for new establishments. Furthermore, in Qatar, the Ministry of Transport and Communications ('MOTC') released guidelines on their privacy law which included guidance to support compliance with the law on, among other things, data breach notification, special nature processing, Data Privacy by Design and Default, direct marketing, and privacy notices.

Additionally, the Central Bank of the United Arab Emirates ('CBUAE') issued the Consumer Protection Regulation, as part of its Financial Consumer Protection Regulatory Framework and under its mandate to establish regulations for the protection of customers of licensed financial institutions. The CBUAE outlined that the Regulation is principled-based and provide guidance to the protection of consumer data and privacy. Lastly, the CBUAE announced final sanctions totalling AED 45,758,333 (approx. €10.3 million) to eleven banks operating in the UAE for failing to achieve appropriate levels of compliance in relation to AML and sanctions compliance frameworks.

After the conclusion of a public consultation, the South African Regulator published its Guideline to Develop Codes of Conduct pursuant to Section 65 of POPIA and announced the commencement of the POPIA Regulations issued under Section 112(2) of POPIA. In particular, the Regulator noted that the guidelines are to be used by all relevant stakeholders, including bodies and organisations, and outlined that they are divided into five parts which include code of conduct development, a complaints mechanism procedure, and reviewing procedures for codes of conduct. Moreover, the Regulator issued a standard and checklist for making and dealing with complaints alleging breaches of approved codes of conduct which comprised of eight general principles and requirements to govern the complaint handling by the responsible parties and independent adjudicators.

March

Negotiation for a new and enhanced EU-US Privacy Shield framework intensified in March with the EU Commissioner for Justice and US Secretary of Commerce reaffirming in a joint statement a common commitment to privacy, data protection and the rule of law, and mutual recognition of the importance of cross border data flows. The UK's ICO and the Secretary for the Department for Digital, Culture, Media and Sport agreed to a Memorandum of Understanding that acknowledges the roles both will play in carrying out adequacy assessments. The ADGM enacted, on 25 February 2021, its new electronic transactions regulation, giving electronic transactions equal legal effect as written records.

Cybersecurity continued to be of critical importance for regulators and legislators across the region. In its conclusion on the EU's cybersecurity strategy, the Council of the EU highlighted a number of actions including defining a joint cyber unit, supporting the development of strong encryption, and strengthening cooperation with international organisations. Moreover, the EDPS published its opinion on the Proposal for the Network and Information Systems 2.0 Directive, which is also part of the EU's cybersecurity strategy. In addition, authorities in Denmark, Latvia, and the Czech Republic issued guidance on employer obligations in relation to the processing of vaccine data of employees, access to vaccine information, as well as consent requirements.

In Ad Tech, a group of 40 privacy, antitrust, and consumer protection organisations formed a coalition calling on a ban on 'surveillance advertising.' Furthermore, CNIL published updated FAQs on its guidelines and recommendations on cookies and other trackers, which came into force 1 April 2021. Specifically, the FAQs cover general questions regarding the commencement of CNIL compliance audits from April 2021, the guidelines and recommendation's scope of application, audience measurement cookies, conditions for obtaining valid consent from users for the use of cookies, and the manner in which users should be able to opt-out from the use of cookies and other tracking mechanisms. Additionally, the EDPB published a statement on the Draft ePrivacy Regulation, welcoming the negotiation mandate reached by the Council of the EU on the protection of privacy and confidentiality in the use of electronic communication services and noted that the ePrivacy Regulation should complement and not *de facto* change the GDPR. However, the EDPB did express concern over the rules on confidentiality of electronic communications. Furthermore, the UK's ICO continued to focus efforts on regulating the processing of children's data online and urged business to make necessary changes to comply with their Age Appropriate Design Code.

In Africa, the Media Institute of Southern Africa Zimbabwe ('MISA Zimbabwe') underscored the need for a robust cybersecurity and data protection framework in Zimbabwe following the launch of the National Data Centre in Zimbabwe for the deployment of ICT at the government level. For enforcement in the EU, authorities in Italy, Poland, and the UK issued penalties for violations of the GDPR including data breach notification failures and spam text messages.

What to look out for:

- Adoption of the UK adequacy decision
- EU Member States implementation of the Whistleblowing Directive
- The EU's final proposal for Digital Green Certificates
- POPIA compliance deadline in South Africa approaching
- EDPB final guidance following Schrems II

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

Insights

Americas and Caribbean

- Argentina: Evolution of the data protection landscape
- Brazil: Government guides for LGPD compliance
- Brazil: The importance of cooperation between the ANPD and consumer protection authorities
- Panama: One week to go - is Panama ready to enforce data protection law?
- Quebec: Legal and technological developments in AI
- USA: Future of privacy legislation in 2021
- USA: Business associate liability under HIPAA
- USA: Harnessing AI in compliance with HIPAA
- Washington: People's Privacy Act introduces "significant shift" on consumer interaction

APAC and the CIS

- Australia: The News Media and Digital Platforms Mandatory Bargaining Code and its impact on privacy
- Australia: A peek into the dark web with the proposed new surveillance legislation
- China: The Draft PIPL and the GDPR - A comparative perspective
- China: CAC issues regulation on necessary scope of personal information on mobile internet apps
- China: Draft Data Regulations of the Shenzhen Special Economic Zone
- India: An overview of digital payments
- Indonesia: New regulatory framework for payment systems
- Russia: New consent requirements for data processing
- Singapore: PDPA reforms - Data protection enters a new phase
- South Korea: Proposed amendments and the reactive legislature strategy

EMEA

- ADGM: Data Protection Regulations 2021 and what they mean for businesses
- EU: EDPB issues guidelines on connected vehicles
- EU: The updated IAB Guide on the post third-party cookie era - changes and residual challenges
- EU - UK: Necessary, proportionate, and adequate - European Commission issues draft adequacy decision of UK
- EU: Council of EU agrees on finalised negotiating mandate of ePrivacy Regulation
- EU: EDPB adopts recommendations on adequacy assessments under the Law Enforcement Directive
- EU: EDPB and EDPS joint opinion on cross border transfer SCCs
- EU: European Commission's proposal for a new Data Governance Act
- EU: European Commission package on digital finance - harmonisation of internal policies and the technological neutrality principle
- Italy: Garante's new guidelines on cookies and similar tracking technologies - key takeaways
- Switzerland: Distributed ledger technology reforms
- South Africa: The development of codes of conduct under POPIA
- South Africa: The role and liability of an operator under POPIA
- South Africa: POPIA and the regulation of direct marketing
- UK: Brexit has transitioned – what next for GDPR, data transfers, EU Representatives?
- UK: Digital identity and attributes Trust Framework

International

- International: Comparing Virginia's CDPA with the CPRA and the GDPR
- International: Data protection is the answer to vaccine passports

Webinars

- Ad Tech and the Challenges of a Compliant Digital Strategy
- Comparing privacy laws: GDPR v. PIPA
- Know Your Laws: Japan's APPI
- On the Road to Privacy: Autonomous Vehicles and Privacy Compliance
- Panama's Personal Data Protection Law
- US Privacy Updates: Recent Developments at State and Federal Level
- UK Adequacy: The Future of Data Transfers
- Virginia CDPA Lands: What You Need To Know

Portals & Comparisons

- Retention Schedules
- Virginia Consumer Data Protection Act (CDPA)