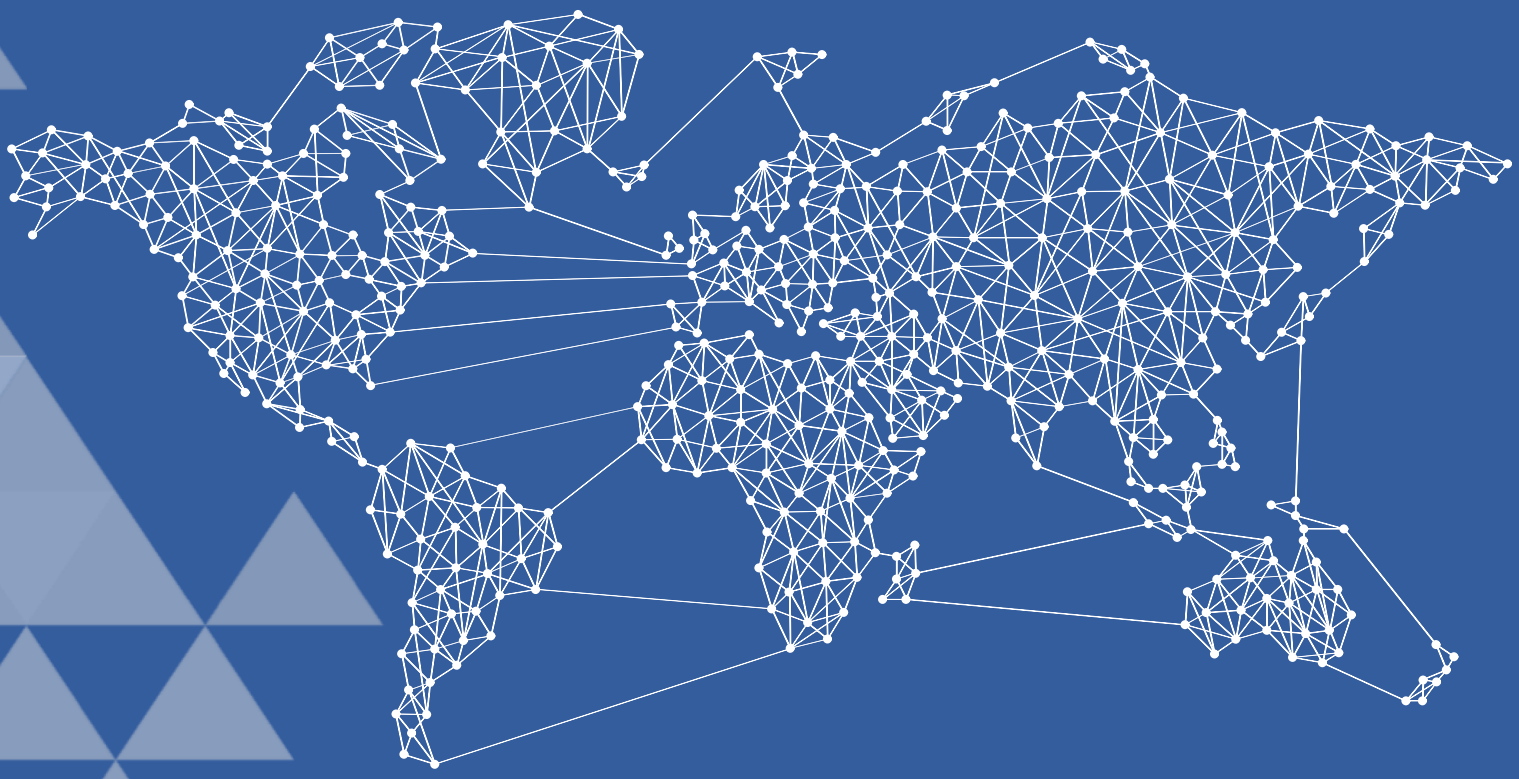
OneTrust DataGuidance Privacy Review

Q2 2020



OneTrust DataGuidance™
REGULATORY RESEARCH SOFTWARE

About the report

The second quarter of 2020 saw several expected and unexpected data protection milestones around the world. These included both the postponements of key laws and the introduction of major legislative reform. There were notable court decisions and guidelines released on topics such as cookies, temperature screening, contact tracing, and anonymisation. Enforcement actions increased and significant sanctions and settlements were proposed in a wide range of jurisdictions. OneTrust DataGuidance's Privacy Analyst team here considers the most notable developments between April and June of 2020 and highlights some key areas to monitor next quarter.

About the authors

OneTrust DataGuidance™

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

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

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

For more information visit dataguidance.com

Contributors

OneTrust DataGuidance™

Angela Potter, Nikolaos Papageorgiou, Rhiannon Gibbs-Harris, Angus Young, Victoria Ashcroft, Alexis Kateifides

Image production credits

Cover page: pop_jop / Signature collection / istockphoto.com

Global

Key takeaways:

- Postponements to Brazil's LGPD and Thailand's PDPA
- South Africa's POPIA given commencement date and DIFC enacts new law
- Privacy Bill in New Zealand and significant amendments to Japan's APPI are passed
- Cookies and international data transfers dominate major stories in the EU

Continued release of Coronavirus guidance

COVID-19 ('the Coronavirus') remained a preeminent concern across the world, particularly in April and May, where contact tracing and temperature screening were regularly commented on by numerous data protection authorities. Although there was a decrease in the amount of information being published regarding privacy and the pandemic in June, a lack of a harmonised approach to such issues has meant that the need to continually review national approaches remains.

Enforcement actions increase

Across the world there has been a marked increase in enforcement actions compared to the first quarter of 2020, and particularly a notable escalation in monetary penalties. For example, a $225 million settlement has been proposed by the Federal Communications Commission ('FCC') in the US, and several fines were issued in June by the Spanish data protection authority. In addition, notable penalties were announced throughout the Americas and Europe with significant sanctions issued in Canada, Colombia, Finland, Italy, and the Netherlands, among others. Privacy infringements in the financial sector also resulted in considerable monetary penalties in Hong Kong, Ukraine, and the UK. Most of these sanctions have resulted from investigations that began prior to the Coronavirus' impact on data protection authority activities. However, it should be noted that several authorities have initiated further investigations in recent months and while some are providing flexibility from obligations, others are reiterating the importance of compliance.

Artificial intelligence (AI) a common talking point

Following the European Commission's publication of its AI white paper on 19 February 2020, conversations around privacy and AI have gained momentum. Several direct responses to the white paper have been published and the topics brought into focus have ranged from ethics and fundamental human rights, to the business impact of regulations and the challenges of explaining decision-making in the context of machine learning. These discussions have tended to be broadly framed as the parameters of the AI privacy conversation continues to be shaped. Key issues that have been highlighted include AI vendor management, the potential for risks in systems designed to protect data subjects, explaining algorithms, and how to turn ethical concerns into practical policies. A notable development in this area has been the establishment of the Global Partnership on Artificial Intelligence ('GPAI'), which is comprised of Australia, Canada, France, Germany, India, Italy, Japan, Mexico, New Zealand, South Korea, Singapore, Slovenia, the UK, the US, and the EU.

International trade

The Digital Economy Partnership Agreement ('DEPA') between Chile, New Zealand, and Singapore was signed on 12 June 2020. Singapore has taken a leading role in developing these digital partnership agreements and has now concluded talks on a similar agreement with Australia and begun talks on the same with South Korea. Although these agreements still need to be brought into effect within the participating jurisdictions, they have the potential to form the basis for a general framework for cross-border data flows.

Trade discussions between the UK and US, and the emphasis being placed on digital trade, are likely to become increasingly important. The European Data Protection Board ('EDPB') has also raised concerns regarding the UK-US CLOUD Act agreement and the potential for a UK adequacy decision. Moreover, there have been suggestions that bilateral digital trade discussions commence between Brazil and the US, although these may be subject to the ongoing legislative reform in Brazil.

In relation to more established instruments, Serbia and Poland became the fourth and fifth countries, respectively, to ratify Convention 108+, while Romania became the 39th country to sign this modernised version of Convention 108. Meanwhile, Japan announced its efforts in relation to data flow agreements between itself and the EU and the US through a framework based on the EU-US Privacy Shield, 'Economic Cooperation' Asia-Pacific Economic Cooperation Cross-Border Privacy Rules ('APEC CBPR'), and the EU adequacy decision for Japan.

What to look out for:

- Several legislative milestones are likely to have a major global impact, particularly the entry into effect of laws in South Africa, DIFC, New Zealand, and Japan
- Whether trends of Coronavirus developments declining and enforcement actions increasing will continue
- Whether the fast-developing discussions on digital trade agreements will be implemented and guide a process of closer global alignment
- How data flows with the EU will be affected by adequacy decisions and the judgment in the Schrems II case

Americas & Caribbean

Key takeaways:

- Brazil's General Personal Data Protection Law ('LGPD') enforcement provisions postponed until 1 August 2021
- Enforcement actions increase throughout the Americas, including a record $225M proposed settlement by the FCC
- Final regulations for the California Consumer Privacy Act of 2018 ('CCPA') submitted for approval

April

The Coronavirus dominated privacy related headlines in many jurisdictions throughout April. Guidance was released in the BES Islands, Bermuda, Brazil, the Cayman Islands, Ecuador, Mexico, Paraguay, and the US on a range of key topics, such as working from home, tracing apps, employee data, and videoconferencing. Privacy news in Canada at both the provincial and federal level almost entirely consisted of Coronavirus related comments and guidelines. There were also announcements in several jurisdictions regarding enforcement discretion during the pandemic. A smaller set of jurisdictions, including Chile, Peru, and the US, began to take further steps towards more robust legislative responses through Coronavirus related laws and decrees.

One of the more complicated repercussions of the Coronavirus continued to develop in Brazil as President Bolsonaro released Provisional Measure No. 959 of 29 April 2020. The Provisional Measure allowed the President to issue an executive order that would postpone the LGPD until 3 May 2021. Bill 1179/2020, which would also postpone the LGPD, was still pending at this stage.

Activity also increased in Colombia as the Colombian data protection authority ('the SIC') took a mixed approach to enforcement. On the one hand, the SIC eased obligations by extending the registration deadline with the National Registry of Databases ('RNBD') until 3 July 2020. On the other hand, the SIC opened multiple investigations relating to third party data subject identifications and adherence to the principle of accountability and issued a fine of approximately €80,000 to a bank following a data subject complaint.

Enforcement actions were likewise seen in the BES Islands and the US. The BES Islands data protection authority issued an audit report that urged the use of impact assessments, while three settlements in the US exceeded $45 million combined. Approximately a quarter of this total resulted from a class action lawsuit following a health data breach case. The remaining roughly $37 million arose from two State level settlements following a 2017 data breach.

May

While guidance on privacy protection and the Coronavirus continued to be released

throughout the region, and particularly in Canada and Latin America, the most significant Coronavirus developments related to legislative reform. In Chile, a bill on sensitive data processing during an emergency was submitted to the Senate that would introduce new safeguard requirements for health data, and, likewise, a public health emergency bill was submitted in the US Senate. In Brazil, Bill 1179/2020 continued to progress through the Chamber and Senate and was passed on to President Bolsonaro to sign.

There were several notable events in the US during May, including the announcement from the Californians for Consumer Privacy advocacy group that the Consumer Privacy Rights Act ('CPRA') proposal had obtained enough signatures to be entered onto the November 2020 ballot. The CPRA seeks to amend the CCPA and establish, among other things, an enforcement authority as well as rights related to sensitive personal information. In general, privacy advocacy groups in the US were particularly active this month and issued a variety of calls for investigations. Notable developments from authorities included the American Medical Association ('AMA') releasing a set of privacy principles, the Federal Communications Commission ('FCC') strengthening enforcement against robocalls, and the publication of numerous pieces of guidance, primarily related to cybersecurity.

Authorities were also active elsewhere in the region with Colombia's SIC announcing further investigations, the Argentinian data protection authority ('AAIP') issuing a fine of approximately €3,770, and the Uruguayan data protection authority ('URCDP') releasing a Resolution that clarifies data protection officer ('DPO') appointment requirements. The most substantial action taken in May, though, came from the Competition Bureau of Canada, which settled with a prominent social media company approximately for €6 million for misleading claims related to privacy of personal information between 2012-2018. In addition, the bill for the Data Protection Act, 2020 passed the House of Representatives in Jamaica and moved on to the Jamaica Senate.

June

While the Coronavirus continued to have a notable influence throughout the Americas, the volume of guidance and privacy developments related to the pandemic declined significantly. The main news stories during the month were instead focused on more general privacy legislation and enforcement actions. In particular, the effective date for the enforcement provisions of Brazil's LGPD was postponed until 1 August 2021, while Provisional Measure No. 959 continued to await approval by the Congress of Brazil. Furthermore, the controversial Bill 2630/2020 was passed by the Federal Senate of Brazil. It would establish provisions related to fake news, including requirements for account registration.

The bill for the Data Protection Act, 2020 was passed by the Jamaica Senate. Although the Bill still needs to be signed the Governor-General and published in the Gazette, and provides for a two-year transition period before it will be fully in effect, it will introduce a new privacy framework in Jamaica with provisions for data processing registration, data protection officers, data subject rights, and a set of detailed and obligatory data protections standards. There were several discussions on legislative reform in Canada at both the provincial and federal level. A central point of discussion in these conversations has been the importance of recognising privacy as a fundamental right, potential reforms of access to information requirements, and the challenges of aligning to federal law and to the EU's GDPR.

In California, the AG submitted for approval the final regulations under the CCPA. In the US more broadly, the main stories focused on enforcement actions and, most notably, the FCC proposal for a record $225 million settlement against an insurance company for a range of robocall related violations. There were also multiple fines for infringements of the Children's Online Privacy Protection Act ('COPPA'), and a class action following a data breach resulted in a $192,000 settlement.

What to look out for:

- CCPA final regulations expected to be approved in the short term
- CPRA eligible for November 2020 ballot
- US-Mexico-Canada Agreement ('USMCA') commencement on 1 July 2020
- Bill for Data Protection Act, 2020 awaiting final sign-off in Jamaica

APAC & the CIS

Key takeaways:

- Entry into effect of Thailand's Personal Data Protection Act ('PDPA') postponed until 31 May 2021
- Privacy Bill passed in New Zealand, commences 1 December 2020
- Major amendments passed to Japan's Act on the Protection of Personal Information ('APPI')
- Data protection bills advancing in Pakistan and Indonesia

April

More Coronavirus related tracking apps were introduced in the APAC and the CIS than anywhere else during April, and many of these resulted in privacy discussions, amendments, and guidelines. In addition, several jurisdictions released guidelines on working practices under the Coronavirus and related matters, including Australia, Belarus, China, India, Japan, Lao PDR, Macau, Malaysia, Moldova, Philippines, Ukraine, and Uzbekistan. Of these, Australia was the most active jurisdiction in addressing the Coronavirus, releasing a contract tracing app, numerous pieces of guidance, and providing a 3-month exemption to certain Consumer Data Right ('CDR') requirements. The Office of Personal Data Protection ('GPDP') in Macau likewise issued a series of authorisations that provided exceptions from usual obligations due to the Coronavirus.

Beyond the Coronavirus, April saw a diverse range of legislative proposals in APAC and the CIS. These included a proposed data protection bill in Pakistan, which replaces a 2018 bill, and bills on employee data and on cyber fraud and biometric data in Russia. Discussions on amending the Personal Data Protection Ordinance ('PDPO') in Hong Kong continued, and it was noted that the Office of the Privacy Commissioner for Personal Data ('PCPD') would update guidance on cross-border data transfers. Meanwhile, China introduced significant new cybersecurity review measures for critical information infrastructure operators and released new standards on personal information health codes.

Financial monitoring continued to be at the forefront in Ukraine, with not only a new law entering into force that is designed to address Financial Action Task Force ('FATF') recommendations but also several enforcement actions from the National Bank of Ukraine. Similarly, a series of warnings related to anti-money laundering violations were issued in New Zealand, and the Securities and Futures Commission ('SFC') in Hong Kong issued a fine of approximately €2.3 million for internal control deficiencies.

May

Although the Coronavirus, and the focus on contact tracing applications, continued to dominate privacy developments across the APAC and the CIS regions in May, the most notable announcement was that the coming into effect of Thailand's PDPA would be delayed for one year until 31 May 2021

In China, the Civil Code of the People's Republic of China was adopted by the 13th National People's Congress, and will enter into effect on 1 January 2021. The Civil Code contains a section on personal information protection that would provide an overarching, general establishment of privacy rights in China. Meanwhile, a bill to amend the Personal Data Protection Act ('PDPA') in Singapore was released for public consultation. The Bill would introduce significant new measures, such as data breach notification requirements and rights for data portability.

Australia's CDR framework was further developed through a joint Compliance and Enforcement Policy released by the Office of the Australian Information Commissioner ('OAIC') and the Australian Competition and Consumer Commission ('ACCC'), and Russia's Duma announced it would adopt a financial services biometrics law in the near future. Indeed, privacy developments in the CIS were again focused on financial services, with anti-money laundering and countering the financing of terrorism laws discussed in Belarus and Moldova, and further enforcement actions announced by the National Bank of Ukraine.

June

Most notably, on 24 June 2020, the Privacy Bill was passed in New Zealand. On 1 December 2020 it will replace the Privacy Act 1993 and introduce a wide range of obligations including requirements for data breach notifications, restrictions and new mechanisms for international data transfers, and an expansion of the territorial scope of New Zealand's privacy framework.

Similarly, a bill to amend Japan's Act on the Protection of Personal Information ('APPI') was promulgated on 12 June 2020, which will broaden rights for erasure and restriction of processing, introduce the concept of pseudonymised data, provide for mandatory data breach notifications, further restrict international data transfers, and enable new extraterritorial enforcement options. Although the amendments have been passed, they are now expected to be supplemented through additional rules and guidelines before coming into effect before June 2022. Another bill was also promulgated on 12 June 2020 in Japan that introduces less radical but still significant amendments to the Whistleblowers Protection Law.

Further legislative developments included amendments to the Competition and Consumer (Consumer Data Right) Rules (2020) entering into effect in Australia, Singapore's PDPA being amended to recognise APEC CBPR and PRP certifications, and the Ministry of Communication and Information Technology ('Kominfo') seeking to accelerate the Personal Data Protection Bill in Indonesia. There were comparable discussions in Ukraine on the development of a bill to amend the data protection law, as well as the passing of amendments to the Law on Information Protection in Telecommunication Systems, and the introduction of a bill on virtual assets. In Russia, a bill was introduced to the Duma that seeks to better regulate remote-working.

What to look out for:

- Commencement of new Privacy Act in New Zealand on 1 December 2020
- Further guidelines and rules expected to clarify amendments to the APPI in Japan
- China's draft data security law continues to develop in National People's Congress ('NPC')

EMEA

Key takeaways:

- South Africa's Protection of Personal Information Act, 2013 ('POPIA') enters into effect
- New law enacted in Dubai International Financial Centre ('DIFC')
- Notable increase in enforcement actions, particularly in Finland, Spain, and Turkey
- Major decisions from courts in France and Germany on cookies

April

As in the rest of the world, the Coronavirus dominated privacy related headlines in EMEA during April, and a steady stream of guidance was released on relevant topics. In particular, thermal imaging became an important area of focus and data protection authorities in Cyprus and the Netherlands warned that the use of thermal imaging at workplaces is at high risk of violating the GDPR. More general guidance was issued in the DIFC, most EU Member States, Israel, Mali, Mauritius, Morocco, Senegal, and South Africa.

Discussions continued in Germany as the Federal Commissioner for Data Protection and Freedom of Information ('BfDI') highlighted its concerns with the draft second law on the protection of the population during an epidemic of national importance. In a similar vein, the Malian data protection authority ('APDP') released its concerns regarding the lack of data protection enforcement measures in Law No. 2019-056 of 5 December 2019 on the Repression of Cybercrime. Notable pieces of guidance were published in France covering ISO 27701 and the right to delisting, and the long-awaited clarification of binding corporate rules ('BCR') was issued in Turkey.

April also saw a series of enforcement actions across Europe. The Polish data protection authority ('UODO') issued one fine of approximately €4,400 and opened several investigations, and the Estonian Data Protection Inspectorate ('DPI') issued formal warnings of two potential fines that would equate to a combined €6,000. A sanction of approximately €3,000 was issued in the Czech Republic for violations relating to commercial messaging, and two fines of approximately €27,800 and €2,450 were issued in Turkey. In Sweden, a government centre was fined €18,700 for failing to notify a breach, while in Belgium a failure to notify of a data protection officer appointment resulted in a penalty of €50,000. The most significant fine, of €750,000, was issued to an organisation in the Netherlands for requiring its employees to have their fingerprints scanned to record attendance.

May

While guidance regarding the Coronavirus continued to be released on a regular basis, May also commenced with the European Data Protection Board ('EDPB') releasing its adopted updated guidelines on consent. The guidelines recommend that service providers cannot prevent data subjects from accessing a service on the basis that they do not consent, highlight that cookie walls are prohibited, and that scrolling or swiping through a webpage

does not constitute a clear and affirmative action providing unambiguous consent. In addition, the Interactive Advertising Bureau Italy ('IAB Italy') published its white paper Programmatic Advertising 2.0, which considers digital advertising in a post-cookie era.

The German Federal Court of Justice ('BGH') issued its decision on the validity of consent for placing cookies on users' end devices through pre-ticked checkboxes, which echoed the opinion of the Court of Justice of the European Union ('CJEU') on the matter. This decision thereby placed the BGH in opposition to German data protection authorities in regard to the applicability of Section 15(3) of the Telemedia Act ('TMG'). The French data protection authority ('CNIL') also issued guidance detailing anonymisation and pseudonymisation requirements. Meanwhile, a progress report on the draft ePrivacy Regulation highlighted that Member States had mixed reactions to the inclusion of legitimate interest as a legal ground and that further discussions would be needed.

Similarly to April, there were a wide range of enforcement actions. Most notably, the Data Protection Commission ('DPC') of Ireland issued its first fine, several monetary penalties were issued in Finland and Denmark, and there were substantial sanctions in Turkey and Norway. In legislative developments, Iceland passed a whistleblowing act and the Cybersecurity and Data Protection Bill was gazetted in Zimbabwe, which now needs to be debated by the National Assembly and signed by the President in order to become law.

June

Coronavirus and privacy related developments continued for much of June at the same rate as in April and May in Europe, before beginning to decline later in the month. However, several long-awaited legislative reforms and announcements of key decisions were some of June's most significant developments within the EMEA region. In particular, having been anticipated since its enactment in 2013, it was finally announced that the most substantive portions of POPIA would come into effect in South Africa on 1 July 2020 with a 12-month transition period for organisations to become compliant. POPIA has been followed closely as it will introduce significant obligations for organisations and has a notably broad scope.

Moreover, the Dubai International Financial Centre ('DIFC') announced the enactment of the DIFC Data Protection Law No. 5 of 2020, which replaces the Data Protection Law No. 1 of 2007. This new law comes into effect on 1 July 2020 with a three-month grace period for businesses to become compliant, it is also supplemented through a new set of regulations. While the law is significantly influenced by the EU's GDPR and in several areas echoes the same principles as the GDPR, the DIFC law also extends further in some respects. For instance, the DIFC law will introduce specific requirements for data protection officers to annually assess data controller activities. In addition, the Federal National Council of the United Arab Emirates approved a draft consumer protection law that would establish several consumer rights, including rights related to privacy and data security, as well as related obligations for businesses.

The most notable developments in the EU included the Conseil d'Etat's partial annulment of CNIL's cookies guidelines in France, and specifically CNIL's efforts to ban cookie walls,

and the decision of the BGH provisionally allowing the Federal Cartel Office's ('BKA') order prohibiting a social network from further processing without additional consent. Several fines were issued in Spain, and significant fines were also issued in Finland, Hungary, Italy, Norway, Romania, Sweden, and Turkey. The European Commission released a two-year review of the GDPR in which it celebrated the impact of the legislation, noted challenges including reaching adequacy decisions, modernising standard contractual clauses, and the untapped potential of the right to portability, and highlighted the benefits of alternative enforcement actions than fines, such as bans on processing. Late in June, the Commission postponed its adequacy decision with Switzerland, with an expectation that this will be revisited once the progress of the proposed new Federal Data Protection Act in Switzerland is made clear.

What to look out for:

- Judgment in the case of Schrems II to be delivered on 16 July 2020
- DIFC law enforceable from 1 October 2020
- Ongoing discussions and decisions being issued on cookies
- Continued review of global adequacy decisions following postponement of decision in Switzerland

Further reading:

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

Insights

- New Zealand: New Privacy Act "step towards the gold standard of data protection"
- International: Update on status of privacy related legislation from APAC region
- Switzerland: Data protection revisions and GDPR equivalence
- EU: A privacy guide for AI vendors
- Germany: Consequences of BGH ruling on cookies
- Canada: Cross-border transfers and data localisation after the USMCA
- California: Status of CCPA and other privacy related bills in the State Legislature
- Japan: Impact of adopted APPI amendment bill
- Australia: OAIC and ACCC outline their enforcement approach for the Consumer Data Right
- DIFC: DIFC announces enactment of Data Protection Law
- China: Civil Code introduces data protection and privacy rights
- Turkey: International data transfers
- Singapore: Key amendments from PDPA amendment bill
- Germany: BGH issues decision on cookie consent based on CJEU Planet49 case
- Italy: IAB Italy publishes white paper on programmatic advertising 2.0
- Coronavirus Guidance Rolling Report (weekly update available here)

Videos/Webinars

- Japan APPI Amendments: What You Need To Know
- New Zealand Privacy Bill: What You Need To Know
- DIFC Data Protection Law: What You Need To Know
- Practical Requirements for Digital Marketing Across APAC and the EU (webinar 5 June 2020)
- Middle East Data Privacy Update (webinar 10 June 2020)
- Data Protection and Whistleblowing in China (webinar 19 June 2020)
- A Practical Guide to Breach Notification: Australia, EU and California (webinar 24 April 2020)
- HIPAA Compliance and Cybersecurity Challenges (webinar 6 May 2020)

Comparisons

- Cookies Portal
- California Consumer Privacy Act Portal
- Privacy Index
- Financial Sector