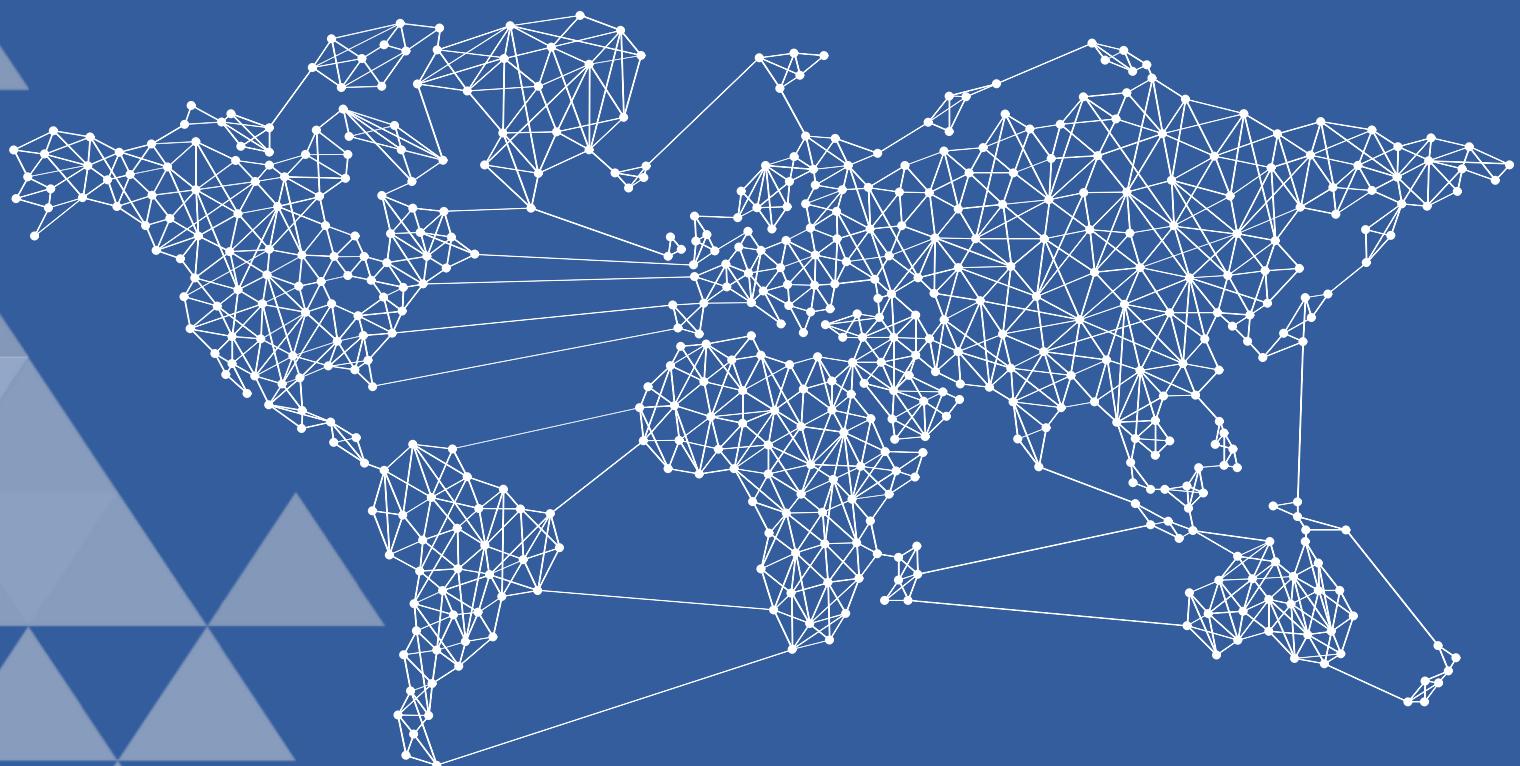


OneTrust DataGuidance

Privacy Review

Q1 2020



About the report

2020 has already been a significant year for data protection developments worldwide. Major changes have been proposed, debated, and introduced in some of the most and least active jurisdictions. Authorities have been busy releasing guidance on key topics ranging from binding corporate rules to working from home, while enforcement actions continue to be of central concern. COVID-19, the Coronavirus, has also had a notable global impact, including causing delays to guidance and legislation. OneTrust DataGuidance's Privacy Analyst team considers the most significant developments over the first three months 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™

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

Image production credits

Cover page: pop_jop / Signature collection / istockphoto.com

Global Regulatory Research Software

40 In-House Legal Researchers
500 Lawyers Across 300 Jurisdictions

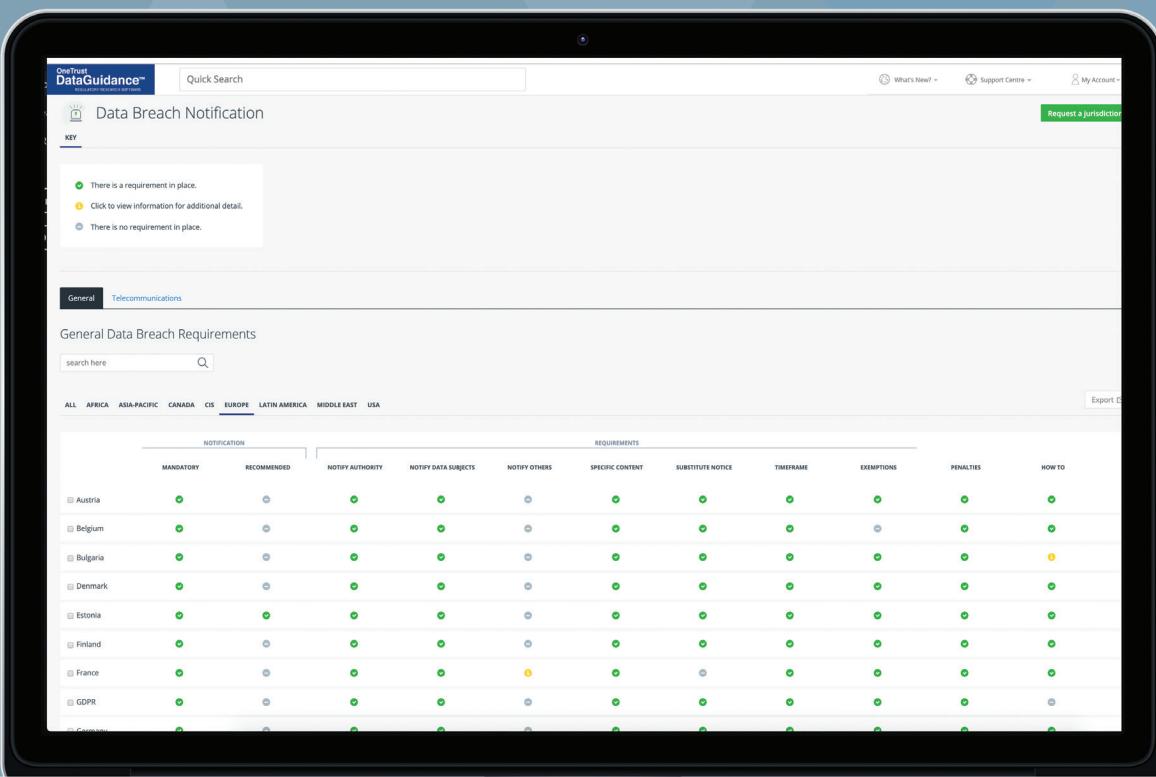
With focused guidance around core topics, Comparison Charts, a daily customised news service and expert analysis, OneTrust DataGuidance provides a cost-effective and efficient solution to design and support your privacy program

 Legal Guidance & Opinion

 Law Comparison Tools

 Breach & Enforcement Tracker

 Ask-An-Analyst Service



The screenshot displays a comparison chart for 'Data Breach Notification' requirements across 300 jurisdictions. The chart is organized into columns for 'NOTIFICATION' (Mandatory, Recommended) and 'REQUIREMENTS' (Notify Authority, Notify Data Subjects, Notify Others, Specific Content, Substitute Notice, Timeline, Exemptions, Penalties, How To). Each jurisdiction is listed with a green circle indicating a requirement is in place, a blue circle indicating a recommendation, or a yellow circle indicating no requirement is in place. The jurisdictions listed include Austria, Belgium, Bulgaria, Denmark, Estonia, Finland, France, and GDPR.

SCAN TO ACCESS
FREE TRIAL
Use your camera or a QR code reader



OneTrust
DataGuidance™
REGULATORY RESEARCH SOFTWARE

Global

Key takeaways:

- California Consumer Privacy Act of 2018 ('CCPA') comes into effect, UK begins transition out of EU, and Uruguay transforms its approach to data protection
- Laws passed in Egypt and the Republic of North Macedonia
- Major amendments proposed in Japan, South Korea, Malaysia, and Mexico
- New bills introduced in several US States, Indonesia, and Vietnam
- Coronavirus creates challenges and ignites privacy debates around the world

Global privacy legislation advances in key jurisdictions

The coming into effect of the CCPA at the start of the year established substantial obligations for organisations doing business in California and ushered in a wave of Federal and State level privacy-related bills across the US. Most of these bills are still in their early stages, however it is expected that the CCPA will have a lasting impact beyond its territorial scope. Uruguay also took major steps in strengthening its data protection provisions. In what can be considered part of a global trend inspired by the EU's General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR'), Uruguay set out measures for data breach notifications, Data Privacy Impact Assessments ('DPIAs'), and data protection officer ('DPO') appointments.

Similarly, major amendments that echo provisions in the GDPR were proposed in Japan and South Korea. Amendments were also discussed in Hong Kong and proposed in Malaysia and Vietnam, and laws were passed in Egypt and North Macedonia, with all of these jurisdictions likewise noting that developments were intended to meet international standards that have been set by the GDPR. Furthermore, a commencement date of 1 November 2020 was scheduled for New Zealand's privacy bill.

Trade and data transfers

The US led developments related to data transfers, with the Federal Trade Commission ('FTC') announcing several settlements related to allegedly false Privacy Shield certifications and the U.S. Department of Commerce International Trade Administration introducing the appointment of the third accountability agent in the US under the Asia-Pacific Cross-Border Privacy Rules ('APEC CBPR') system. Furthermore, the implementation of the US-Mexico-Canada Agreement ('USMCA') began with acts signed in the US and Canada. Meanwhile, Russia announced two notable fines related to data localisation requirements and the UK released an explanatory framework regarding its request for an EU adequacy decision following Brexit.

On 21 January 2020, ministers from Chile, New Zealand, and Singapore announced the substantial conclusion of the Digital Economy Partnership Agreement ('DEPA') negotiations. Although DEPA will need to be signed before coming into effect, it is the latest of several

notable international trade agreements that contain substantial provisions for personal data transfers, including the USMCA. DEPA sets out some of the most significant requirements for personal information protection, cybersecurity, online consumer protection, and data flows to be found in an international trade deal. While bespoke mechanisms such as EU adequacy decisions, Privacy Shield, or APEC CBPR, currently dominate international personal data transfer agreements, such broader trade deals may be on the verge of becoming a more active player in global data flows.

Coronavirus

COVID-19 ('Coronavirus') shifted events, focus, and discussions throughout March. Data protection authorities from around the world have been issuing guidance on a regular basis since, which ranges from addressing specific concerns on employee health, tracking, and working from home, to more general warnings and overviews of privacy and the Coronavirus. There have also been notable legislative developments in Germany and Paraguay. In some jurisdictions, including Germany, heated debates have been started as questions related to civil liberties, individual privacy, and managing the crisis come to the forefront.

While there have been several data protection authority office closures and delays to publications, privacy developments have continued in both the most and least affected jurisdictions.

What to look out for:

- Coronavirus related delays and debates
- CCPA proposed regulations and the progress of amendments in Japan and South Korea
- The development of Australia's Consumer Data Right system and New Zealand's privacy bill
- Whether US State and Federal privacy bills progress
- Breach notification requirements are being introduced or strengthened around the world

AUTOMATE CCPA CONSUMER PRIVACY RIGHTS

Simplify the manual process of fulfilling a request through robotic process automation workflows

-  User Request Portal
-  Data Discovery & Deletion
-  Toll Free #
-  Identity Verification
-  Opt-Out of Sale



JOIN THE CCPA MASTER CLASS SERIES TO LEARN MORE

FREE EXPERT-LED WEBINAR SERIES

Webinar Topics Include:

Consumer Rights | Do Not Sell | Identity Verification
Targeted Data Discovery™ | Data Mapping | Awareness Training
Cookie Banner Management | Vendor Management

REGISTER | [ONETRUST.COM/CCPA](https://onetrust.com/ccpa)

Americas & Caribbean

Key takeaways:

- CCPA enters into effect and changes US privacy landscape
- Major legislative reforms happening in Latin America with new requirements proposed in several jurisdictions
- Notable enforcement actions in US and Argentina

January

On 1 January 2020, the CCPA entered into effect and fundamentally changed the approach to personal data protection in the State of California as well as the US more broadly. The CCPA sets out several obligations for organisations that conduct business in California, and particularly emphasises transparency, privacy policies, and restrictions on the selling of personal information. In the wake of the CCPA, several personal data protection related bills were proposed at the State level across the US in January, including in New York, Florida, New Hampshire, Vermont, Virginia, and Washington. In addition, provisions amending data breach notifications came into effect in Texas, Illinois, and Oregon, and the National Institute of Standard and Technology ('NIST') released its first Privacy Framework.

The US-Mexico-Canada Agreement ('USMCA') also gained significant traction this month with the US signing the implementation act for the agreement into law. While the FTC announced a series of settlements related to the Privacy Shield, a \$550 million settlement was made by a social media organisation with a class of plaintiffs in order to address allegations that the organisation had violated the Illinois Biometric Information Privacy Act of 2008.

In Chile, a newer version of the data protection bill was announced on 9 January 2020, which would transform the current Law No. 19.628 on the Protection of Private Life 1999. The Bill is intended to bring Chilean data protection legislation into closer alignment with international standards and the EU's GDPR. Late in the month, the Argentinian data protection authority ('AAIP') issued one of its most substantial fines to date, of approximately €45,000, to a telephone company for violations related to the Do Not Call registry. Authorities in Argentina and Uruguay also jointly released guidance for DPIAs in recognition of the international Data Protection Day.

February

Significant changes came in Uruguay as Decree No. 64/020 on the Regulation of Articles 37-40 of Law No. 19.670 of 15 October 2018 and Article 12 of Law No. 18.331 of 8 November 2008 ('the Decree') was promulgated on 21 February 2020. The Decree extends the territorial scope of Uruguay's data protection legislation, and introduces new obligations for breach notifications, data security, DPIAs, DPO appointments, and measures for Privacy by Design

and Privacy by Default. A bill was also introduced in Mexico, on 11 February 2020, that would establish new data breach notification requirements.

CCPA developments continued when the California Attorney General ('AG'), Xavier Becerra, released a modified text of the proposed regulations. The modifications included clarifying definitions of 'personal information' and 'employment-related information', the inclusion of 'opt-out' buttons that organisations may utilise, as well as changes to the procedures regarding requests to know or delete and the exemptions afforded to service providers. While State level privacy related bills continued and more were introduced in Arizona, Hawaii, Maryland, Nebraska, New Jersey, and Wisconsin, there were also several reports of health-related data breaches from organisations across the US.

March

Guidance on the Coronavirus and its impact on data protection was released in Argentina, Bermuda, Canada, Cayman Islands, Mexico, Peru, USA, and emergency Coronavirus laws are being discussed and passed in Brazil, Paraguay, Uruguay, and elsewhere. Although the impact of the Coronavirus has been extensive, there were still several other developments in March.

The Act to Implement the United States-Mexico-Canada Agreement received royal assent in Canada, and it was announced that NCC Group North America would be the US' third accountability agent under the Asia-Pacific Cross-Border Privacy Rules ('APEC CBPR') system.

The data security provisions of the New York Senate Bill 5575B for the Stop Hacks and Improve Electronic Data Security ('SHIELD') Act entered into effect on 21 March 2020. A US Federal bill for the Consumer Data Privacy and Security Act of 2020 was introduced by Senator Jerry Moran, and a relatively unique bill on neurodata rights was proposed in Minnesota. There were further health data breaches, FTC settlements related to Privacy Shield, and State privacy-related bills progressed. The California AG, Xavier Becerra, also published, on 11 March 2020, the second set of modifications made to the proposed regulations under the CCPA for public comment. However, the main data protection concerns in the US, and elsewhere in the Americas & Caribbean region, were related to civil liberties and measures to combat Coronavirus.

What to look out for:

- Coronavirus impact on whether laws come into effect, and most notably the potential postponement of Brazil's Law No. 13.709 of 14 August 2018, General Personal Data Protection Law (as amended by Law No. 13.853 of 8 July 2019) ('LGPD')
- Progress of US bills at both State and Federal level
- Movements towards GDPR-styled data protection in Latin America and how this may affect EU adequacy decisions

APAC & the CIS

Key takeaways:

- Significant legislative reform in progress in Japan, Malaysia, New Zealand, and South Korea
- Vietnam and Indonesia propose new personal data protection bills
- Less expansive but notable developments in privacy legislation and guidance in China, Russia, and Kazakhstan

January

Early in January, South Korea announced major amendments to its main three data protection laws in the form of the Data 3 Act. The amendments are expected to come into effect this summer and will centralise data protection regulations within the Personal Information Protection Act 2011 ('PIPA') and under the remit of the Personal Information Protection Commission ('PIPC'). The Data 3 Act will also introduce several requirements for pseudonymised personal data and credit information and is directly aimed at increasing the chances of South Korea obtaining an adequacy agreement with the EU. Although less advanced, similarly sweeping amendments to core data protection legislation came to the forefront in Hong Kong in the form of a discussion paper in the Legislative Council of Hong Kong ('LegCo'). The discussion paper considers several amendments to the Personal Data (Privacy) Ordinance 1996 as amended in 2013 (Cap. 486) ('PDPO'), including mandatory breach notifications, regulations on data processors, and new data retention requirements.

Near the end of January, the draft of the Personal Data Protection Act ('the PDP Bill') was submitted by the President of Indonesia, Joko Widodo, to the Chairperson of the Indonesian House of Representatives ('DPR'). The PDP Bill, if enacted, will bring major changes to data protection in Indonesia as it sets out data subject rights, legal bases for data processing, accountability requirements, and restrictions on international data transfers.

February

A draft decree on personal data protection was released on 5 February 2020 for public consultation in Vietnam. The Draft Decree sets out the principles of data protection, which include purpose limitation, data security, accuracy and quality of data, and data subjects' right of information about any processing activities, as well as requiring the registration of sensitive data processing and cross-border transfers of personal data of Vietnamese citizens. While Vietnam thus began the process of establishing its first general data protection law, proposed amendments to the Personal Data Protection Act 2010 ('PDPA') were published in Malaysia. These amendments would introduce requirements for DPOs, Privacy by Design, data portability, a Do Not Call registry, and the possible introduction of civil litigation. As has been the case in many other jurisdictions, these amendments explicitly refer to standards set by the EU's GDPR. In Australia, development continued on the Consumer Data Right ('CDR') system with the release of the Office of the Australian Information Commissioner's ('OAIC') CDR guidelines. Although the CDR system will only be implemented in the banking sector from July 2020, it will then

be extended to other sectors of the economy, starting with energy and telecommunications. The OAIC CDR guidelines set out best practices and also consider the CDR system alongside the Australian Privacy Principles established by the Privacy Act 1988. With a similarly unique approach to personal data protection, Russia announced, on 13 February 2020, that fines of €58,000 related to data localisation requirements had been issued to two well-known international social media companies.

Notices on the Coronavirus and data protection began to be released this month in China. These notices tend to emphasise the importance of data subject consent as well as the value of Big Data in combatting the spread of the virus.

March

The Coronavirus began to have a broad impact across the region, with guidelines and other material released in most jurisdictions. In particular, New Zealand and Hong Kong issued detailed guidance on employment and the Coronavirus.

Early in March, however, significant proposed amendments to Japan's Protection of Personal Information Act (Act No. 57 of 2003 as amended in 2016) ('APPI') were released. The proposals include introducing data breach notification requirements, expanding the right to request the cessation of data processing, increasing penalties, and establishing new restrictions on data transfers. Not long later, on 18 March 2020, the Office of the Privacy Commissioner of New Zealand ('OPCNZ') announced that the privacy bill will commence on 1 November 2020. Similar to the APPI amendments, the New Zealand privacy bill addresses breach notifications, cross-border transfers, and sanctions, and is expected to usher in a new era of data protection in the jurisdiction. On the same day, Kazakhstan's Mazhilis, the lower house of Parliament, passed the digital technology regulation bill through its first reading. The Bill aims to either introduce a new body or establish an existing one as the data protection authority for Kazakhstan while also addressing a wide range of digital related concerns.

A draft regulation for electronic system operators was submitted in Indonesia, and, in China, a finalised draft of the updated Standard GB/T 35273-2020 on Information Security Technology – Personal Information Security Specification ('the Specification') was released. The Specification provides a set of non-binding but far reaching recommendations that provide nuanced parallels with the GDPR. In late March, a bill on digitalising healthcare joined several other bills in Russia that have been submitted to the Duma. A draft bill on cybercrime was also introduced in Fiji, which would bring Fijian law into closer alignment with the Budapest convention on cybercrime.

What to look out for:

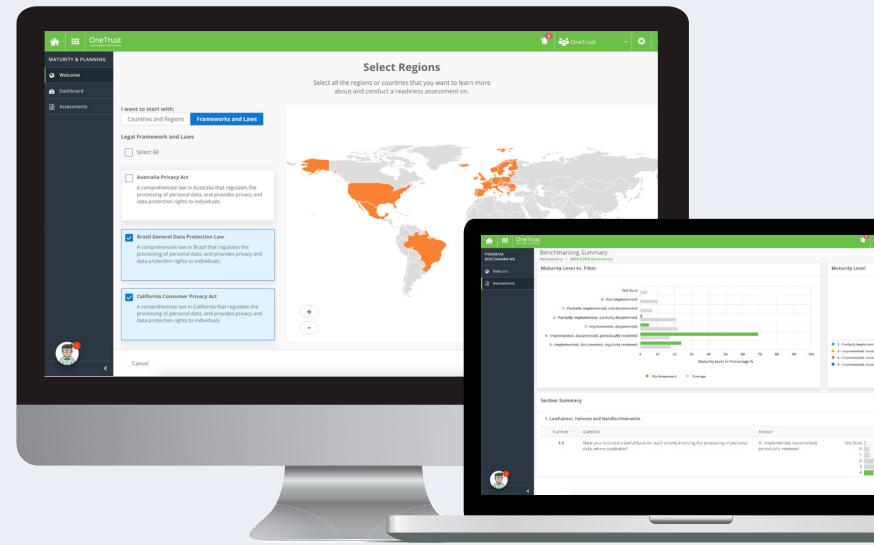
- Japan APPI amendments expected in June
- South Korea amendments expected in July/August, and details of amendments to Enforcement Decrees related to the Data 3 Act will be released before this time
- Thailand's Personal Data Protection Act set to come into full effect on 27 May 2020
- Impact and development of Consumer Data Right system in Australia



OneTrust Maturity & Planning and Program Benchmarking Solutions

DEMONSTRATE ACCOUNTABILITY & ORGANIZATIONAL READINESS, PRIORITIZE REQUIREMENTS FOR COMPLIANCE & PROVIDE EXECUTIVE-LEVEL VISIBILITY

- Quickly assess your organizational readiness for compliance and plan your privacy programs accordingly
- Built-in readiness assessment templates across privacy and security frameworks such as the CCPA, GDPR, Privacy Shield, ISO 27001, NIST and APEC CBPR
- Powered by the OneTrust DataGuidance Regulatory Research Portal, the most comprehensive source for privacy, security, and third party risk research



CHOOSE FRAMEWORK

Assess maturity against relevant laws & frameworks



ASSESS MATURITY

Guidance and collaboration in the assessment process



BENCHMARK

Benchmark your maturity against industry peers



PLAN REMEDIATION

Identify gaps with intelligence engine recommendation for remediation



REPORT ON PROGRESS

Dashboards and reports to demonstrate progress to board and executives



RE-ASSESS OVER TIME

Layer on new regulations and frameworks as your business and the regulatory landscape evolves



READY TO GET STARTED? **TRY FREE FOR 14 DAYS AT [DATAGUIDANCE.COM](https://dataguidance.com)**

OneTrust DataGuidance™
REGULATORY RESEARCH SOFTWARE

ATLANTA | BANGALORE | HONG KONG | LONDON | MELBOURNE
MUNICH | NEW YORK | SAN FRANCISCO | SÃO PAULO

OneTrust is the #1 most widely used privacy, security and third-party risk technology platform trusted by more than 4,500 companies to comply with the CCPA, GDPR, ISO27001 and hundreds of the world's privacy and security laws. OneTrust's primary offerings include OneTrust Privacy Management Software, OneTrust PreferenceChoice™ consent and preference management software, OneTrust Vendorpedia™ third-party risk management software and vendor risk exchange and OneTrust GRC integrated risk management software. To learn more, visit OneTrust.com.

Copyright © 2020 OneTrust LLC. All rights reserved. Proprietary & Confidential.

EMEA

Key takeaways:

- New laws in Egypt and North Macedonia
- Revised draft of ePrivacy Regulation released
- Guidelines on several topics published by CNIL and the ICO
- Potential for long term impact of coronavirus measures

January

On 31 January 2020, the UK officially began the transition phase of its departure from the EU. During the transition period, which is set to last until 31 December 2020, the UK's data protection regime remains aligned to the GDPR. However, several data protection authorities have already begun issuing guidance to address the concerns of how Brexit may affect data flows. For the most part, these pieces of guidance highlighted and focused on the continuing application of the GDPR until the end of the year. The UK's Information Commissioner's Office ('ICO') also released, on 21 January 2020, an Age Appropriate Design Code, which outlines the key standards that online service providers should meet to protect children's privacy.

The Hellenic data protection authority ('HDPA') issued, on 27 January 2020, its opinion on the compatibility of the GDPR with Law No. 4624/2019 on the Personal Data Protection Authority, Implementing the General Data Protection Regulation (Regulation (EU) 2016/679) and Transposing into National Law Data Protection Directive with Respect to Law Enforcement (Directive (EU) 2016/680) and Other Provisions ('the Law'). In particular, the opinion notes that several aspects of the Law are incompatible with EU legislation and suggests that Articles 24-26 of the Law conflict with the GDPR by attempting to set new legal bases for processing personal data.

February

The Parliament of the Republic of North Macedonia adopted, on 16 February 2020, the Law on Personal Data Protection 2020 ('the Law on PDP'). Even though North Macedonia is not an EU Member State, the Law on PDP explicitly seeks to harmonise Macedonian legislation with the GDPR. There are, however, certain differences with the GDPR, such as that direct marketing requires data subject consent, and that health, genetic, and biometric data processing requires prior approval from the data protection authority, even when there is data subject consent.

In the EU, France's data protection authority ('CNIL') was particularly active in February and released a series of important pieces of guidance covering binding corporate rules ('BCRs'),

codes of conduct, and the use of contracts as a legal basis for data processing. The ICO similarly released guidance on codes of conduct, as well as a guide for certifications.

Towards the end of the month, it was announced that the Egyptian House of Representatives had passed the country's first law on data protection. This law will introduce data subject rights, set out obligations for data controllers and processors, establish a Personal Data Protection Center, and stipulate strict requirements for data transfers. The law is currently awaiting issuance by the Egyptian President.

March

The dominating headlines across EMEA, and Europe in particular, related to the Coronavirus. Several supervisory authorities released guidance and there was a particular emphasis on working from home. Outside of Europe guidance was issued in, among other places, Dubai, Israel, Morocco, Nigeria, and South Africa. One of the most notable Coronavirus related developments have been Amendments to the Infection Protection Act in Germany, which were adopted, on 23 March 2020, by the Federal Cabinet. These amendments have sparked heated debates as they could have a significant impact on individual privacy, particularly in relation to transport and the identification of travellers.

Beyond the Coronavirus, there were major developments including the release of a revised text of the Regulation concerning the Respect for Private Life and the Protection of Personal Data in Electronic Communications and Repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) ('the Draft ePrivacy Regulation'). While the re-emergence of the Draft ePrivacy Regulation is significant, how it will develop and whether it will come into effect remain to be seen. Another ongoing concern that made small steps towards clarity came when the UK's Department for Digital, Culture, Media & Sport published, on 13 March 2020, its explanatory framework for adequacy discussions. The framework confirms that the UK will seek an adequacy decision from the EU after Brexit, and further details plans to implement GDPR provisions into UK legislation.

The Coronavirus, however, is having the most significant impact with several authorities closing buildings and delaying their activities. One such example is CNIL postponing its final recommendations on cookies and other trackers until a calmer time.

What to look out for:

- The impact of the Coronavirus and what may be postponed
- Whether strict approaches to combatting the Coronavirus in Germany and Israel, among other jurisdictions, have a lasting impact
- How the EU will negotiate adequacy discussions going forward, particularly as jurisdictions around the world move closer to GDPR styled approaches to data protection

Further reading:

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

Insights

- International: COVID-19: Q&A with William Long, Partner at Sidley Austin (and the associated OneTrust DataGuidance Coronavirus webinar series)
- California: Service providers and the CCPA
- Greece: HDPA's Opinion may signal need for "complete revamp of the Law"
- New Zealand: Privacy bill reflects new needs in digital age
- Indonesia: Current and upcoming developments to data protection framework
- EU: Opinions of the supervisory authorities on data protection and COVID-19
- UK: DCMS publishes Explanatory Framework in support of post-Brexit data transfers with the EU
- USA: Senator introduces comprehensive federal data privacy bill
- Japan: Cabinet proposes bill to amend APPI
- International: Concerns about Coronavirus and its spread should "not override privacy and security laws"
- UK: ICO issues guidance on codes of conduct and certification
- New York: Key obligations for businesses under SHIELD Act
- International: The coronavirus privacy dilemma
- Australia: OAIC's CDR guidelines recommend holistic approach to compliance
- Uruguay: Decree on protection of data published in Official Gazette
- France: CNIL releases guidance on BCRs and codes of conduct
- Malaysia: PDPA amendments include introduction of data breach reporting
- Republic of North Macedonia: New law is "almost entirely aligned with GDPR"
- EU: Navigating Brexit data protection uncertainty, risks, and options
- South Africa: Update on the status of POPIA

Comparisons

- US State Law Tracker
- Data Breach Notification
- California Consumer Privacy Act portal
- Data Transfer Agreements in the Data Transfers portal

Research and reports

- GDPR v. Australian Privacy Act
- GDPR v. China's CSL and Specification
- GDPR v. Nigeria Data Protection Regulation
- AG's Second Set of Modified CCPA Proposed Regulations

PRIVACYCONNECT ONLINE EVENTS

Focus on regulatory requirements, updates, and trends while learning how to implement in practice

 Earn 2 CPE Credits

 Network with Professionals

 Share Best Practices for Compliance

 Engage in a Panel Discussion



REGISTER FOR A FREE EXPERT-LED
VIRTUAL EVENT IN YOUR CITY

REGISTER | PRIVACYCONNECT.COM

