aosphere
an affiliate of
ALLEN & OVERY

Privacy Developments Tracker

Thank you for requesting the Privacy Law Developments Tracker, a horizon scanning resource to help you identify and track key legislative developments. The Tracker is maintained and available as part of Rulefinder Data Privacy, an online legal solution from aosphere. We are pleased to share this sample version with you and invite you to find out more about Rulefinder Data Privacy by requesting a product demo or free trial here.

What is Rulefinder Data Privacy?

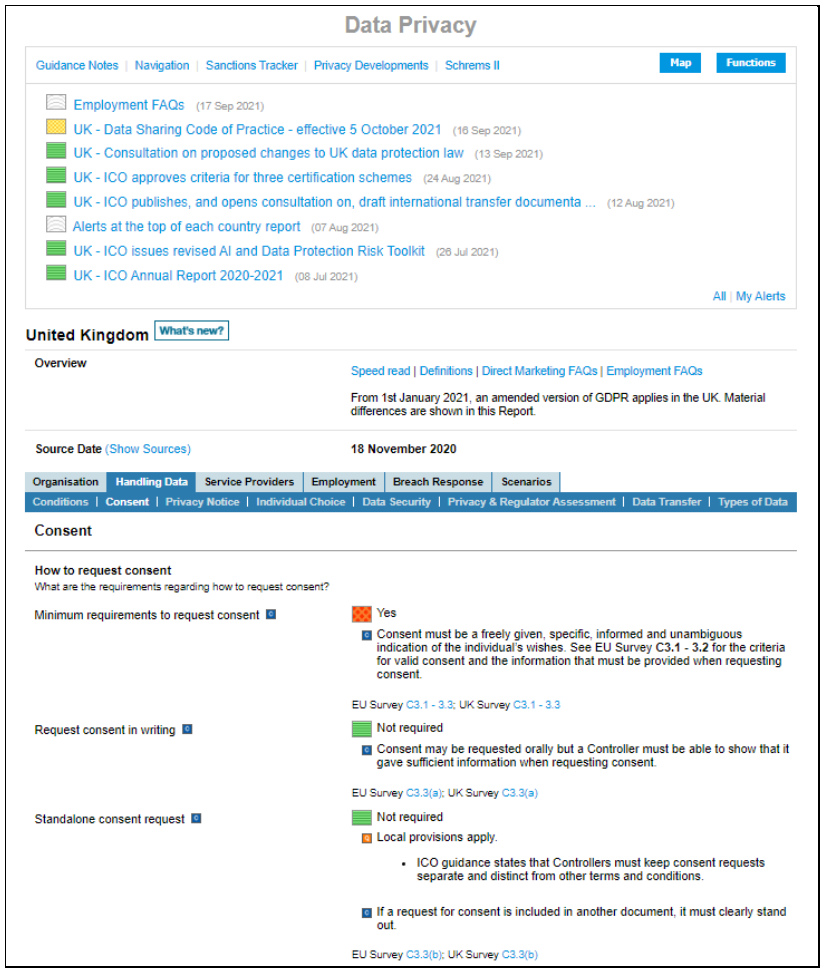
Rulefinder Data Privacy is an easy to use online resource that provides practical analysis of data privacy laws across key global markets.

The analysis is simple to access online, easy to navigate and maintained by a dedicated team of senior lawyers. As a part of the service, users can access:

- Daily Monitoring and Alerts.
- Links to underlying sources (memoranda from leading counsel, legislation and colour-coded reports).
- Territorial Scope and Compare feature that allows you to compare all data points across multiple jurisdictions and customise your own reports.
- Three dedicated "Trackers" provide access to an overview of Sanctions, Schrems II and Privacy Law Developments. The following pages provide an example of our Privacy Developments Tracker.

This Overview comprises selected information extracted from the Privacy Developments Tracker contained in Rulefinder Data Privacy. This document may not be shared outside of your organisation without the consent of aosphere LLP.

Sample screenshot from Rulefinder Data Privacy



Privacy Developments Tracker

Published: 14th September, 2021

The aosphere Privacy Developments Tracker is an overview of developments under data privacy related legislation covered in our Rulefinder Data Privacy Reports based on our daily monitoring of regulator websites and other sources including draft laws. The likelihood of a draft law being enacted varies significantly between jurisdictions. We therefore select items to follow and publish an updated tracker quarterly.

The tracker below contains various source links. Where there are numerous source links for a development we may not have included every link in this document. Full aosphere subscribers do have access to all the source links, as well as memoranda from leading counsel, legislation and colour-coded reports.

Jurisdiction	Region	Development	Type	Topic	Entry last updated	Links
Argentina	Americas	**New Data Protection Law** On 17 November 2020, a bill (6234-D-2020) was submitted to the Argentine Parliament proposing a new regime for the protection of personal data, replacing the existing laws relating to data protection and direct marketing (Laws 25326, 26343, 26951). The Bill follows, in many respects, the standards and provisions of the EU GDPR, including breach response and accountability obligations. It also incorporates concepts of biometric data and genetic data, and provides for the use of tacit consent for non-sensitive data. There is no indication of when this Bill will be considered in full by the Parliament. In light of the current economic climate in Argentina and the Covid-19 emergency, counsel does not expect that it will be considered soon and notes that the previous attempt at major data protection reform (much of which is replicated in the new Bill) lost parliamentary status due to other priorities.	Draft Law	data protection law breach response consent rights direct marketing sanctions sensitive data	Sep-21	Bills
Australia	APAC	**Participation in CBPRs System** In November 2018 APEC endorsed an application from Australia to participate in the Cross Border Privacy Rules (CBPRs) system. In order for the system to be implemented domestically, Australia must appoint an independent accountability agent which will assess whether participating businesses' privacy policies are consistent with the APEC Privacy Framework. Although Australia's attorney general had expressed an intention to work during 2019 to implement the CBPRs system, no progress was made. The Issues paper issued in the recent review of Australia's Privacy Act included a discussion of the costs and other challenges around implementing CBPR (see pages 54-62) and sought industry views on the challenges and benefits of doing so.	Expected development	international transfer	Sep-21	APEC CBPRs system website Issues Paper

Jurisdiction	Region	Development	Type	Topic	Entry last updated	Links
Australia	APAC	**ACCC Digital Platforms Inquiry** The Australian Competition and Consumer Commission (ACCC) carried out a Digital Platforms Inquiry concluding in 2019. The ACCC is focused on competition issues and consumer protection and concluded that existing regulatory frameworks have not held up well to the challenges of digitalisation, and that this is now a core focus for the ACCC. The Australian government indicated a desire to review the Privacy Act from 2020-2021 and to introduce a range of reforms strengthening consumer protections, increasing penalties, introducing a direct right of action and creating a binding online privacy code. Consultation and draft legislation implementing these reforms was scheduled to occur in 2020; however there have been no updates as yet.	Proposal	adtech consumers digital	Dec-20	Final report from the ACCC's Digital Platforms Inquiry ACCC Digital Platform Enquiry Page
Australia	APAC	**Review of the Privacy Act** The Attorney-General's Department conducted a public consultation in Q4 2020 on a review of the Privacy Act. Areas addressed include: • the scope and application of the Privacy Act; • whether the Privacy Act effectively protects personal information and provides a practical and proportionate framework for promoting good privacy practices; • whether individuals should have direct rights of action to enforce privacy obligations under the Privacy Act; • the impact of the notifiable data breach scheme and its effectiveness in meeting its objectives; • the effectiveness of enforcement powers and mechanisms under the Privacy Act; • the desirability and feasability of obtaining EU adequacy status and implementation of the APEC CBPR system; and • the desirability and feasibility of an independent certification scheme to monitor and demonstrate compliance with Australian privacy laws. The consultation generated a significant level of industry responses as well as from the OAIC and the Government is currently considering submissions received.	Consultation	data protection law rights international transfers codes of practice/certification	Sep-21	Issues Paper Terms of reference OAIC submission
Australia	APAC	**Review of OAIC Guide to Securing Personal Data** The Office of the Australian Information Commissioner (OAIC) opened a public consultation on its Guide to Securing Personal Data (the Guide). OAIC is seeking comments from interested stakeholders on: • how the Guide could be improved; • any additional topics or areas to include; and • whether the Guide provides adequate information on technical issues involving information security. The deadline for submissions was 12 March 2021.	Consultation	security	Mar-21	Guide to Securing Personal Data Consultation
Australia	APAC	**Consultation on Consumer Data Right rules** The Australian Government Treasury and the Data Standards Body have launched a consultation on the development of Consumer Data Right (CDR) rules and standards design papers. Currently, the CDR only applies to the banking sector. This consultation is part of extending the CDR to the energy sector, which would enable energy consumers to share their data and obtain the best offer that is available to them. The consultation closed on 26 May 2021.	Consultation	portability rights	Aug-21	Consultation#2 Consultation#1

Jurisdiction	Region	Development	Type	Topic	Entry last updated	Links
		Following the initial consultation, on 17 August 2021 the Australian Treasury published a consultation paper including draft CDR rules amendments (version 4) which would extend the CDR to the energy sector and also include minor amendments to ensure the rules operate as intended. The draft CDR rules and other proposals are open to public consultation until 13 September 2021.				
Australia	APAC	**Cross-Border Data Access Law passed** On 24 June 2021, the Australian parliament passed legislation establishing a framework for its enforcement agencies to access certain electronic data held by companies outside of Australia for law enforcement and national security purposes. The law paves the way for the establishment of a bilateral agreement with the United States under the U.S. Clarifying Lawful Overseas Use of Data (CLOUD) Act.	New Law Expected Law	International transfer	Jul-21	Telecommunications Legislation Amendment (International Production Orders) Bill 2021 Explanatory Memorandum
Bahrain	Middle East	**Effective Implementation of Data Protection Law** The Ministry of Justice, exercising temporary powers as data protection authority, has published the following draft orders which will finally provide substance to the high level data protection law (Law no. 30 of 2018) which took effect in August 2019: • 'Regarding the duties of the Data Protection Guardian' - setting out the formalities for appointment and duties of data protection officers. • 'Regarding the Data Subject Rights' - Strengthening consent requirements and prohibiting the use of cookie walls. • 'Regarding the conditions to be met in the technical and organisational measures that guarantee protection of data' - as well as setting out minimum technical security requirements this also specifies wider organisational requirements regarding employee training, data protection impact assessments, vulnerability assessment and penetration testing, transfers to external processors, and breach response obligations. The draft order also requires all data controllers to hold insurance issued by a Bahrain licensed insurance company. • 'With Respect to Public Directories' - setting requirements for the inclusion of personal data in publicly available directories. • 'With Respect to the Rules and Procedures of Data Processing' - setting requirements regarding DPA notification and authorisation for processing. • 'With Respect to the Rules and Procedures Governing Submission of Complaints Relating to Personal Data Protection' - dealing with the process for lodging complaints to the data protection authority. • 'With Respect to Sensitive Data Processing Procedures' - providing exemptions from the consent requirement for processing sensitive data, requirements regarding policies and records and authorisation of processing and providing for further rules to be published restricting cross-border transfer of sensitive data. • 'With Respect to States, Countries and Territories with Adequate Legislative and Regulatory Protection for Personal Data' - specifying the list of countries deemed adequate for transfers.	Draft Laws	consent data protection officer DPIA international transfer security regulator rights sensitive data	Sep-21	Draft regulations
Brazil	Americas	**Effective Implementation of Data Protection Law** The new data protection law (Law no. 13.709 of 14 August 2018) (**LGPD**) was signed into law with effect on 18 September 2020. The data protection authority (the **ANPD**) has been established and its board of directors were appointed in January 2021. The ANPD regulatory agenda for 2021-2022 designates a number of actions as priority, including: • Regulations for micro enterprises and small businesses; • Regulations on individual rights;	Expected development Consultation Proposal	regulatory agenda sanctions breach notification	Mar-21	ANPD regulatory agenda Press release and consultation on breach notification

Jurisdiction	Region	Development	Type	Topic	Entry last updated	Links
		• Regulations on administrative penalties for breach of the LGPD; • Guidance on breach notification including timing and form (see link for press release and public consultation); • Regulations on data protection impact assessments; • Guidance and supplementary rules on data protection officers; • Guidance on international transfers, including in relation to adequate recipients and the content of standard contractual clauses; and • Guidance for the public on various aspects of the LGPD, including legal bases for processing.				
Brazil	Americas	**Sanctions** The imposition of sanctions under the LGPD was postponed to 1 August 2021. However, the ANPD is still taking comments on and finalising the Regulation for Inspection and Application of Administrative Sanctions, including the methodology for calculating fines. The ANPD has clarified that it will start to impose sanctions after the approval by the ANPD Board of Directors of the Regulation for Inspection and Application of Administrative Sanctions and that such action may be taken in relation to facts occurring after August 1, 2021 including in relation to continuing offences initiated before that date.	Draft Law	sanctions	Sep-21	ANPD FAQs on Administrative Sanctions including draft Regulation
Brazil	Americas	**ANPD Consultation on Inspection Standard** Brazil's National Data Protection Authority (**ANPD**) announced on 28 May 2021 a 30-day public consultation on its proposed inspection standard. The consultation is the first to be carried out by the ANPD in accordance with the General Law for the Protection of Personal Data **(LGPD**) which requires the ANPD to consult and hold a public hearing before publishing its rules. A public hearing was held on 15-16 July 2021. The proposed standard establishes the intended inspection mechanism and makes provision for monitoring, guidance, preventative actions and the application of sanctions.	Consultation	sanctions	Jul-21	Consultation page Draft standard ANPD Press Release
Brazil	Americas	**Artificial Intelligence Bill** Brazil's Chamber of Deputies approved urgency rules for a bill establishing principles on the use of artificial intelligence. Bill 21/20 states AI use must be based on a respect for privacy, human rights, democratic values and cannot be discriminatory in nature. It also establishes principles around transparency. The proposal may be voted on during the next plenary session - date to be confirmed.	Draft law	AI	Jul-21	Press Release
Brazil	Americas	**Regulatory agenda 2021 - 2022** The ANPD has issued its regulatory agenda for 2021-2022, setting out its 10 priority projects. These include: • Data privacy for small and medium businesses • Establishment of norms for the Inspection and Sanctions Standard (see above) • Specification of data breach reporting and notification • Personal data protection impact assessment	Expected development	breach response privacy assessment sanctions	Aug-21	Announcement
Canada (Alberta)	Americas	**Consultation on modernisation of privacy laws** The Alberta government has consulted on modernising its privacy laws, with the intention that the input will *help to strengthen and modernise privacy protections and may contribute to new or updated policies, processes or legislation*. Consultation closed on 20 August 2021.See below for developments at a federal level and how other Canadian provinces are responding to the proposed federal changes.	Consultation	data protection law	Jul-21	Consultation survey

Jurisdiction	Region	Development	Type	Topic	Entry last updated	Links
Canada (British Columbia)	Americas	**Review of Data Protection Law** The 6-year statutory review of the British Columbia Personal Information Protection Act (**PIPA**) started in May 2020; as of June 2021 the Special Committee of the legislature which is carrying out the review is still receiving submissions. It has requested that these focus on the Bill and GDPR (see comments of the OIPC below). In June 2020, the Information and Privacy Commissioner for British Columbia (**BC OIPC**) filed a briefing paper with the Special Committee, calling for significant reform, based on the GDPR model. In February 2021, the BC OIPC filed a supplementary briefing paper, updating its recommendations to ensure that PIPA will be aligned where necessary with the proposed new federal CPPA (see above), and highlighting where BC OIPC's recommendations differ from CPPA. BC OIPC recommendations include mandatory data breach notification, obliging organisations to ensure service providers comply with the law, strengthening the requirement for informed consent, transparency of automated decisions, data portability and BC OIPC power to impose administrative fines.	Expected development	data protection law breach response service providers consent automated decision-making portability sanctions	Jun-21	BC OIPC Supplementary briefing paper February 2021 BC OPIC Speech February 2021 IPC Briefing paper June 2020
Canada (Federal)	Americas	**Proposed Regulation of AI** On 12 November 2020, the Office of the Privacy Commissioner of Canada (**OPC**) issued new recommendations for the regulation of artificial intelligence (**Recommendations**). The Recommendations follow a consultation conducted by the OPC in early 2020 and analyse how the challenges presented by artificial intelligence (AI) can be addressed in the reform of the Personal Information Protection and Electronic Documents Act 2000 (PIPEDA). The OPC calls for the amendments of the PIPEDA that would: • permit the use of personal information for new purposes towards responsible AI innovation and for societal benefits; • authorise these uses within a rights-based framework that recognises privacy as a human right; • create the right to a meaningful explanation of the basis for automated decisions and a right to contest these decisions, to ensure transparency, accuracy and fairness; • increase accountability obligations on businesses to demonstrate compliance with privacy requirements and establish privacy by design principles for AI systems; and • strengthen supervisory and enforcement powers of the OPC, including the right to issue binding orders and financial penalties.	Consultation	AI facial recognition	Dec-20	Press release
Canada (Federal)	Americas	**Modernisation of Data Protection Law** The Government of Canada has published a proposed new privacy law for the private sector. Public consultation closed on 14 February 2021. The Digital Charter Implementation Act, 2020 (**DCIA**) which includes the Consumer Privacy Protection Act (**CPPA**) would modernise the framework for the protection of personal information in the private sector including: • increased control and transparency; • data portability provisions; • rights to erasure; • providing the Privacy Commissioner (OPC) with broad order-making powers, including the ability to force an	Draft Law	consent portability erasure regulator sanctions transparency	May-21	Government of Canada Press release, which contains links to the Factsheet explaining the proposed law and the recent public consultation

Jurisdiction	Region	Development	Type	Topic	Entry last updated	Links
		organisation to comply and the ability to order a company to stop collecting data or using personal information; and • providing for the fines of up to 5% of revenue or $25 million, whichever is greater, for the most serious offences. The OPC will have the power to issue orders and make recommendations for administrative monetary penalties and a new tribunal will be established to levy these monetary penalties and hear appeals. In March 2021, the Office of the Privacy Commissioner (**OPC**) published its responses to the consultation, with recommendations on a range of topics including further provisions on automated decision-making and artificial intelligence. In May 2021, the OPC made a further detailed submission, setting out proposed enhancements to the DCIA including a rights-based approach, more specific obligations and wider scope for administrative fines, as well as improvements to provisions on international transfers.				OPC response to consultation March 2021 OPC submission May 2021
Canada (Ontario)	Americas	**Proposed Data Protection Law** Following initial consultation in Q2 2020, in June 2021, the Ontario government published a white paper for consultation on *Modernizing Privacy in Ontario,* outlining proposals to implement a new provincial privacy law, in light of concerns with the proposed new federal privacy law. Consultation closes on 3 August 2021.The proposals address artificial intelligence and automated decision-making, the need for consent and other legal uses of personal data, transparency and protection of vulnerable groups including children.	Consultation	data protection law	Jun-21	Government announcement August 2020 Consultation June 2021
Canada (Quebec)	Americas	**Proposed Data Protection Law** Quebec's National Assembly is considering Bill 64, an Act to modernise legislative provisions as regards the protection of personal information; the Bill 64 would update Quebec's data protection law (the Quebec PPIPS) and the Quebec IT Act. The Bill was reviewed at the Committee stage in February-May 2021.	Draft Law	data protection law	May-21	Bill (showing current status)
Chile	Americas	**Proposed Amendments to Data Protection Law** Chile currently has a limited data protection law. Draft Bill 11144-07 (merged with 1092-07) proposes a number of changes including: • new regulator • accountability principle • right to portability • restrictions on international transfers • new legal bases for processing for legitimate interests or to performance of a contract with the individual. • administrative sanctions for breach of the DPA, up to approx USD 700,000. The Bill was a priority piece of legislation and was passed by the Senate early in 2020; progress has been halted since 16 March 2020 due to the Covid pandemic. It is expected that the DPA Bill may be enacted in the next 12-24 months. The DPA Bill will come into effect 12 months after it is enacted, with an additional 6 months for existing databases to be brought into compliance with the new rules.	Draft Law	international transfer regulator sanctions portability conditions for processing legitimate interests	May-21	Progress of the DPA Bill
China	APAC	**Data Security Law** The Data Security Law was adopted on 10 June 2021 and will come into force on 1 September 2021. The Data Security Law introduces stricter requirements in relation to the processing of state critical data (i.e., data related to national security, economic security, important people's livelihood, or material public interest) and increases the penalties for non-compliance including fines of up to RMB 10 million, suspensions of operations, revocation of operation permits or business licences, sanctions for non-compliant transfer of 'important data' outside China and fines imposed on company officials directly responsible for violations. The Data Security Law will have	New Law	localisation data transfer sanctions	Jun-21	Data Security Law

Jurisdiction	Region	Development	Type	Topic	Entry last updated	Links
		extra-territorial reach, expand data localisation requirements to any organisations processing 'important data' (and not only to operators of critical information infrastructure) and impose requirements on entities to obtain authorisation for disclosure of data stored in China in response to requests of foreign judicial or law enforcement agencies.				
China	APAC	**Personal Information Protection Law** On 20 August 2021, China's National People's Congress Standing Committee voted to adopt the draft Personal Information Protection Law (PIPL), which will take effect on 1 November 2021. There is no transitional period set out in the PIPL. The PIPL represents China's first comprehensive data privacy law, and sets out relatively high level principles and obligations, which will sit alongside existing data privacy legislation such as the Cybersecurity Law and the Data Security Law. While the PIPL does not amount to a complete re-writing of Chinese data privacy law, it does create a clear legal framework with which personal data processing must comply. The key provisions include obligations relating to: extra-territoriality: the PIPL has extra-territorial effect and so will apply to certain instances of processing outside of China; • foreign data controllers: such entities will need to appoint a representative in China and register with the authorities; • international data transfers: there are increased (and prescriptive) restrictions on transfers of personal data outside of China; • assisting overseas authorities: personal data cannot be transferred to an overseas judicial or law enforcement agency without approval from competent authorities in China; • individual rights: these have been strengthened and broadened in scope; and • data protection officers: it will become mandatory to publish details of the DPO, and to register with the data protection authorities. Non-compliance may lead to fines of up to 5% of the annual turnover or RMB 50m (c.$7.5m) and persons directly responsible may also be subject to fines between RMB 100,000 (c.$15,000) to RMB 1m (c.$150,000).	New law	data protection law	Aug-21	Full text (in Chinese)
China	APAC	**Critical Infrastructure Data Security Regulations** China's State Council passed new legislation in August 2021 aimed at protecting the country's critical information infrastructure and increasing controls on domestic data. The Regulations on the Security Protection of Critical Information Infrastructure (which are formulated in accordance with China's Cybersecurity Law) come into effect on 1 September 2021, and are relevant to sectors such as telecommunications, finance, public services, e-government, national defence technology and science, transportation, and energy. Regulators for specific sectors will need to identify the critical operators within their sector, who will then be notified to the State Council's public security department. The regulations set out detailed obligations, including in relation to carrying out background checks on key employees, undertaking information security audits and risk assessments, and submitting to national network security reviews.	New Law	critical infrastructure	Aug-21	Full text (in Chinese)

Jurisdiction	Region	Development	Type	Topic	Entry last updated	Links
Denmark	Europe	**Marketing guidance** The Danish data protection authority (**Datatilsynet**) called for proposals for topics and issues to be addressed by its forthcoming guidance on processing of personal data in connection with marketing. The closing date for input was 15 August 2021. Datatilsynet initially intends that the guidance will address: • legal basis for processing, including consent and legitimate interests • data retention • individuals' rights to request access and deletion, and to object • profiling	Consultation	marketing	Jun-21	Call for input
European Union	Europe	**Draft AI regulation** In April 2021, the European Commission published its proposal for a regulation on a European approach for Artificial Intelligence (**draft AI regulation**). The draft AI regulation will now be considered by the Council of the EU and the European Parliament. It is likely that there will be prolonged discussions and further amendments before the regulation is finally adopted. Once finally adopted, the regulation will come into force 20 days after its publication in the Official Journal of the EU – and apply 24 months after that date. Key provisions of the draft AI regulation include: • harmonised rules for the placing on the market, the putting into service and the use of AI systems in the EU • prohibition of certain AI practices considered a threat to the safety, livelihoods and rights of individuals. e.g use of subliminal techniques to exploit individuals or manipulate their behaviour in a manner that causes physical or psychological harm (e.g. toys using voice assistance encouraging dangerous behaviour of minors) • specific requirements for high-risk AI systems and obligations for operators of such systems. • harmonised transparency rules for certain AI systems that take into account specific risks of manipulation they pose. e.g. AI systems that interact with individuals, detect emotions or generate or manipulate content • rules on market monitoring, surveillance and obligations for providers of high risk AI systems including informing national competent authorities about serious incidents, malfunctioning or recalls of AI systems from the market. Note: AI systems posing a minimal risk such as AI-enabled video games or spam filters are not covered by the draft AI Regulation. The European Commission highlights that the vast majority of AI systems fall into this category. In June 2021, EDPB and EDPS issued a joint opinion on the draft AI regulation, raising a number of criticisms and called for compliance with GDPR (and other EU law) to be a condition for marketing an AI system in the EU, for the prohibitions of social scoring by any organisation, of use of AI to infer emotions, to categorise individuals based on discriminatory bases using biometric data and of automated recognition of individuals in public.	Draft Law	AI biometric data automated decision-making	Jun-21	European Commission's webpage on AI policy including useful links to related documents Draft AI Regulation European Commission webpage on draft AI regulation

Jurisdiction	Region	Development	Type	Topic	Entry last updated	Links
European Union	Europe	**New Standard Contractual Clauses for international transfer** On 4 June 2021, the European Commission adopted modernised standard contractual clauses for international data transfers **(new SCCs)**, following consultation at the end of 2020. The new SCCs came into effect on 27 June 2021 and provide a basis for transfer of personal data to recipients outside the EEA. The previously adopted standard contractual clauses (**original SCCs**) remain in effect for contracts entered before 27 September 2021. Contracts entered after this date must incorporate the new SCCs. Contracts containing the original SCCs must be updated to incorporate the new SCCs by 27 December 2022 or earlier if there is a change in the relevant data processing activity.	New development	international transfer contracts	Aug-21	Standard Contractual Clauses for international transfers European Commission press release
European Union	Europe	**Collective Redress Mechanism** Directive 2020/1828 on Representative Actions for the Protection of the Collective Interests of Consumers (the Directive) came into force on 24 December 2020.Member states have until 25 December 2022 to transpose the Directive into national law, and an additional 6 months to apply it. So the new collective redress procedures should be available after 25 June 2023.Once implemented in national law, the Directive will enable qualified entities designated by EU Member States to seek injunctions and/or redress, including compensation, on behalf of a group of consumers that has been harmed by a trader who has allegedly infringed one of a number of specified EU law, including GDPR and the e-Privacy Directive (relevant to cookies and e-marketing). Currently consumer groups can only bring collective action where the relevant EU Member State law permits. The Directive will ensure consumer groups can bring collective actions across the EU, either within a single country or as a cross-border action.	New Law	sanctions compensation claims	Jan-21	Directive 2020/1828 Press Release of the European Parliament
European Union	Europe	**EDPB Guidelines on Examples regarding Data Breach Notification** The EDPB has adopted guidelines on examples regarding data breach notification. These guidelines were subject to consultation which closed on 2 March 2021. The guidelines set out examples of data breaches seen as most common by supervisory authorities, including ransomware attacks; data exfiltration attacks; and lost or stolen devices and paper documents. For each example, the guidelines present the most typical good or bad practices, advice on how risks should be identified and assessed, highlight the factors that should be given particular consideration, as well as inform in which cases the Controller should notify the SA and/or notify the individuals concerned.	Consultation	breach response	Jan-21	EDPB press release Guidelines
European Union	Europe	**E-Privacy regulation** A new draft e-privacy regulation was proposed by the European Commission in January 2017. This regulation was originally intended to apply from 25 May 2018 together with the GDPR and would replace the Privacy and Electronic Communications Directive (Directive 2002/58/EC). The new regulation aims to ensure the privacy and security of all data transferred via electronic means and strengthen rules on cookies and unsolicited electronic marketing. The EU Council agreed a draft regulation in February 2021, which is now subject to discussion with the European Parliament.	Draft Law	e-privacy cookies marketing	Mar-21	EU Council draft February 2021 EU Council press release February 2021 EU dossier

Jurisdiction	Region	Development	Type	Topic	Entry last updated	Links
		The EDPB and the German federal data protection authority have separately raised concerns that the draft regulation agreed by the EU Council for not providing sufficient protection for personal data and privacy.				
European Union	Europe	**NIS Directive** The European Commission has proposed a revised NIS Directive (**NIS 2 Directive**). The NIS Directive is a framework within which EU Member States implement local rules establishing security and notification requirements for operators of essential services and digital service providers. The NIS 2 Directive will replace the distinction between operators of essential services and digital service providers with categories of "essential" or "important" entities having different obligations. All medium and large companies in selected sectors will be included in the scope. Micro and small enterprises will be excluded, unless they are a sole provider of a service in the Member State, or provide certain electronic services. New sectors will be added to the scope of the Directive. New Cybersecurity risk management obligations will be introduced, along with harmonised sanctions including fines up to the higher of EUR 10 million and 2% of total worldwide annual turnover. At the end of January 2021, the Commission released a report summarising the outcomes of the 2020 consultation on the NIS Directive, which were used to draft the NIS 2 Directive. In March 2021, the EDPS published its opinion on the Cybersecurity Strategy and the NIS 2 Directive. The proposal is subject to negotiations between the Council of the EU and the European Parliament. Once the proposal is adopted, Member States will have 18 months to transpose the NIS 2 Directive.	Draft Law	NIS Directive critical infrastructure security breach response	Mar-21	European Commission page on the NIS Directive NIS 2 Directive Proposal A&O summary of NIS 2 Directive and EU Cybersecurity strategy
European Union	Europe	**Adequacy decisions** **South Korea**: The European Commission announced in March 2021 that it had successfully concluded discussions with South Korea's data protection authority for an adequacy decision covering transfers of personal data to commercial organisations and public authorities in South Korea. The European Commission will adopt a final adequacy decision once it has received approval from a committee of EU Member States. **US**: The European Commission and US Secretary of Commerce announced in March 2021 that negotiations have intensified on an enhanced EU US Privacy Shield that would be compliant with Schrems II. **Japan**: The EC Adequacy Decision for Japan is due for formal review in 2021. The European Commission review of all existing adequacy decisions is on-going. In March 2021, the European Parliament adopted a resolution on GDPR, emphasising the importance of adequacy decisions beyond the current 9 jurisdictions, but also reiterating its position that a country with a mass surveillance programme encompassing bulk data collection should not receive an adequacy finding.	Expected development	international transfer	Jun-21	Commission's webpage on Adequacy Decisions Commission Statement on South Korea adequacy decision Joint Statement on EU US Privacy Shield negotiations March 2021
European Union	Europe	**Digital Services Act** The European Commission published a draft regulation, the Digital Services Act (**DSA**) in December 2020. The DSA will address e-commerce and the handling of illegal or potentially harmful content. The DSA will also introduce transparency obligations in relation to online adverts and, for very large online platforms (45 million users or 10% of the population in the EU), in relation to parameters of algorithms used to offer content and options for modifying those parameters. The DSA is now subject to the ordinary legislative procedure and must be agreed by the European Commission, European Parliament and the Council of the EU. Once adopted, the DSA will apply directly in all EU Member States.	Draft Law	adtech online services	Feb-21	Commission's Digital Services Act webpage Draft Digital Services Act A&O blog on DSA

Jurisdiction	Region	Development	Type	Topic	Entry last updated	Links
		The EDPS published its opinions on the proposals for the DSA and DMA (see below) in February 2021, recommending additional measures to protect individuals.				
European Union	Europe	**Digital Markets Act** The European Commission published a draft regulation, the Digital Markets Act (**DMA**) in December 2020. The DMA will require certain large online platforms, designated by the Commission as gatekeeper platforms, to comply with certain prohibitions and obligations to avoid unfair practices. These include a prohibition on combining personal data sourced from core platform services with personal data from any other services offered by the gatekeeper or with personal data from third-party services, and from signing in end users to other services of the gatekeeper in order to combine personal data, unless the end user has consented. The DMA is now subject to the ordinary legislative procedure and must be agreed by the European Commission, European Parliament and the Council of the EU. Once adopted, the DMA will apply directly in all EU Member States. In June 2021, the European Commission published its preliminary findings from its sector inquiry into consumer Internet of Things. The potential competition concerns identified may contribute to the legislative debate on the Digital Markets Act.	Draft Law	online services	Jun-21	Draft Digital Markets Act A&O blog on DMA A&O blog on EDPS opinion
European Union	Europe	**European health data space** The European Commission has published its inception impact assessment of policy options for establishing a European Health Data Space (**EHDS**). Consultation on this assessment closed on 3 February 2021. The EHDS will provide a common framework across EU Member States for the sharing of health data (e.g. health records, patient registries and genomic data), with the objectives of: ensuring access for healthcare delivery, research and innovation, policy and regulatory activities; fostering a genuine single market in digital health services and products; and enhancing the development of trusted digital health services and produces including those using AI. The EHDS will set conditions for private organisations to participate. The European Commission has also published an assessment on Member State rules on health data in light of GDPR, highlighting issues regarding the fragmented approach to health data that need to be addressed to support the EHDS.	Expected development	health data	Feb-21	European Commission webpage EDPS Preliminary opinion on EHDS Digital Health Europe industry consultation on EHDS
European Union	Europe	**Data Governance Act** In November 2020, the European Commission published its proposal for the Data Governance Act, which aims to facilitate access to data and enable data sharing across sectors and Member States (both public and private sector data). In February 2021, the Council of the EU responded with its compromise proposal, including changes to clarify that the Data Governance Act will not create a new legal basis for processing personal data. The Act continues to be discussed and revised, and must be approved by both European Parliament and the Council of the EU before adoption. It will become effective 1 year after adoption, and organisations providing data sharing services will have a further 2 years to comply.	Draft Law	data transfer	May-21	Data Governance Act - Compromise proposal February 2021 EDPB & EDPS joint opinion on Data Governance Act - March 2021 European Parliament LIBE Committee

Jurisdiction	Region	Development	Type	Topic	Entry last updated	Links
		In March 2021, the EDPB and EDPS published a joint opinion on the Act, and in May 2021 issued a further statement reiterating its concerns and calling for consistency between the Act and GDPR. The EDPB is concerned that law-makers have not followed its advice to ensure that the Act is fully compatible with GDPR, does not weaken safeguards for individuals and does not create new legal bases for processing. In May 2021, LIBE Committee of the European Parliament issued an opinion recommending further changes.				opinion on Data Governance Act
European Union	Europe	**Guidelines on processing personal data for scientific research** The EDPB is currently preparing guidelines on processing personal data for scientific research, due for publication in 2021.	Expected development	health data research	Feb-21	
European Union	Europe	**ENISA Cybersecurity Certification Scheme for Cloud Services** ENISA published a draft version of a candidate European Cybersecurity Certification Scheme for Cloud Services (EUCS) on 22 December 2020. Public consultation closed on 7 February 2021. The EDPB has provided feedback on the scheme, in relation to potential synergies between EUCS and compliance with GDPR.	Consultation	security cloud	Mar-21	ENISA Cloud Services Scheme - draft EDPB feedback
European Union	Europe	**Guidelines on codes of conduct as tools for international transfers** EDPB has published for consultation guidelines on how codes of conduct may be adopted and used as a tool for international data transfer. Consultation will close on 1 October 2021.	Consultation	international transfer	Jul-21	Guidelines on codes of conduct as tools for international transfers
European Union	Europe	**EDPB Work programme for 2021 – 2022** On 16 March 2021, the EDPB published its work programme for 2021 and 2022. As part of this programme, guidelines are expected on • individual rights • children's data • processing for medical and scientific research purposes • compliance mechanisms • new technologies, addressing blockchain anonymisation and pseudonymisation, and social media platforms. • international transfers, including the role of codes of conduct (**see above**) and certification and disclosures required by foreign regulators or courts. EDPB has also indicated that it is in the process of updating its guidelines on the requirements for binding corporate rules to reflect the Schrems II decision (see EDPB Recommendations 01/2020 on Supplementary Measures).	Expected developments	individual rights children research compliance programme blockchain anonymisation pseudonymisation international transfer	Aug-21	EDPB Work Programme 2021-22
Finland	Europe	**Cookie Guidance** The Finnish Transport and Communications Agency (Traficom) has confirmed that it will update its guidelines on cookies to be in line with decisions made by the Helsinki Administrative Court establishing that it is not sufficient to rely on web browser settings to establish consent. Traficom will consult the Data Protection Commissioner with the aim of publishing revised guidelines during the summer of 2021.	Expected development	cookies e-privacy	Apr-21	Traficom press release Finnish Data Protection Commissioner press release

Jurisdiction	Region	Development	Type	Topic	Entry last updated	Links
France	Europe	**CNIL Cookie Enforcement Campaign** The CNIL has continued the enforcement stage of its cookie campaign, sending a further 40 formal notices to organisations breaching its guidelines. Recipients of the notices have until 6 September 2021 to comply. This is the second round of enforcement notices following the issuance of 20 notices in May, which mainly targeted digital organisations. Cookies are one of the priority areas for the CNIL's 2021 controls and cookie compliance may also come into focus for other data protection authorities as the privacy campaign group noyb has sent 560 complaints to companies in 33 countries including every EU state other than Malta and Liechtenstein.	Regulator focus	cookies e-privacy	Sep-21	CNIL Press Release noyb press release
France	Europe	**Consultation on logging measures to support security** The CNIL held a public consultation in July 2021 on its draft recommendation on logging measures to identify security incidents. It considers the logging of user identifiers, date and time of access and the device used, to be essential tools for ensuring security, ideally automatically analysed to detect issues. The draft recommendation includes guidance on the amount of data to retain and the duration of retention. The public consultation closed on 23 July 2021.	Draft Recommendation	security	Sep-21	Consultation
Germany	Europe	**Employee Data Protection Act** The Coalition Agreement of the current German Federal Government has convened an advisory board of external data protection and information technology experts to draft a separate Act for processing of employee data to implement the GDPR and repeal relevant provisions in the current data protection law (BDSG). The final report with concrete recommendations is expected in spring 2021.	Proposal	employees	Dec-20	
Germany	Europe	**Centralising German State Supervisory Authorities** There are ongoing political discussions on centralising the regulators for private commercial organisations into a single German Supervisory Authority. The proposal is supported by the Data Ethics Commission, an advisory body appointed by the Federal Government but opposed by German Supervisory Authorities. The Conference of the German State Economics Ministers (Wirtschaftsministerkonferenz) is reviewing two possible models for the centralisation: (1) from Federal State Supervisory Authorities to the Federal Data Protection Commissioner (BfDI); or (2) for the Federal States create a joint Supervisory Authority through a state treaty.	Proposal	regulator	Dec-20	
Germany	Europe	**Telecommunications Telemedia Data Protection Act** On 10 February, the German Federal Ministry for Economic Affairs and Energy adopted a draft law on data protection and privacy in telecommunications and telemedia (the Act). The Act has yet to pass the legislative process. The Act extracts data protection provisions from the existing Telemedia and Telecommunication Acts into a new Act, to the extent the provisions apply alongside GDPR and implement the e-Privacy Directive. It contains provisions on the confidentiality of electronic communications, the use of location data, cookies and similar technologies, requirements for cookie consents, technical and organisational security measures, and fines. In particular, the use of cookies and other identifiers requires consent; the Act however also recognises browser settings as valid consent and provides that consent is not required where using cookies/identifiers has been expressly agreed in a contract with the user to provide certain services.	Draft Law	e-privacy	Mar-21	The Act Press release of the federal government

Jurisdiction	Region	Development	Type	Topic	Entry last updated	Links
		The Federal Data Protection Commissioner will be competent for enforcement of the new Act against private commercial organisations processing personal data on electronic information or telecommunication services via public communications networks.				
Hong Kong SAR, China	APAC	**Proposed amendments to Data Protection Law** The Hong Kong Government and the data protection regulator (**PCPD**) are reviewing proposed amendments contained in a review of the data protection law (**PDPO**) published by the Constitutional and Mainland Affairs Bureau of the Hong Kong Government for discussion at the Legislative Council panel on constitutional affairs meeting on 20 January 2020. Key items proposed for amendment were: mandatory data breach notification; requirement for a data retention policy; obligations to be imposed on processors; to widen the definition of personal data to include "identifiable person" and enhanced PCPD powers to impose fines (linked to annual turnover), to carry out criminal investigations and prosecutions and to demand removal of malicious online contents. In July 2021, the Personal Data (Privacy) Amendment Bill 2021 was gazetted. This Bill contains proposed amendments focusing on malicious online content. Proposed new criminal offences include the publication of personal data without consent with intent (or being reckless) to threaten, intimidate or harrass, or cause psychological harm to, the individual or their family. The Bill also proposes new powers for the PCPD to prosecute offences under the PDPO and to investigate non-compliance with the PDPO generally (e.g. power to require materials or assistance, to search and seize materials at premises (with a warrant), to access to electronic devices (with or without a warrant) and to stop, search and arrest suspects) and power to demand the removal of malicious online content relating to a Hong Kong resident or other individual in Hong Kong.The Bill was formally introduced to the Legislative Counsel on 21 July 2021, and may go through a committee stage.It is possible that other amendments previously raised in 2020 (see above) may be introduced at a later stage of the legislative process.	Draft Law	breach response data retention processors sanctions	Jul-21	Proposal January 2020 Personal Data (Privacy) Amendment Bill - draft July 2021 with government briefing Government press release - July 2021
India	APAC	**Proposed New Data Protection Law** A draft Personal Data Protection Bill, 2019 (**PDP Bill**) was introduced in the lower house of the Indian parliament on 11 December 2019, and was referred to a joint committee of the Houses of Parliament. As a result of delays caused by the Covid-19 outbreak, the joint committee has been granted a number of extensions, and is now expected to report to the in the first week of the winter session, which usually starts around the last week in November. The PDP Bill (as originally drafted) proposes significant changes including: • extension of the territorial scope of the laws • introduction of general principles for processing, including lawfulness, fairness, purpose limitation, data minimisation, transparency, data accuracy and retention • specific requirements for obtaining consent • requirements for data protection officers • introduction of privacy by design obligations and privacy impact assessments • further individual rights (including the right to data portability) • changes to the data breach notification requirements • new rules on international data transfer It is expected that the bill will undergo significant change as a result of the joint committee review.	Draft Law	breach response consent data protection officer data protection law data retention data minimisation data quality fairness international transfer privacy by design privacy assessment rights sanctions scope	Jul-21	PDP Bill (as introduced in the Lok Sabha)

Jurisdiction	Region	Development	Type	Topic	Entry last updated	Links
Ireland	Europe	**Consultation on collection and use of children's personal data** On 18 December 2020, the Data Protection Commission published the Fundamentals for a Child-Oriented Approach to Data Processing, which provides guidance and recommendations on how to process children's personal data safely. The Fundamentals were subject to public consultation until 31 March 2021; the final form is yet to be published.	Consultation	children	Sep-21	Press release with consultation document
Israel	Middle East	**Regulator Recommendations on the Appointment of Privacy Protection Officers** On 29 October 2020, the Israeli Privacy Protection Authority (PPA) published recommendations on the appointment of privacy protection officers for public consultation on the matter. Israel's law does not include a general requirement to appoint a data protection officer but the PPA recommends appointment as best practice. The recommendations issued for consultation are open for public consultation until noon on 29 November 2020; they will provide guidance on the functions of privacy protection officers, their areas of expertise and functions, and necessary training.	Consultation	data protection officer	Dec-20	
Israel	Middle East	**Review of the Privacy Protection Act** The Ministry of Justice has opened a public consultation on the Privacy Protection Act, 5741-1981 (PPL) aimed at identifying which areas of the law require change, update or addition. The Ministry highlights that, given the significant changes in technology, economics and worldwide privacy landscape since the PPL was enacted in 1981, it is considering whether the law remains fit for purpose and which areas of the law require comprehensive amendments. Specific areas highlighted by the Ministry for review in its consultation document include additional lawful bases for processing and expanded rights for individuals.	Consultation	data protection law conditions for processing rights	Dec-20	Press Release with Consultation Document
Israel	Middle East	**Consultation on Data Portability** Israel's Privacy Protection Authority (PPA) and other government agencies have published a policy paper which sets out the main considerations for the adoption of a right to data portability in Israel. The policy paper recommends adopting a general right of data portability of personal information in Israeli law, which would include giving citizens the opportunity to have their information securely sent to them online in a readable format at no additional cost.The consultation is open until 24 January 2021.	Consultation	data portability	Jan-21	Press release with consultation document -
Israel	Middle East	**Consultation on guide for Privacy Impact Assessments** Israel's Privacy Protection Authority (PPA) has issued a guide containing recommendations on how to conduct a privacy impact assessment - for public consultation. Consultation closes on 30 September 2021.	Consultation	privacy assessment	Aug-21	Press release with Consultation Document
Italy	Europe	**Online Services: Minors** The Garante announced in January 2021 that it will be examining social media network practices in relation to children, in particular with respect to age verification of children accessing the platforms. The Garante had already been making enquiries as to the practices of various platforms regarding minors; this announcement came after the death of a 10-year-old child using social media. Other issues highlighted by the Garante are the degree of protection for minors, transparency, clarity in user information and the use of default settings. A working group on the protection of children's rights in the context of social networks and digital products on the net has also been established by the Ministry of Justice.	Regulator Focus	consent children digital online services	Sep-21	Garante Press Release Jan 21 Statement of the First meeting of the technical table on the protection of children's rights in the context of social networks and online digital products

Jurisdiction	Region	Development	Type	Topic	Entry last updated	Links
Japan	APAC	**Amendments to the APPI** Changes to the opt-out procedure under APPI amendments passed in May 202 will take effect in stages. From 1 October business operators will need to provide additional information to the PPC and to notify the PPC if they stop providing personal data under the opt-out regulations.	New Law	data transfer	Jun-21	PPC Press release -
Malaysia	APAC	**Amendments to the PDPA** The Malaysian data protection authority (PDPC) is in the process of reviewing the Personal Data Protection Act. In particular, the review focuses on: processor obligations; data portability; appointing a data protection officer; breach reporting; consent requirements and withdrawal of consent; international transfers; privacy by design; establishment of a Do Not Call registry; individual information rights; civil claims; technology and security measures; exemptions for business contact information; disclosure to regulators; registration with the PDPC; territorial and material scope; direct marketing; and cloud computing. The consultation closed in March 2020. There has been no further information as to the status of the consultation or the timeline for tabling amendments to Parliament.	Consultation	breach response consent cloud data protection law international transfer marketing portability privacy by design processors rights security territorial scope	Jun-21	
Mexico	Americas	**Right to Erasure** Amendments to the Mexican Data Protection Law have been proposed by the Senate to incorporate an erasure right particularly in relation to online services. As of May 2021 the amendments had not been passed.	Draft Law	erasure	May-21	
Mexico	Americas	**National Register of Mobile Phone Users** In April 2021, the Federal Telecommunications and Broadcasting Law (LFTR) was amended to create the National Register of Mobile Phone Users. This Register requires cellphone companies to gather customers' identification and biometric data (e.g. fingerprints or eye scans) allegedly needed to fight crimes such as extortion and kidnapping that frequently involve the use of mobile phones. Mobile phone companies have 2 years to collect the data and make it available to the government. If customers fail to register once the term expires, their line will be cancelled. The creation of the registry remain in effect but several organisations and individuals have challenged the amendment to the LFTR and recently, a Mexican federal judge granted an injunction against the part of the law that provides that anyone refusing to submit data would lose phone access.	New Law	telecoms	Jun-21	LFTR
New Zealand	APAC	**Proposed national data portability program** The New Zealand government has decided to introduce a "consumer data right" that would enable consumers to securely share data that is held about them with trusted third parties in a machine-readable format. The consumer data right will be rolled out on a sector-by-sector basis. A bill to implement the consumer data right will be introduced to Parliament in 2022 and will need to go through the bill drafting process, further consultation and legislative process.	Proposal	portability	Jul-21	Ministry web page on proposed consumer data right
Norway	Europe	**Implementation of NIS Directive** The NIS Directive is expected to be implemented. However the current legislation (including the Norwegian Safety Act) is assumed to already contain most of the requirements in the NIS Directive. There is at present no clear timeline for when the NIS Directive is to be implemented.	Expected development	NIS Directive critical infrastructure	Dec-20	

Jurisdiction	Region	Development	Type	Topic	Entry last updated	Links
Philippines	APAC	**Participation in CBPR System** In March 2020 APEC endorsed an application from the Philippines to participate in the Cross Border Privacy Rules (CBPR) system. In order for the system to become fully operational in the Philippines it must appoint an independent accountability agent which will assess whether participating businesses' privacy policies are consistent with the APEC Privacy Framework. The Philippines' data protection authority (NPC) must now appoint an accountability agent in order for the system to become operational.	Expected development	international transfer	Dec-20	APEC CBPRs system website
Philippines	APAC	**Amendments to the Privacy Laws** In 2019, two bills were proposed to amend the Data Protection Act: The following bills seeking to amend the DPA have been filed: House Bill 1188, which seeks to increase the penalties for violations of the DPA and House Bill 5612, which seeks to amend the territorial scope of the DPA; introduce additional conditions when Sensitive Personal Information may be processed; enhance individual rights; make breach notification mandatory within 72 hours; and enhance NPC enforcement powers. In February 2021, the Committee approved a new bill to substitute House Bills 1188 and 5612. We have not yet seen a draft of this substitute bill.Based on comments made by the Privacy Commissioner at a conference in June 2021, we understand that the substitute bill was approved by the House of Representatives - Committee on Information and Communications Technology, on 4th February 2021, and that key provisions of the substitute bill include: • Redefining "sensitive personal information" to include biometric and genetic data, and political affiliation. • Clarification on extraterritorial application of the DPA by specifying clear instances when processing personal data of Philippine citizens and/or residents is concerned. (i.e., offering of goods or services, or monitoring of behavior within the Philippines or when the entity has a link with the country) • Define the digital age of consent to process personal information to more than 15 years, applicable where information society services are provided and offered • Inclusion of performance of a contract as a new criterion of the lawful basis for processing of sensitive personal information. • Allowing Controllers outside of the Philippines to authorize Processors in the country to report data breaches to the Commission on behalf of the Controller. • Modifying criminal penalties under the DPA, giving the proper courts the option to impose either imprisonment or fine upon its sound judgment. • Senate Bill 1446, which seeks to amend the scope of the application of the DPA during times of national health emergencies and pandemics. This has been pending before the Committee of Science and Technology since 4 May 2020.	Draft Law	rights sanctions	Jun-21	House Bill 1188 House Bill 5612 Senate Bill 1446
Philippines	APAC	**Circular on administrative fines** The data protection authority for the Philippines **(NPC)** has published a draft circular on administrative fines for non-compliance with the Data Privacy Act **(DPA)** by private sector controllers and processors. The related NPC press release explains the rationale behind the level of fines proposed. The draft circular is subject to public consultation, closing on 25 June 2021. Once it is finalised, the NPC will be able to impose administrative fines. Under the draft circular, administrative fines would range between 0.5% to 5% of an organisation's annual gross income. No maximum limit is proposed, in contrast to the 5 million peso (approx €85,000) maximum for criminal penalties under the DPA.	Consultation	sanctions	Jun-21	Draft Circular NPC press release Announcement of extension of consultation to 25 June 2021

Jurisdiction	Region	Development	Type	Topic	Entry last updated	Links
Poland	Europe	**Regulation of electronic communications services** As part of implementing the European Electronic Communications Code, the Polish government has proposed a new draft Electronic Communication Law. This will consolidate and replace the current Telecommunication Law (which regulates cookies and using automated call systems for direct marketing) and will also affect the law that regulates e-marketing (PSEM).	Proposal	marketing cookies	Dec-20	Latest status of the proposal
Russia	Europe	**Amendment to Personal Data Protection law** In September 2019 the Ministry of Communications suggested a set of amendments to the Personal Data Law which, amongst other things, introduces the concepts of "depersonalised data" and "depersonalised personal data" generally corresponding to the concepts of anonymised and pseudonymised data; and sets out basic principles and rules for processing of depersonalised personal data. The draft federal law has not been introduced to the Russian State Duma.	New Law	anonymisation	Sep-21	regulation.gov.ru/projects#npa=95069 (Draft federal law)
Singapore	APAC	**Further changes to the Do Not Call provisions** In 2018, the PDPC organised a public consultation on managing unsolicited marketing messages. This included proposals to reduce the period for organisations to effect a withdrawal of consent to receiving marketing messages from 30 calendar days to 10 business days. These changes were not included in the major changes made to Singapore data protection law in 2021. It is now not known if or when these proposed changes will be made.	Proposal	marketing	Dec-20	
Singapore	APAC	**Amendment to Data Protection Law** On 1 February 2021, a number of changes to the Personal Data Protection Act and the Spam Control Act came into effect (as reflected in the latest Singapore Survey). Further changes are to come into effect at a future date (yet to be announced), in respect of data portability and an increase of the maximum fine to 10% of annual turnover in Singapore. The increase in fines is not expected to take effect until 2022.	New Law	portability sanctions	Feb-21	Amended Personal Data Protection Act Press release
South Africa	Africa	**Code of Conduct for Banking Association South Africa** The Information Regulator issued a code of conduct under Chapter 7 POPIA following a request from the Banking Association South Africa (BASA). The Code outlines specific processing practices which demonstrate how the conditions for the lawful processing of personal information will be applied by BASA member banks subject to POPIA.	Consultation	codes of practice/certification	Sep-21	Banking Code of Conduct
South Korea	APAC	**PIPC consultation on personal information security measures** On 13 November 2020, the Personal Information Protection Commission (PIPC) announced a public consultation on the consolidated version of the notice establishing security standards for personal information and on the organisational and technical measures for protection of personal information. The consultation closed on 23 November 2020. On 31 August 2021, the PIPC announced a further consultation of the standards for technical and administrative protection of personal information, which closed on 6 September 2021.	Consultation	security	Sep-21	Press release about November 2020 consultation Draft Standards Press release August 2021

Jurisdiction	Region	Development	Type	Topic	Entry last updated	Links
South Korea	APAC	**PIPC consultation on amendments to PIPA** The data protection authority for South Korea **(PIPC)** has published draft amendments to the Personal Information Protection Act 2011 **(PIPA)** for public consultation. The consultation closed on 16 February 2021. The proposed amendments include: • clarifications on pseudonymised personal data; • specific requirements for CCTV/video surveillance, drones and autonomous vehicles; • for individuals, a right of data portability and rights in relation to automated decision-making; and • tighter restrictions on data transfers out of South Korea, including the possibility of suspending non-compliant transfers. The PIPC published further proposals in May 2021, intended to enable self-regulation in the area of data protection and introduce a personal information management agency to facilitate the exercise of individuals' rights.	Consultation	automated decision-making international transfer portability pseudonymisation video surveillance autonomous vehicles drones	May-21	PIPC consultation February 2021 (Korean language only) PIPC proposals May 2021
South Korea	APAC	**PIPC Consultation on amendments to pseudonymised data notice** The PIPC has published amendments to its notice on pseudonymised data, aimed at clarifying proper pseudonymization practices and simplify the ability to export pseudonymous data. Consultation closed on 23 August 2021.	Consultation	pseudonymisation	Aug-21	PIPC press release with link to consultation document
Switzerland	Europe	A revised Swiss Data Protection Act (new DSG) was passed by the Swiss legislature on 25 September 2020; its provisions are reflected in the Rulefinder Data Privacy report. The new DSG is to be supplemented by the Data Protection Ordinance (DPO) providing detail on matters including minimum security requirements, details of information obligations, breach notification requirements, exemption from the obligation to maintain records of processing activities. The DPO is currently under consultation until 14 October 2021. The revised DPA and DPO are expected to take effect in the second half of 2022, at a date to be set by the Federal Council. Simultaneously with the entry into force of the new DSG, Switzerland will also ratify the modernised data protection convention 108 of the Council of Europe Below are some of the key changes: • The territorial scope of the Swiss regime is expanded to cover processing activities outside of Switzerland that take effect in Switzerland and controllers located outside Switzerland will be required to appoint a local representative. However, unlike the current law, the new DSG will not protect data relating to legal entities. • The new DSG will preserve the ability to transfer personal data outside Switzerland to adequate jurisdictions; the Federal Council will issue binding adequacy decisions replacing the current list of assessments made by the regulator (FDPIC). The draft DPO sets out the criteria according to which the Federal Council will assess the adequacy of other countries' data protection laws. Transfers made on the basis of approved standard contractual clauses will no longer need to be notified to the FDPIC. The new DSG also enables transfers to be made for foreign regulatory proceedings before administrative authorities (rather than only courts). • Controllers will need to provide more information to individuals including in relation to automated decision-making and where transferring personal data to non-adequate countries. The draft DPO sets out further detail on the format and method by which to provide information. • Individuals will have increased rights in relation to their data; much of the detail on how to comply, including time limits, is contained in the draft DPO. • Controllers will have wider documentation and governance processes requirements including a requirement to maintain records of processing activities and to carry out a data protection impact assessment for high risk processing activities. The draft DPO provides for organisations with 250 employees or less to be exempt from the requirement to maintain records of processing activities.	New Law	breach response data protection law international standard privacy assessment sanctions territorial scope	Sep-21	FDPIC Summary of key Changes (German) FDPIC Summary of key Changes (Italian) FDPIC Summary of key Changes French)

Jurisdiction	Region	Development	Type	Topic	Entry last updated	Links
		• Minimum security requirements will apply as specified by the draft DPO. • There will be a mandatory breach notification obligation; details of the information to be provided to FDPIC and to affected individuals are set out in the draft DPO. • Breaches may result in the responsible individuals being fined up to CHF 250,000; companies will be fined only in limited circumstances.				
Switzerland	Europe	**Critical Infrastructure** The Federal Department of Finance has been tasked with preparing a consultation draft setting out a reporting obligation for operators of critical infrastructure in the event of cyber attacks and the discovery of security vulnerabilities. The draft is to cover designation of a central reporting office for all sectors, the criteria and time limits for reporting and is to be completed by the end of 2021.	Proposal	breach response critical infrastructure	Mar-21	Federal Council Press release
Taiwan, China	APAC	**Participation in CBPR System** In December 2018 APEC endorsed an application from Taiwan, China to participate in the Cross Border Privacy Rules (CBPR) system. In order for the system to become fully operational in this region it must appoint an independent accountability agent which will assess whether participating businesses' privacy policies are consistent with the APEC Privacy Framework. The National Development Council (NDC) noted in its announcement of the APEC endorsement that it could now initiate the process of assigning an accountability agent but there has been no news of progress since then.	Expected development	international transfer	Dec-20	APEC CBPRs system website
Taiwan, China	APAC	**Children's personal data** A draft legislative proposal focusing on the protection of children's personal data on the internet was proposed to the Legislative Yuan (Congress) for deliberation in March of 2020. There is not yet a clear timeline as to when the legislation will be passed into law.	Draft Law	children	Dec-20	
Taiwan, China	APAC	**Amendments to the PDPA** The PDPP Office proposed amendments to the PDPA which is under review by the National Development Council. The proposed amendments include: • establishing an independent personal data protection agency; and • abolishing the distinction between "collection," "processing," and "utilization" of Personal Data as provided under the current PDPA. The amendments, if passed by the legislature, would be in addition to the current PDPA unless it otherwise overrides certain provisions of the current PDPA.	Draft Law	regulator	Dec-20	
Thailand	APAC	**New Data Protection Law** Thailand's Personal Data Protection Act B.E. 2562 (2019) (**PDPA**) took effect in May 2020. For most types of business the deadline for compliance is 31 May 2021. Secondary legislation and further guidance is being prepared on: obtaining consent; privacy notice; security measures; international transfer; record of processing activities; access requests; reporting data breaches; appointment of data protection officers; complaints and enforcement. In February 2021, the Ministry of Digital Economy and Society (MDES) published the outcome of a public hearing	Draft Law	data protection officer international transfer security consent privacy notice access requests register of activities enforcement	May-21	DES update February 2021 Public hearing - proposals and responses Royal Decree No 2

Jurisdiction	Region	Development	Type	Topic	Entry last updated	Links
		on this secondary legislation. Public consultation closed on 28 February 2021. On 5 May 2021, MDES requested and Cabinet approved a draft royal decree proposing a second postponement to the enforcement of the PDPA that applies to a wide range of organisations (see Thailand Survey Part I). Royal Decree No.2 was confirmed and published in the Royal Gazette shortly afterwards and the PDPA will now be fully enforceable from 1 June 2022 onwards. The reasons given by the MDES and Cabinet for the further postponement are the impact of the Covid-19 pandemic on organisations in Thailand and that the Personal Data Protection Committee (PDPC) has yet to be established.				
Turkey	Middle East	**Proposal to align with GDPR** In April 2021, the Ministry of Justice published a Human Rights Action Plan including certain amendments to be made to the Data Protection Law, to align it with the EU GDPR. Action should be taken to introduce these amendments by April 2022.	Expected development	data protection law	Jun-21	Press release
UAE (DIFC)	Middle East	The data protection authority for the DIFC has launched a consultation on updated guidance materials for international transfers. Consultation closes on 26 September 2021. The draft updated materials include: • revised data export handbook • revised data export standard contractual clauses • standards and process for adequacy decisions • approval process for binding corporate rules • ethical data management risk index tool and methodology for international transfers	Consultation	international transfer	Sep-21	Consultation document Commissioner page on international transfer including all draft guidance
United Kingdom	Europe	**Draft direct marketing code** The ICO published a draft direct marketing statutory code for consultation which closed in March 2020.	Consultation	marketing	Dec-20	Draft marketing code
United Kingdom	Europe	**NIS Regulations** Following consultation in May 2020, the UK Government called for views on proposed amendments to the NIS Regulations, in September 2020. The proposed amendments include an express requirement that notification of security incidents to the relevant Competent Authority or the ICO must be in writing. The UK Government has published its response to consultation on 9 November 2020. In July 2021, the UK Government issued a further consultation on setting the thresholds for the reporting of incidents by digital service providers - proposing that thresholds be set by ICO guidance. This consultation closed on 27 August 2021.	Proposal	critical infrastructure	Jul-21	Details of the September 2020 consultation July 2021 consultation
United Kingdom	Europe	**Statutory guidance on regulatory action** The ICO published an updated version of statutory guidance on how it will exercise its enforcement powers under the DPA. Consultation closed on 12 November 2020. Final guidance is to be published in 2021.	Consultation	sanctions	Dec-20	Draft statutory guidance and consultation

Jurisdiction	Region	Development	Type	Topic	Entry last updated	Links
United Kingdom	Europe	**Data Sharing Code** The ICO published the final data sharing statutory code of practice in December 2020 (**Code**). The Code was laid before Parliament on 18 May 2021, and will come into effect after it has been laid before Parliament for 40 sitting days (expected by approx end July/August 2021).The Code applies to all forms of sharing between controllers, including routine and one-off sharing. It does not apply to sharing Personal Data processors or within the same organisation. See our alert of 21 December 2020 for detail on the content and significance of the Code.	New Code of Practice	data transfer children	May-21	Data Sharing Code of Practice ICO Data sharing information hub Laid before Parliament on 18 May 2021
United Kingdom	Europe	**Guidance on anonymisation and pseudonymisation** In its blog in March 2021, the ICO announced that it will be updating its guidance on anonymisation and pseudonymisation (last updated before GDPR came into effect). The key topics to be addressed in the new guidance will be: legal framework, identifiability and re-identification risk; pseudonymisation techniques and best practices; governance requirements; research; the role of privacy enhancing technologies in data sharing; technical solutions and data sharing options and case studies. The ICO will publish and ask for views on each chapter of the guidance before the main public consultation. In May 2021, the ICO published for consultation the first chapter of its draft guidance on anonymisation, pseudonymisation and privacy enhancing technologies. Consultation closes on 28 November 2021.	Consultation	anonymisation pseudonymisation	May-21	ICO blog - announcement First chapter consultation
United Kingdom	Europe	**Employment practices - call for views to inform new guidance** The ICO plans to replace its existing employment practices code and supplementary guidance (which has not been updated since GDPR came into force). To inform this project, the ICO is seeking input from relevant stakeholders in a survey that asks broad, high level questions on the topics, changes in data protection law and other developments that should be covered and case studies or scenarios that should be included. Survey responses must be provided by 21 October 2021.	Consultation	employees	Aug-21	Consultation survey
United Kingdom	Europe	**Adequacy regulations - priorities** The UK Government's Department of Digital, Culture, Media & Sport (**DCMS**) has announced that it will be prioritising striking data adequacy partnerships (including adequacy decisions for international data transfers) with Australia, Colombia, Dubai DIFC, Singapore, South Korea, and the US. Future partnerships with India, Brazil, Kenya and Indonesia will also be prioritised in the longer term.	Proposal	international transfer data protection law	Aug-21	DCMS press release DCMS - UK approach to adequacy decisions
United Kingdom	Europe	**Consultation on proposed changes to UK data protection law** The UK Government has launched a consultation on proposed changes to UK data protection law. Consultation closes on 19 November 2021. Key proposed changes include:	Consultation	AI anonymization automated decision-making breach response conditions for processing	Sep-21	Consultation DCMS press release

Jurisdiction	Region	Development	Type	Topic	Entry last updated	Links
		• **Compliance programme**: to remove the current, specific requirements for DPOs, DPIAs and records of processing activities, and replace these with a general requirement for a risk based privacy management programme and a new requirement for organisations to have a simple and transparent complaints handling process. • **Legitimate interests**: to create a list of purposes for which organisations can process personal data relying on the legitimate interests legal basis but without applying the balancing test currently required. • **Access requests**: to allow organisations to charge a fee for responding to individuals' requests to access their data in certain circumstances and to allow organisations to refuse to comply with vexatious requests. • **International transfers**: to allow repeated transfers on the basis of derogations such as consent, or performance of a contract with the individual, to allow organisations greater flexibility to identify transfer mechanisms that provide appropriate safeguards and to allow data originating overseas to be sent back to the original sender. • **Data breach reporting**: to raise the threshold for mandatory data breach reporting so that only data breaches with a material risk for individuals have to be reported to the ICO. • **Direct marketing:** to increase the level of fines to be in line with UK GDPR (up to £17.5 million or 4% of turnover). • **Cookies**: to remove the requirement for consent for cookies used for analytics or other limited purposes, or potentially to remove the requirement for cookie consent and instead rely on web browser technology or data fiduciaries to manage individual preferences. • **Artificial intelligence and automated decisions**: to clarify what is required for 'fair' data use in AI, to allow greater scope for organisations to train and test AI systems and enable organisations to use personal data to manage the risk of bias in AI systems. Also to allow automated decision-making on the basis of legitimate interests and other legal bases. • **ICO**: to require the ICO to have regard for economic growth, innovation and competition when discharging its functions, and allow the ICO not to investigate a complaint on the basis of specified criteria.		compliance programme cookies data protection officer international transfer legitimate interests marketing privacy assessment research rights sanctions		
United States (California)	Americas	**California Privacy Rights Act of 2020 (CPRA)** The California Privacy Rights Act of 2020 (Proposition 24) (CPRA) was passed on 3 November 2020. The CPRA amends the California Consumer Privacy Act (CCPA); most changes will take effect on 1 January 2023 with respect to personal information collected on or after 1 January 2022. • **Regulator** - The amendment establishes the California Privacy Protection Agency to assume some of the DoJ's current responsibilities for enforcing and implementing consumer privacy laws and imposing fines. • **Scope** - The CPRA changes one of the thresholds which determine whether the CCPA applies to a business. Currently it applies to businesses that buy, sell, or share for business purposes the personal data of 50,000 or more consumers, households, or devices annually; this is amended to 100,000 or more consumers or households and devices are no longer included in the computation. • **Consumer rights** - Consumers will have rights to direct businesses to take reasonable efforts to correct personal data. They may also request businesses not to share their personal data and to limit the processing of sensitive personal information (including precise geolocation; race; ethnicity; religion; genetic data; private communications; sexual orientation; and specified health information) only to the extent necessary to (1) provide requested services or goods and (2) fulfil key business purposes (such as providing customer service).	New Law	data protection law data quality regulator rights sensitive personal information	Dec-20	California voter guide Text of the CPRA Legislative analysis
United States (Federal)	Americas	**Cybersecurity Act of 2020** The Internet of Things (IoT) Cybersecurity Improvement Act of 2020 was signed into law on 4 December 2020. The IoT Cybersecurity Improvement Act empowers the National Institute of Standards and Technology (NIST) to create cybersecurity standards for internet-connected devices purchased and used by federal agencies. However, such NIST standards are expected to become recommended practice more widely.	New Law	security	Dec-20	IoT Cybersecurity Improvement Act of 2020

Jurisdiction	Region	Development	Type	Topic	Entry last updated	Links
United States (Federal)	Americas	**Cybersecurity requirements** New security standards are to be published pursuant to the Executive Order on Improving the Nation's Cybersecurity (the **Order**), signed on 12 May 2021. All Federal Information Systems must meet or exceed the standards and requirements for cybersecurity issued pursuant to the Order. The Order directly impacts the private sector with the creation of incident reporting obligations for providers and the establishment of minimum cybersecurity standards and transparency for developers. Private sector companies are also encouraged to follow the Federal government's lead to augment and align cybersecurity investments. • **Information sharing** - Service providers to Federal agencies will be required to ensure that they collect data relevant to cybersecurity event prevention, detection, response, and investigation on all information systems over which they have control. They will be required to share with Government any data that relates to cyber incidents or potential incidents relevant to any agency with which they have contracted. Details of the contractual terms imposing these requirements, which are to be 'consistent with applicable privacy laws, regulations, and policies', will be published for comment. • **Cybersecurity standards** - The Order sets out requirements for Federal Agencies to take to migrate towards the use of cloud adopting 'Zero Trust Architecture' and mandates deployment of multifactor authentication and encryption within a set time period. • **Software supply chain security** - Baseline security standards will be established for development of software sold to the government, with a priority on addressing 'critical software'. NIST is to produce guidelines setting criteria for evaluating the security of software and of developers as well as guidance identifying practices to enhance the security of the supply chain. The White House explains that the aim is to use the purchasing power of the Federal Government to drive the market to build security into all software from the ground up and the Order also creates a pilot program to create a consumer software label to indicate whether software was developed securely. • **Cyber response playbook** - The Order mandates the creation of a standardised playbook incorporating all NIST standards for cyber incident response by federal departments and agencies. The White House Fact Sheet states that this playbook will also provide the private sector with a template for its response efforts. • **Incident detection, investigation and remediation** - The Order creates cybersecurity event log requirements and a Cybersecurity Safety Review Board which may convene following a significant cyber incident.	New Law	security	Jun-21	Executive Order White House Fact Sheet
United States (Federal)	Americas	**Bill to Update COPPA** A bill to update the Children's Online Privacy Protection Act (COPPA) has been introduced to the Senate as a bipartisan initiative by democrat Senator Markey and republican Senator Cassidy. If enacted, the Children and Teens' Online Privacy Protection Act (the Bill) would tighten requirements under COPPA. **Key provisions** • Companies would be deemed to have constructive knowledge that a user is a child in specified circumstances. • Internet companies prohibited from collecting personal information from users who are 13 to 15 years old without the user's consent and a limitation on data collected. • A prohibition on targeted advertising (as opposed to contextual advertising) directed at children. • Requirements to permit users to eliminate personal information from a child or teen when technologically feasible. • Notice requirements addressing the types of personal information collected, how that information is used and disclosed, and the policies for collection of personal information. • Cyber security standards for internet connected devices targeted at children.	Draft Law	children online services	Jun-21	Bill Press Release

Jurisdiction	Region	Development	Type	Topic	Entry last updated	Links
		• Creation of a Youth Marketing and Privacy Division at the Federal Trade Commission responsible for addressing the privacy of children and minors and marketing directed at children and minors.				
United States (Federal)	Americas	**Information Transparency & Personal Data Control Act** This bill would not create a data protection law but would require the Federal Trade Commission (**FTC**) to establish requirements for entities providing services to the public that collect, store, process, use, or otherwise control sensitive personal information. The Bill provides for the FTC to require controllers of sensitive personal information to: (1) provide consumers with a privacy and data use policy; (2) obtain affirmative consent to collect or use consumers' sensitive data; and (3) obtain an annual privacy audit that evaluates the sufficiency of the controller's data privacy and security controls.	Draft Law	data protection law privacy policy conditions consent privacy audit	Jun-21	Information Transparency & Personal Data Control Act (link is to the Bill in Congress) US Chamber of Commerce letter in support of bill
United States (Federal)	Americas	**Bipartisan bill to update COPPA** The Children and Teens' Online Privacy Protection Act introduced as a bipartisan bill by Democrat and Republican Senators would tighten requirements under COPPA. • Companies would be deemed to have constructive knowledge that a user is a child in specified circumstances. • Internet companies prohibited from collecting personal information from users who are 13 to 15 years old without the user's consent and a limitation on data collected. • A prohibition on targeted advertising (as opposed to contextual advertising) directed at children. • Requirements to permit users to eliminate personal information from a child or teen when technologically feasible. • Notice requirements addressing the types of personal information collected, how that information is used and disclosed, and the policies for collection of personal information. • Cybersecurity standards for internet connected devices targeted at children. • Creation of a Youth Marketing and Privacy Division at the Federal Trade Commission responsible for addressing the privacy of children and minors and marketing directed at children and minors.	Draft Law	children	May-21	The Children and Teens' Online Privacy Protection Act Senator's Press Release
United States (Federal)	Americas	**Executive Order on Cybersecurity** President Biden issued Executive Order on Cybersecurity (14028) in May 2021. The Executive Order charges various agencies with providing guidance and other materials to improve the security and integrity of the software supply chain. Several agencies were mandated with providing guidance, standards and contractual provisions for improving security. To date NIST has published guidance outlining security measures for critical software and guidelines recommending minimum standards for vendors' testing of their software source code. It is to publish three further pieces of guidance and procedures in the coming months. The Federal Acquisitions Regulatory Council (FAR) was mandated to publish updated contractual requirements for agencies to use in contracting with IT and OT providers; these have yet to be published.	Guidance	security	Sep-21	Executive Order: Improving the Nation's Cybersecurity NIST Announcement including links to all guidance published to date
United States (Federal)	Americas	**FTC Review of Health Breach Notification Rule** The FTC is currently undertaking a review of the Health Breach Notification Rule, and is actively considering public comments regarding the application of the Rule to mobile applications and other direct-to-consumer technologies that handle consumers' sensitive health information.	Consultation	breach response health data	May-21	FTC Call for Comments

Jurisdiction	Region	Development	Type	Topic	Entry last updated	Links
United States (**Connecticut**)	Americas	**Connecticut - Data Privacy Breaches Act: bill passed** Connecticut Public Act No. 21-59 (*An Act Concerning Data Privacy Breaches*) makes important changes to data breach notification obligations in **Connecticut**, including: (1) reducing the time period for notifying a breach (to both affected individuals and to the Attorney General) from 90 days to no more than 60 days; (2) establishing an obligation to provide individuals with a "preliminary substitute notice" of a breach (via email, and by way of a public notice on the affected organisation's website and in state-wide media) if a direct notification cannot be made within the 60 day limit; and (3) broadening the categories of personal data that can trigger the obligation to notify, to include: (i) a range of identification numbers (such as taxpayer ID numbers, personal ID numbers, health insurance ID numbers, and passport numbers); (ii) medical and biometric information; and (iii) usernames or email addresses which, in combination with a password or security question and answer, would enable access to an online account. The revised legislation will have effect from 1 October 2021.	Draft Law	data protection law breach response	Aug-21	Act and related documentation published by the Connecticut General Assembly
United States (**Colorado**)	Americas	Colorado's Act Concerning Additional Protection of Data Relating To Personal Privacy (the **Act)** was signed by the Governor on 7th July 2021 and will take effect on 1st July, 2023. **Scope** The new law will apply to legal entities that conduct business or produce commercial products or services that are intentionally targeted to Colorado residents and that either: • control or process personal data of more than 100,000 consumers per calendar year; or • derive revenue from the sale of personal data and control or process the personal data of at least 25,000 consumers. Exemptions include processing governed by the Gramm-Leach-Bliley Act (GLBA) and employment records. **Key Provisions** Consumers will have the right to opt out of the processing of their personal data; to access, correct, or delete the data; or obtain a portable copy of the data. The Act specifies how controllers must fulfil duties regarding consumers' assertion of their rights and provides power for the attorney general to specify technical specifications for a universal opt-out mechanism that controllers must use. The Act includes principles of care, transparency, purpose specification, data minimisation, avoiding secondary use and unlawful discrimination, and a concept of sensitive data; Controllers will be required to conduct a data protection assessment for processing activities involving personal data that present a heightened risk of harm to consumers, such as processing for purposes of targeted advertising, profiling, selling personal data, or processing sensitive data. **Rulemaking and enforcement** The attorney general may promulgate rules to administer the Act. Local governments are pre-empted from adopting laws that govern the processing of personal data by controllers or	New Law	data protection law erasure privacy notice rights security	Jul-21	Washington (SB 5062) (showing current status) Colorado Bill (SB21190) showing current status

Jurisdiction	Region	Development	Type	Topic	Entry last updated	Links
		processors. Violation of the law will constitute a deceptive trade practice, but the Act may be enforced only by the attorney general or district attorneys.				
United States (**Nevada**)	Americas	**Amendment to Online Privacy Law** A Bill (SB260) to amend Nevada's online privacy law was enrolled and delivered for signature by the Governor on 27th May. The existing law requires website operators which collect certain personally identifiable information about Nevada consumers to allow consumers to opt-out of the sale of covered information. If signed by the Governor, the new bill will impose similar requirements upon data brokers and provide that the 30-day window of opportunity for remedying a failure to comply and avoid being deemed to be in breach of the law only applies to a first failure to comply.	Draft Law	Sale of data	Jun-21	Bill SB260 showign current status
United States (**Virginia**)	Americas	**The Consumer Data Protection Act (CDPA)** The CDPA was signed into law on 2 March 2021 and will take effect on 1 January 2023. **Scope**The CDPA will apply to all persons that conduct their business in Virginia, or that produce products or services that are targeted to residents of Virginia and either: • control or process personal data of at least 100,000 consumers per calendar year; or • control or process personal data of at least 25,000 consumers and derive over 50 percent of gross revenue from the sale of personal data.Exemptions include non-profit organisations, financial institutions or data subject to the Gramm-Leach-Bliley Act (GLBA) and organisations subject to the Health Insurance Portability and Accountability Act (HIPAA). **Key Provisions**The CDPA is the most comprehensive State data protection law after California's. It introduces: • Consumer rights to access, correct, delete, obtain a copy of personal data, and to opt out of the processing of personal data for the purposes of targeted advertising, sale of data, or certain types of profiling. • Principles of data minimisation, purpose limitation, security and non-discrimination. • An obligation to obtain consent before processing sensitive data concerning a consumer or, in the case of the processing of sensitive data concerning children, to comply with the federal Children's Online Privacy Protection Act (COPPA). • Prescribed content requirements for privacy notices. • An obligation to carry out data protection impact assessments for higher risk activities including targeted advertising, sale of data and profiling. • Data processing by a processor must be governed by contract containing specified provisions. Specific processor obligations include security, adherence to the controller's instructions and assisting it with data protection assessments and data breach notification requirements under Virginia's separate breach notification law. **Enforcement** The Attorney General will be responsible for enforcement. Controllers and processors breaching the requirements may be subject to an injunction and liable for a civil penalty of not more than $7,500 for each violation.	New Law	adtechconsentcontracts data minimisation data protection lawerasure non-discrimination processorspurpose limitation privacy assessment privacy noticerightssale of datasecurity	Mar-21	Text of the CDPA
Uruguay	Americas	**Guidance on extra-territoriality** Counsel has been unofficially informed that the URCDP is currently drafting guidance regarding extraterritorial applicability of Uruguayan DP Laws.	Draft Guidance	territorial scope	Aug-21	

Jurisdiction	Region	Development	Type	Topic	Entry last updated	Links
Vietnam	APAC	**Proposal for Data Protection Law** Vietnam does not currently have a comprehensive data protection regime. The Ministry of Public Security has published a draft data protection law for consultation, closing on 9 April 2021. In its current form, the draft law would come into effect on 1 December 2021. As currently written, the draft law would introduce: • **Data protection principles**, including lawfulness, purpose limitation, data minimisation, accuracy, security, transparency and confidentiality. • **Consent**: a requirement for voluntary and informed consent to process or disclose personal data, unless an exception applies. • **Privacy notice**: specific information to be provided to the individual about the processing of their data. • **Individual rights** to request access, correction, erasure or stopping the processing of personal data, and also to claim compensation. • **Additional restrictions on sensitive data**: the handling of sensitive personal data must be registered in advance. • **Restrictions on international transfer**, requiring the individual's consent or another condition to apply before data may be transferred out of Vietnam. • **Compliance programme**: a requirement for organisations to implement data protection policies and appoint a data protection officer. The draft law also includes provisions addressing the handling of children's personal data, automatic data processing and scientific research. A new expert Personal Data Protection Committee (Committee) would be established, part of the Department of Cyber Security in the Ministry of Public Security. The Department of Cyber Security would have power to impose administrative sanctions of up to 5% of turnover in Vietnam for repeated, serious infringements, to recover profits arising from infringements and to suspend processing of personal data.	Draft Law	compliance programme conditions for processing consent data protection officer data retention data transfer international transfer rights sensitive data security sanctions	Feb-21	Draft law for consultation - February 2021

Ready to find out more? Contact info@aosphere.com to organise a free trial and demo of Rulefinder Data Privacy