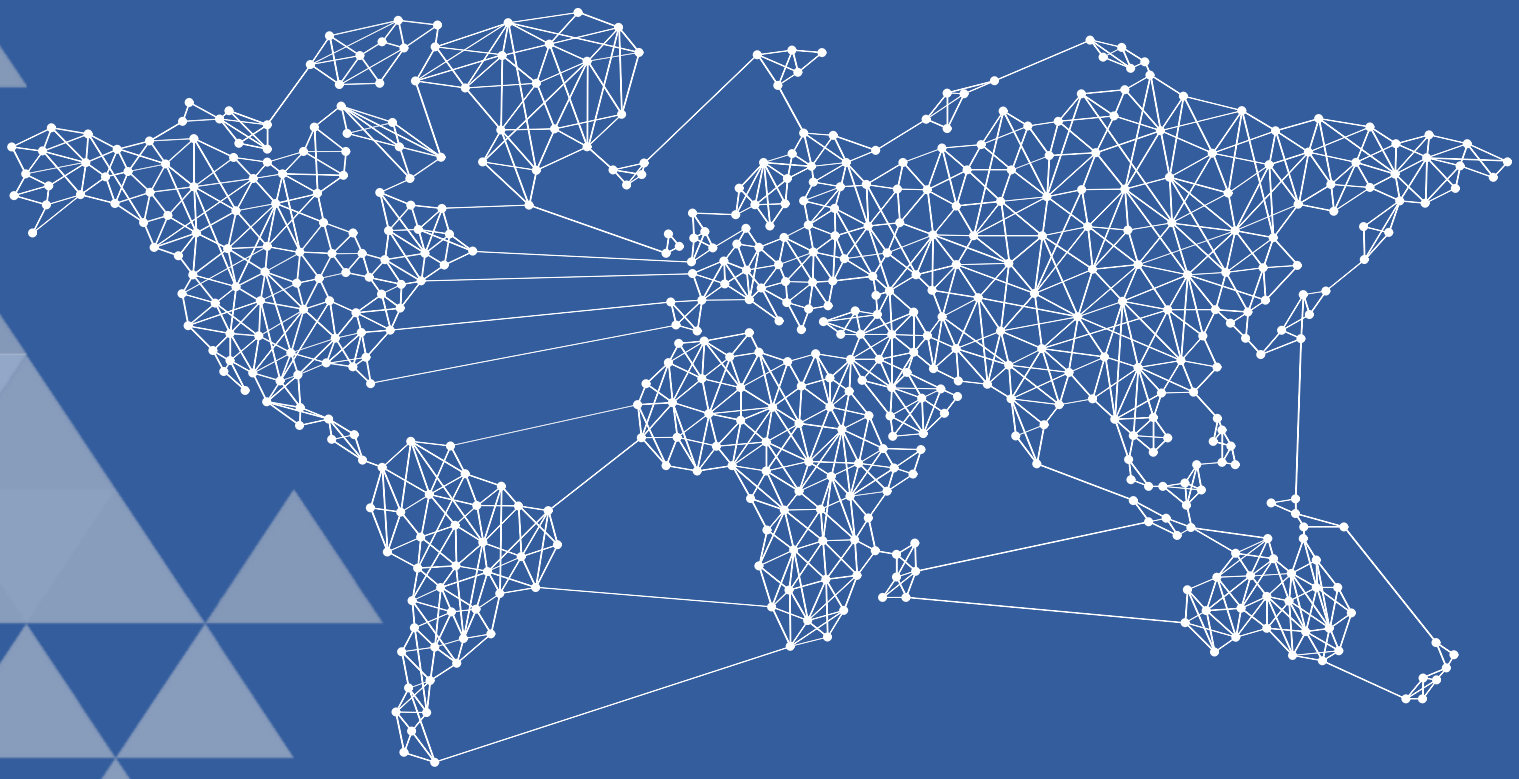
OneTrust DataGuidance Privacy Review

Q4 2020



OneTrust DataGuidance™
REGULATORY RESEARCH SOFTWARE

About the report

Quarter 4 of 2020 continued to be active in terms of legislative developments, guidelines, and enforcement actions. Just months after CCPA enforcement began (insert comma) the CPRA was passed which will provide for further requirements for organisations to take into consideration and prepare for. Legislative reform continued with the entry into force of the New Zealand Privacy Act 2020 as did momentum on a number of comprehensive privacy bills in Canada, Singapore, China and South Korea. With days to spare, the UK and EU regulators (CUT) reached a draft trade agreement, including provisions for the continued free flow of data for no longer than six months. Fallout from the decision of the CJEU in Schrems II continued to dominate headlines, with greatly anticipated recommendations being issued by the EDPB as well as the release of a draft set of revised standard contractual clauses.

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.

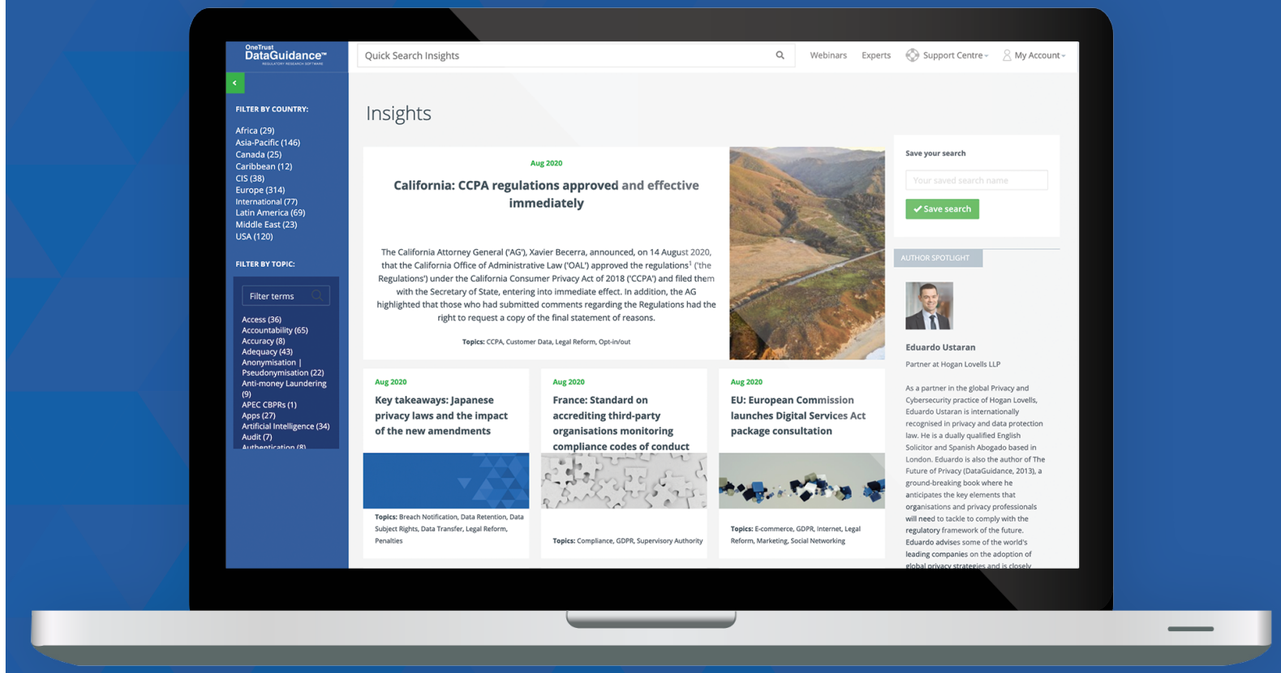
For more information visit dataguidance.com

Contributors

OneTrust DataGuidance™
Edidiong Udoh, Angus Young, Angela Potter, Nikolaos Papageorgiou, Rhiannon Gibbs-Harris, Alexis Kateifides, Victoria Ashcroft

Image production credits

Cover page: pop_jop / Signature collection / istockphoto.com



Global

Key takeaways:

- Ongoing guidance on data transfers after Schrems II
- California votes to pass CCPA 2.0
- Legal reform across China, Singapore, Canada, Switzerland, and Israel

Schrems II – SCCs and EDPB Guidance

Both the European Commission and the European Data Protection Board ('EDPB') released significant documents for public consultation as a response to the Court of Justice of the European Union ('CJEU') judgment in *Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems* (C-311/18) ('Schrems II'), in which the EU-US Privacy Shield was invalidated and data transfers from the EU were more generally brought into issue. On 11 November 2020, the EDPB released detailed guidance for organisations to assist in their responses to Schrems II including supplementary measures for data transfers and an explanation of the European Essential Guarantees in relation to surveillance measures.

The Commission issued, on 12 November 2020, a draft set of new Standard Contractual Clauses ('SCCs'), which seeks to provide a modular approach for data transfers by offering general clauses that can be adapted for different transfer relationships. The new SCCs present additional requirements for onward data transfers, greater flexibility, and obligations for risk assessments that could, to an extent, address Schrems II.

Together, these documents released by the EDPB and the Commission begin to address the fallout from Schrems II and how organisations may remain compliant. However, questions regarding the future of EU-US transfers as well as the specific challenges of assessing adequate data protection in third countries continue to be asked.

California Privacy Rights Act

The California Privacy Rights Act ('CPRA') passed on 3 November and is set to introduce a wide range of amendments to the California Consumer Privacy Act ('CCPA'). In particular, the CPRA provides for a state privacy authority, which will be the first of its kind in the US; introduces and modifies several key definitions; provides for new data subject rights; and will further regulate children's data. There will also be further exemptions, risk assessment obligations, and new contractual requirements with service providers.

Although the CPRA will not enter into effect until 1 January 2023, it will apply to personal information collected by a business on or after 1 January 2022, with the exception of the right of access. The CPRA has also been considered to evidence a growing interest in privacy among US citizens that may influence federal legislative developments.

Legislative reform

With the entry into effect of the New Zealand Privacy Act and stronger obligations for business and expanded enforcement tools for the New Zealand Privacy Commissioner, there will be a shift in the enforcement of legislative responsibilities in the region. Switzerland also reformed its federal legislation and adopted the revised Federal Act on Data Protection with the Councils disagreeing on the introduction of the concept of 'high-risk profiling' which was eventually included in the revised law.

Other countries are in various stages of far-reaching federal data protection reform including Singapore, China, Israel, and Canada. While a majority are taking the opportunity to transform outdated federal privacy legislation, China's draft bill could be the country's first harmonised comprehensive data protection law. A key feature of all draft legislation is both the increased enforcement and corrective powers of supervisory authorities as well as the introduction or increase of penalties for non-compliance, as well as expanded data subject rights.

Privacy and international trade

Data protection provisions have become increasingly prevalent in international trade negotiations. In particular, the topic of cross border data flows, data protection law harmonisation, and data localisation have been important policy objectives of government officials during negotiations. In November, 42 consumer ad digital rights groups issued a statement calling for digital trade negotiations at the World Trade Organisation to address the topic of cross-border data flows. Countries with a more data liberal model have recently included provisions which ban restrictions on the free flow of personal data, these include the US Mexico Trade Agreement and more recently the UK-Japan trade agreement with almost the same text in both, save some minor public policy exceptions. Conversely, the draft EU-UK Trade and Cooperation Agreement includes provision for the continued free flow of personal data until adequacy decisions are adopted and for no longer that six months. Though, an adequacy decision from the EDPB may sit at odds with the liberal data flow provisions of the UK-Japan trade deal.

Another critical topic intersecting trade and privacy is the inclusion of data localisation measures. A report published by the Organisation of Economic Cooperation considered that current trends in data localisation have had the effect of both protecting and undermining data privacy and therefore a holistic approach based on a test of proportionality should be considered to evaluate data localisation measures. Additionally, a study published by the Asia-Pacific Economic Cooperation discussed the importance of improving mutual recognition and interoperability, the need to harmonise national laws, and the adoption of international standards to facilitate cross border e-commerce and enhance global trade.

What to look out for:

- EDPB and European Commission's final documents on supplementary transfers after Schrems II and SCCs
- Possibility of UK adequacy decision
- Legislative progression in China, India, and Pakistan
- New Zealand Privacy Act enforcement
- New USA Biden-Harris administration increasing call for US federal data protection legislation
- Development of state-level privacy laws
- Additional guidance and documentation from the Brazilian data protection authority

Americas & Caribbean

Key takeaways:

- Third set of modifications to the CCPA
- CPRA ballot proposal passes
- Canada's Bill C-11 introduced in legislature which seeks to amend PIPEDA
- HIPAA Privacy Rule amendments proposed
- ANPD issues first guidance and begins hiring public officials

October

There were several announcements and publications released as part of ongoing privacy discussions across the Americas during October. These included advocacy groups opposing the CPRA in California and discussions of reform in Canada. A third set of proposed modifications to CCPA regulations were released for public comment, and the Federal Communications Commission ('FCC') issued a detailed notice on exemptions to the Pallone-Thune Telephone Robocall Abuse Criminal Enforcement and Deterrence Act ('the TRACED Act'). However, privacy headlines across the Americas in October were dominated by enforcement actions.

In particular, several authorities in the US issued fines or settlements for privacy related violations, including the Office of the Comptroller of the Currency ('OCC'), the Department of Health & Human Services' Office for Civil Rights ('OCR'), the FCC, the Department of Justice ('DoJ'), and the Securities and Exchange Commission ('SEC'). The Federal Trade Commission ('FTC') also reached a settlement regarding alleged false Privacy Shield claims. While most of these settlements and penalties ranged between $1 million to $60 million, the OCC issued one settlement of $400 million for multiple risk and data governance related violations.

The Office of the Privacy Commissioner of Canada also released a report that considered alleged illegal use of facial recognition technology within a shopping mall without consent, and notable fines were issued in Colombia for direct marketing related offences.

November

On 3 November 2020, the CPRA was passed by the Californian electorate. The CPRA seeks to strengthen consumer rights and bring Californian privacy legislation into closer alignment with global practices by, for instance, establishing a state privacy authority. The CPRA was not, however, widely supported by advocacy groups with common concerns being raised regarding a potential negative impact on businesses and whether it goes far enough to adequately protect consumers.

Major changes were also proposed in Canada through Bill C-11 for the Digital Charter Implementation Act, 2020. This bill would enact the Consumer Privacy Protection Act, which in turn would introduce a new privacy regime in Canada, including revised consent requirements, more substantial penalties, and an extension of data subject rights.

Enforcement actions continued this month with notable fines issued in the US and Colombia. In addition, Artificial Intelligence and the Internet of Things were brought into focus through guidance and legislation in the US, and a draft data protection law was sent for debate in Ecuador's National Assembly.

December

December proved to be a busy year for US regulators especially in terms of legal and regulatory reform. The OCR proposed changes to the Health Insurance Portability and Accountability Act of 1996 ('HIPAA') Privacy Rule with a majority of the changes aimed at providing data subjects with more access to their electronic personal health information which was a key focus of the OCR throughout 2020 as evidenced in their enforcement action through the HIPAA Right of Access Initiative.

Regulatory changes continued with the federal banking regulators proposing new data breach notification obligations for banks and the Centers for Medicare and Medicaid Services also proposing a rule that seeks to improve the electronic exchange of health care data.

Additionally, the California Office of the Attorney General launched a public consultation on the fourth set of CCPA Regulations which re-introduced the image of an opt-out button and obligations in relation to the convenience of opt-out methods for consumers, among other obligations.

Enforcement also saw an uptick in December with both state and federal regulators filling lawsuits, levying fines, and instigating investigations. In particular, the issues varied from data breaches and telemarketing violations to inadequate vendor security measures and anticompetitive practices. In addition, discussions continued in the US Senate with regards to the invalidation of the EU-US Privacy Shield and the future of data transfers.

In Canada, the OPC released its reports on findings of one of the biggest breach cases of 2019 with total affected individuals at just over four million victims and issued a series of recommendations. Notably, no fine was issued as the OPC currently lacks authority to do so, however the PIPEDA reform bill which is being discussed in Parliament would change this with penalties of up to CAD 10 million (approx. €6.5 million) or 2% of an organisation's worldwide turnover, whichever is greater.

In Brazil, the data protection authority ('ANPD') issued its first guidance addressing the LGPD with a frequently asked questions addressing a number of issues including the applicability of the LGPD, the legal bases that data controllers may use to process personal data, the rights of data subjects, certain actions that public and private organisations need to take in order to comply with the LGPD, and the ANPD structure and powers. In addition, the ANPD appointed a number of public officials as well as initiated talks with the business sector with the aim of fostering a greater sense of

compliance with the LGDP. Elsewhere in Colombia, the SIC continued to levy robust enforcement decisions for topics ranging from amending personal information without consent to violations of the right to erasure. In addition, data protection authorities in Peru, Colombia, and Brazil issued guidance clarifying enforcement procedure, incident management, as well as data protection in the health sector.

What to look out for:

- Increase in LGPD guidance with ANPD infrastructure developing
- Reintroduction of US State privacy bills
- Enforcement of data sharing and HIPAA Privacy Rule amendments

APAC & the CIS

Key takeaways:

- Draft data protection laws in Singapore, China and South Korea
- Public consultation on APPI
- Significant enforcement action in Singapore
- Entry into force of New Zealand Privacy Act

October

Following on from the previous quarter, discussions of significant legislative reform continued in the APAC region. Most notably, a draft personal information protection law was released in China for public consultation. If enacted, this law will introduce a more standardised and centralised approach to data protection in China, as it generally follows international trends in terms of its scope and structure, as well as the potential for substantial monetary penalties.

The Australian Government announced a review into the Privacy Act 1988 (No. 119, 1988), pressure continued in Indonesia for advancement of the draft data protection law, a consultation was launched in Japan on amendments to the enforcement rules of the Act on the Protection of Personal Information (Act No. 57 of 2003 as amended in 2016) ('APPI'), and a consultation was also launched in South Korea regarding detailed guidance on data protection laws.

In addition, there were many developments in Ukraine including regulations for critical information infrastructure, cryptographic security, and guidance on video surveillance. Multiple orders were also issued by the Ukrainian Parliamentary Commissioner for Human Rights following data protection related inspections.

November

On 2 November 2020, the Singaporean Parliament passed amendments to the Personal Data Protection Act (No. 26 of 2012) ('PDPA') and the Spam Control Act 2007. Key amendments include the introduction of an accountability principle, mandatory data breach notifications, higher penalties, right to data portability, and a legitimate interest exception to consent. The Personal Data Protection Commission ('PDPC') released draft advisory guidelines to assist compliance with the amendments.

Several pieces of guidance were also released in China, covering topics such as AI, cybersecurity, online car-booking, and anti-monopoly measures for the platform economy, and a pilot began for Standard GB/T 35273-2020 on Information Security Technology - Personal Information Security Specification. Meanwhile, a high court in India recognised the right to be forgotten as a right *in rem* and highlighted that, in the absence of legislation, victims may seek appropriate orders to have certain offensive posts erased from public platforms to protect their fundamental right to privacy.

A key trend during November in the region was an increase in enforcement actions. While Singapore continued to be one of the most active jurisdictions for issuing numerous, relatively small fines, there were also significant telemarketing sanctions issued in Macau. The most notable monetary penalty, equating to approximately €5.1 million, was imposed by the Personal Information Protection Commission ('PIPC') in South Korea to a major social media platform. This was the first fine to be issued by the PIPC on an overseas business operator.

December

In the CIS, the Ukraine Parliamentary Commissioner for Human rights released a number of results of inspections on entities to vet their compliance with the data protection legislation. Noteworthy bills were adopted in Russia amending both the general data protection legislation and sector specific laws. In particular, the State Parliament ('Duma') announced that it had adopted a bill amending Russia's anti-money laundering law which aims to regulate the collection and use of biometric data by credit institutions under a new unified biometric system. Furthermore, Duma passed a bill amending the federal data protection law which aims to enhance the protection of data subjects whose personal data has been involved in public circulation.

Key legislation entered in to effect in New Zealand with the Privacy Act 2020 establishing key reforms to the country's data protection regime, including a mandatory data breach reporting obligation, new criminal offences, and expanded extraterritorial scope. Furthermore, in Pakistan, the Ministry of Information and Technology and Telecommunication announced that the draft data protection bill of 2020 has been finalised and has been sent for approval, though a text of the legislation is currently not available to the public. Likewise, in South Korea, the PIPC announced a consultation on amendments to the Personal Information Protection Act 2011 which include a right to request data transmission. Legislative proposals continued in Australia with the government introducing bills on data availability and transparency as well as digital surveillance.

A key focus across the region was the issuance of standards and guidance, specifically in relation to AI, the financial sector, and cybersecurity. In China, new financial standards were announced for payment risks based on Big Data, in the Philippines, the Securities and Exchange Commission issued guidance on a new cybersecurity framework for public consultation, the India Reserve bank proposed various measures to enhance the security controls for digital payments, and finally the Chinese Central Bank released guidelines on cybersecurity in the financial industry.

What to look out for:

- Movement on the data protection bills in China, Indonesia, and Pakistan
- Enforcement of New Zealand Privacy Act 2020
- Amendments to India's PDP Bill following the JPC's recommendations

- Guidance from Singapore's PDPA and NZ's OPC in relation to the recent legislative changes
- More doxxing cases being heard in Hong Kong
- Data protection amendment laws passing through the legislative stages in both South Korea and Russia
- Continued review of Australia's Privacy Act

EMEA

Key takeaways:

- Rwanda draft data protection bill approved
- African Union framework agreed upon
- EDPB guidance on transfers and supplementary measures after Schrems II
- Brexit and UK-EU trade agreement with provisional cross border data flows
- Consultation on revision to Israeli privacy law

October

In Switzerland, the revised Federal Act on Data Protection 1992 ('FADP') was published, on 6 October 2020, in the Federal Gazette. Until 14 January 2020, it will potentially be subject to a public referendum and a possible date of entry into force has yet to be decided. The revisions are, though, significant and will establish several new obligations for organisation, particularly regarding matters such as impact assessments and Privacy by Design, if entered into effect.

In the EU, data protection related guidance primarily focused on Brexit, AI, and Schrems II. The guidance on Brexit and Schrems II tended to emphasise best practices that had been identified previously, while the AI discussion continued to be broad and touch on numerous sectors and concerns. Alongside this guidance, several data protection authorities issued fines. Authorities in Spain and Romania remained particularly active, although largely issuing smaller monetary penalties. The most significant fines, of tens of millions of euros, were announced in the UK and Germany.

The Privacy Protection Authority ('PPA') in Israel was also active, releasing guidance on data processing and service providers as well as privacy protection officers. Meanwhile, Rwanda's data protection bill continues to advance, having been approved by Cabinet.

November

The most significant development in November was the release of proposed detailed guidance and SCCs by the EDPB and European Commission, respectively, in light of the Schrems II. However, beyond these efforts to start addressing international data transfers, November saw several other important milestones in Europe and beyond. In particular, the European Commission presented a new data governance regulation, the EDPB adopted its first cross-border dispute resolution decision under Article 65 of the GDPR, and draft Article 28 SCCs for controllers and processors within the EU were released.

Furthermore, a revised draft of the ePrivacy Regulation was issued on 4 November by the German Presidency of the Council of the European Union. By the end of the month, though, it was clear that the revised draft was still not perceived to be adequate by Member States.

Enforcement actions continued in the EU, and particularly in Spain as well as France, Italy, Guernsey, Romania, Norway, Sweden, and the UK. The most substantial fine of €12.2 million was issued in Italy. A key discussion point, though, was the reduction and overturning of fines in Sweden and the Netherlands.

Outside of Europe significant public consultations began in Israel and the Abu Dhabi Global Market ('ADGM') regarding amending and updating their privacy legislation. An initiative for harmonising privacy legislation was started by the African Union. Previous harmonisation efforts by the African Union have, though, met with limited success, such as the 2014 African Union Convention on Cyber Security and Personal Data Protection, which has thus far only received 14 signatures and eight ratifications.

December

Following on from the previous month, the None of your business-European Center for Digital Rights ('NOYB') issued comments on the EDPB guidance on surveillance and supplementary transfers post Schrems II. In particular, NOYB outlined that all instruments of transfer should lead to an equivalent level of protection, reinforced the importance of not undermining GDPR compliance, and stipulated the legal obligations for both data controllers to suspend or end transfers where adequate protection cannot be guaranteed. Further to this, NYOB highlighted the importance of clear guidance so that organisations can ensure compliance.

With the Brexit transition period looming a number of authorities in Norway, France, Ireland as well as Germany published statements on GDPR applicability in the UK after Brexit including authorities in Norway, Ireland, and Germany. Most supervisory authorities directed organisations to the previously mentioned EDPB supplementary transfers guidance with the Ireland Data Protection Commission specifically citing the adoption of SCCs as the most plausible mechanism reinforcing the caveat of the need for equivalent level of protection. Equally the UK Information Commissioner's Office ('ICO') noted that SCCs are the best way to keep data flowing on EU-approved terms until an adequacy decision can be reached. Importantly, the UK and the EU announced that they had reached a draft EU-UK Trade and Cooperation Agreement ('TCA') with provisions included that provide for the continued free flow of personal data from the EU and EEA EFTA States to the UK until adequacy decisions are adopted.

December saw Togo's National Assembly, taking an important step forward in privacy reform with the creation of its new data protection authority, the IPDCP, which will have investigative, corrective, and enforcement powers in support of the Government's policy on the protection of personal data.

What to look out for:

- Ongoing issues surrounding Brexit and potential of an adequacy decision,
- Revised guidance from the EDPB, and final SCCs from the European Commission
- Results of public consultations on data protection laws in Israel and ADGM
- Possible pan-African data protection framework
- Draft data protection bill in Nigeria coming into effect

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

Insights

- USA: OCR issues proposed modifications to HIPAA Privacy Rule, focusing on access rights and care coordination
- Brazil: ANPD issues first guidance addressing LGPD
- Uganda: A comparison between Uganda's data protection framework and the GDPR
- EU: New SCCs and some key provisions
- Australia: Privacy Act Review
- International: Data privacy harmonisation in Africa - Progress, challenges, and predictions
- EU: New model on draft SCCs under Article 28 of the GDPR
- Canada: Bill C-11 and Canada's federal privacy modernisation
- China: Cybersecurity and privacy enforcement
- New Zealand: The Privacy Act 2020 - What to expect from the OPC
- EU: EDPB guidelines on Post-Schrems II Part two: What are Supplementary Measures?
- China: Personal Information Protection Law in context
- California: What CPRA will mean for businesses, consumers, and US privacy landscape
- EU: EDPB recommendations post-Schrems II Part 1: Supplementary measures
- USA: Privacy advocate groups release data protection plan for Biden Administration
- Spain: AEPD guidance on Data Protection by Design and Default
- Egypt: New data protection law and what to expect
- Japan: Privacy governance guidebook
- France: CNIL guidance on online cookies and trackers

Webinars

- New Canadian Privacy Laws ('Bill C-11'): The Consumer Privacy Protection Act and its Business Impacts
- The Revised Swiss FDPA and the GDPR: key differences and their implications for compliance
- GDPR Access and Erasure Rights: How to manage DSARs and Erasure Requests in your company
- New Zealand: New Privacy Act, New Obligations - What all Businesses Need To Know
- Schrems II Fallout Continued: Reaction and Analysis to NEW Standard Contractual Clauses and EDPB Schrems II Recommendations
- Schrems II Fallout - Dealing With International Transfers Post-Schrems II & Reaction to the EDPB's Recommendations
- CPRA: Reaction & Analysis

Portals & Comparisons

- Retention Schedules
- Artificial Inteligence
- Brexit Portal
- Thai PDPA Portal
- ePrivacy Regulation Portal
- POPIA Portal
- Privacy Index