AN OFFERING FROM BDO'S
GLOBAL DATA PRIVACY PRACTICE

PRIVACY INSIGHTS 2023

BDO

FOREWORD

Privacy and data protection legislation continues to evolve across the world. Recent developments, like the EU-U.S. Data Privacy Framework, China PIPL, and the shifting landscape of U.S. privacy laws has organisations of all sizes struggling with staffing, process, and technology to manage their global privacy and data protection programmes.

BDO publishes an annual Privacy Insights Whitepaper, Global Privacy Resources Guide, and PrivacyWatch® as three complementary resources that allow organisations to stay abreast of changing regulations and laws.

While most organisations recognise the importance of data privacy compliance, they struggle with operationalising the privacy programme to effectively address the global patchwork of privacy obligations. Compounded by the increase in security risk due to cyber-attacks and ransomware, it is more important than ever for organisations to enhance and maintain their data protection and privacy compliance programmes. BDO's DPO-as-a-Service and Data Protection Managed Services (DPMS) offer right-sized solutions to address global data protection compliance.

Privacy professionals must maintain up-to-date knowledge of their organisation's obligations, along with a network of trained peers, to effectively manage privacy compliance. BDO's Data Protection Academy enables professionals to address their organisation's privacy challenges. As an official training partner of the International Association of Privacy Professionals (IAPP), the Academy's trainers provide education regarding privacy principles and compliance for data protection professionals.

This whitepaper focuses on data privacy regulatory insights around the globe and how BDO helps our clients to address the complex and dynamic data protection landscape.

Karen A. Schuler,
Partner, BDO Global Privacy
& Data Protection

INTRODUCTION

Another year has passed and once again privacy and data protection developments flood in from around the globe.

Regulators were focused on cookie compliance and cross-border transfer this year, as demonstrated by the following:

- Hefty fines in France and decisions from multiple regulators that Google Analytics violated cross-border transfer requirements
- Companies raced to implement the new EU Standard Contractual Clauses (SCCs) and the UK's standard contractual agreements known as the International Data Transfer Agreement ("IDTA")
- U.S. President Joe Biden signed an Executive Order to establish the EU-U.S. Data Privacy Framework which will be under consideration by European regulators as a valid transfer mechanism
- The Cyberspace Administration of China (CAC) released a long-awaited draft of China's Standard Contractual Clauses

The trend of enhanced privacy laws continues:

- Quebec introduced Bill 64 which became effective in September 2022 and is similar to the EU GDPR
- The U.S. Congress proposed a bipartisan privacy law called the American Data Privacy and Protection Act
- Companies prepare for multiple U.S. state laws which are set to take effect in 2023 in California, Colorado, Connecticut, Utah, and Virginia

Privacy and data protection legislation is complex and evolving, with endless developments applicable to jurisdictions around the globe.

COOKIE COMPLIANCE INSIGHTS

2023 and beyond – A "cookieless" future

Google has announced plans to block third-party tracking cookies in their Chrome browser. While implementing this change has been delayed several times (at the time of this writing, the change will take effect in the second half of 2024), the direction is clear – third-party tracking cookies will eventually be blocked.
With that in mind, many organisations are beginning to investigate "server-side" tracking strategies, where cookies and other tracking technologies are implemented by the web server rather than the client browser. This transition, however, will not release an organisation from privacy and consent obligations. Arguably, the evolution towards server-side tracking might increase privacy risks, given the increased potential for cross-platform data collection and sharing. Regulations like the GDPR and CPRA are technology-agnostic. The basic principles of Notice, Transparency, and Consent still apply.

Cookie, Banner, and Pixel Compliance

Tracking website visitors provides many benefits, including leveraging web analytics to support a digital marketing strategy, personalisation of the website experience, and targeting content based on user activities across multiple websites.

Web tracking is used to build user profiles for advertising and other purposes. On the other hand, core privacy principles like Notice and Consent require that users be made aware of any tracking system used by a website. Organisations meet these requirements by maintaining current and accurate Privacy Notices and ensuring the appropriate procedural and technical measures are in place to honour the commitments made in the Notice. For example, if a Privacy Notice claims "We do not sell personal data", the data collected through tracking technologies must not be shared with third parties. And yet, in many cases, such technologies are implemented for precisely that purpose – to collect, share, and monetise personal data.

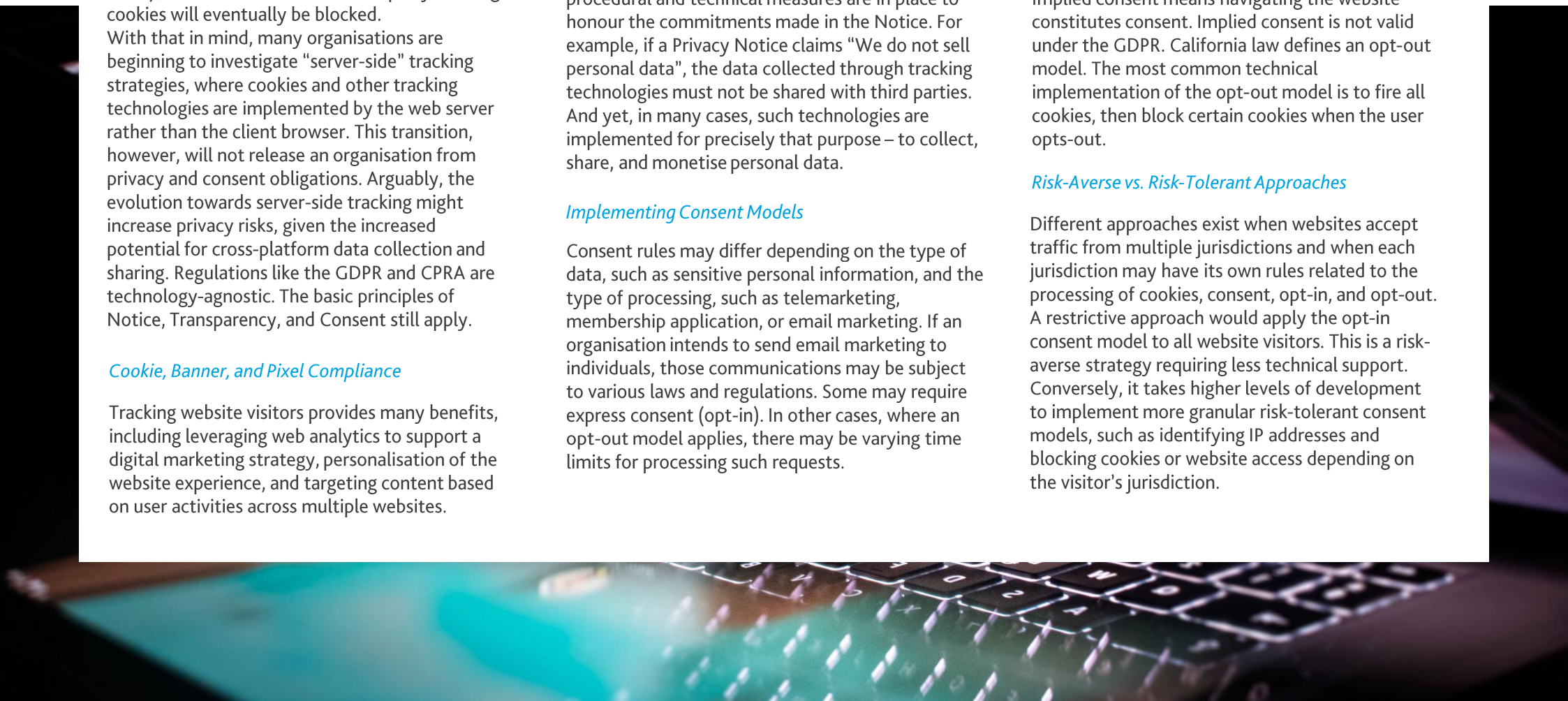
Implementing Consent Models

Consent rules may differ depending on the type of data, such as sensitive personal information, and the type of processing, such as telemarketing, membership application, or email marketing. If an organisation intends to send email marketing to individuals, those communications may be subject to various laws and regulations. Some may require express consent (opt-in). In other cases, where an opt-out model applies, there may be varying time limits for processing such requests.

Many organisations implement geolocation rules to infer user location and apply appropriate consent models. Regulations like the GDPR, and Brazil's LGPD, require explicit opt-in. To implement explicit opt-in consent, only strictly necessary cookies should fire first, then users and visitors would have the option to opt-in to all other types of cookies. Implied consent means navigating the website constitutes consent. Implied consent is not valid under the GDPR. California law defines an opt-out model. The most common technical implementation of the opt-out model is to fire all cookies, then block certain cookies when the user opts-out.

Risk-Averse vs. Risk-Tolerant Approaches

Different approaches exist when websites accept traffic from multiple jurisdictions and when each jurisdiction may have its own rules related to the processing of cookies, consent, opt-in, and opt-out. A restrictive approach would apply the opt-in consent model to all website visitors. This is a risk-averse strategy requiring less technical support. Conversely, it takes higher levels of development to implement more granular risk-tolerant consent models, such as identifying IP addresses and blocking cookies or website access depending on the visitor's jurisdiction.



COOKIE COMPLIANCE INSIGHTS (continued)

Furthermore, cookie consent is not a one-time choice. Consent must be both freely given and able to be freely withdrawn. Data Protection Authorities are aggressively citing service providers who make consent easy to provide, but much more difficult to revoke. The CNIL, for example, fined both Facebook and Google for making opting-in very easy, but opting-out (that is, withdrawing consent) much more difficult. The CNIL wrote, "Users had to select multiple options to refuse cookies, but only one option to provide consent to the use of all cookies."

Technology Assistance

Where multiple consent models are being used, particularly when managing multiple websites, apps, and other collection points, consent becomes challenging to manage. There are numerous consent management platforms available to address consent choices prior to collecting, sharing, or selling user data.

Addressing compliance

By the end of 2024, Gartner estimates 75% of the world's population will have its personal data governed by a modern privacy regulation. That means three out of four visitors to a corporate website could have legal requirements governing their data.

To address compliance obligations, organizations must understand:

- Jurisdictions of website visitors
- Information that is collected from the visitors
- Applicable consent requirements across jurisdictions, considering the type of information that is collected about the individual and their actions on the site
- Ability to offer consent before tracking, customisation, and marketing
- Technical controls to manage consent and web tracking technologies

The first step in identifying website and cookie compliance obligations is typically to understand and document data flows and personal data processing. Then, scan and classify existing cookies, establish controls to manage cookie deployment and consent, and implement a cookie governance process to manage and maintain cookie compliance aligned with business strategy.

IMPACT OF BREXIT ON DATA PROTECTION

– A year in review

Moving into 2022

With the uncertainty surrounding Brexit and the impact it would have on United Kingdom (UK) data flows, the European Commission (subsequent to the Schrems II decision) had been working on a revised version of the European Union Standard Contractual Clauses (EU SCCs) to enable EU based organisations to safeguard transfers to any jurisdiction outside of the EU. This was approved in June 2021. However, due to the impact of Brexit, and the fact that the UK was no longer regarded as a part of the EU, the UK was not able to use the updated EU SCCs.

One of the direct impacts of Brexit was that the UK could no longer follow the EU GDPR and had to revert back to their own separate jurisdictional data protection regulation, The Data Protection Act 2018 (which was aptly given the name 'UK GDPR'). Subsequent to the realisation that the UK was unable to rely on the updated EU SCCs, the initial guidance was to continue using the old EU version of the SCCs for any UK organisation with exposure to an international data transfer.

Given the recent developments surrounding international data transfers because of the Schrems II judgement, and the fact that the old EU version of the SCCs were no longer considered fit for purpose, the UK had no option but to act accordingly, which resulted in the development of the UK Transfer Documents which were fully approved for use in March 2022.

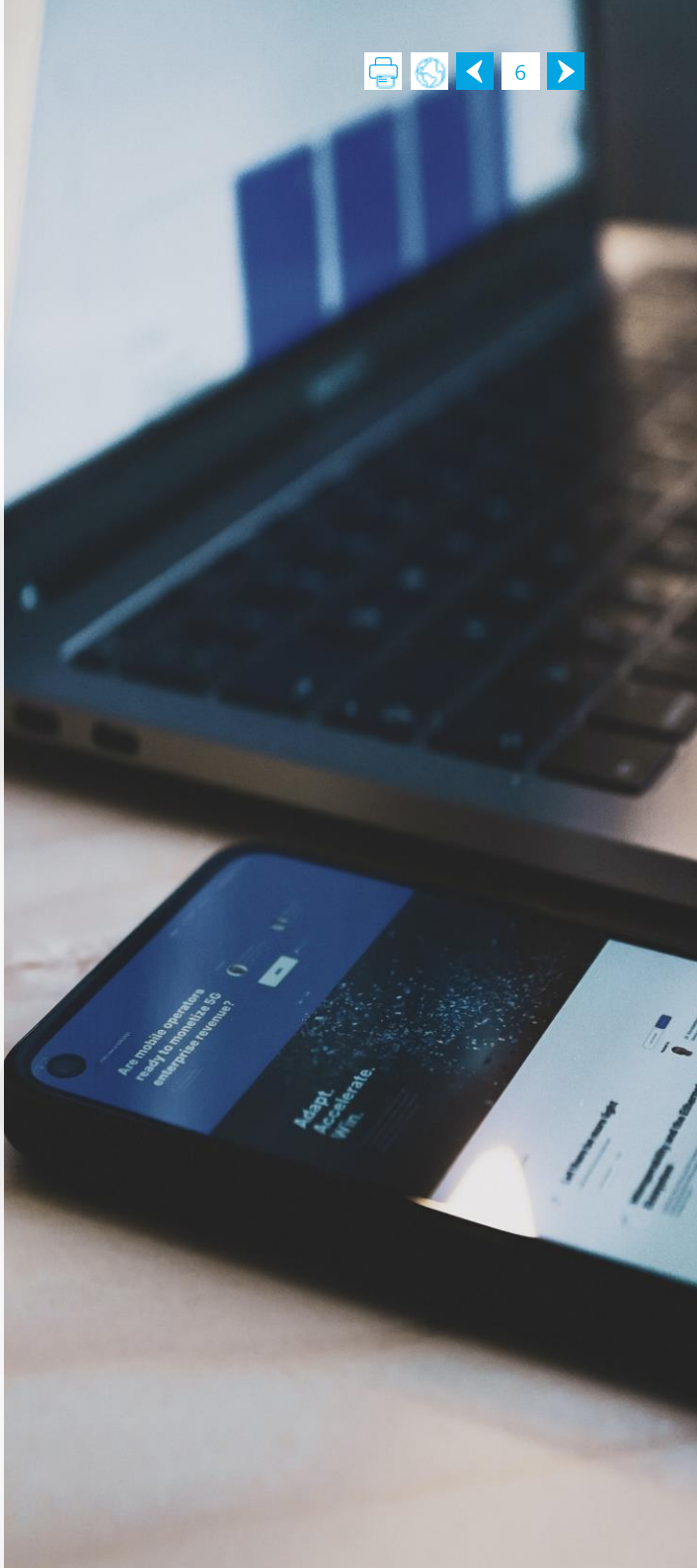
What are the UK Transfer Documents?

Following Brexit, and the newly drafted EU SCCs no longer being a viable option for UK organisations, several changes were laid before the UK parliament in February 2022:

- The new International Data Transfer Agreement (IDTA);
- The new International Data Transfer UK Addendum to the EU's new SCCs (UK Addendum); and
- The relevant transitional provisions.

As a result, for any UK-based organisation that has exposure to international data transfers and relies on contractual safeguards, either an IDTA or UK Addendum would need to be executed. For any legacy international data transfer exposures and corresponding contracts, UK-based organisations would need to make changes within the transitional provisions provided for in the guidance. These documents supersede all other contractual safeguards on which the UK was previously reliant (e.g., the old EU version of the SCCs).

The IDTA is recognised as a standalone agreement that compliments the main agreement in place between the sender and recipient of any information being transferred between the two parties. The IDTA can only be used when international data transfers are subject to UK Data Protection Laws.



IMPACT OF BREXIT ON DATA PROTECTION

– A year in review (continued)

The UK Addendum is used with the new EU SCCs and when a UK-based organisation is looking to transfer personal data where both UK and EU Data Protection Laws are applicable. The UK Addendum removes the need for a separate agreement for the UK data transfer element (i.e., an IDTA).

In line with the published transitional provisions, there are a number of key dates that UK-based organisations must consider:

- 21 March 2022: UK International Transfer documents (i.e., the IDTA and UK Addendum) are effective and can be used by UK based organisations.
- 22 September 2022: UK -based organisations are no longer able to rely on the old EU SCCs for international data transfers. From this date, UK organisations must use the new UK International Transfer documents for all new international data transfers.
- 21 March 2024: UK-based organisations are no longer able to rely on the use of the old EU SCCs for any pre-existing or legacy exposures to international data transfers. For any existing data transfer arrangements entered into prior to 22 September 2022 (that rely on the old EU SCCs as the appropriate safeguard), the organisation must have entered into a new contract on the basis of the new UK International Transfer documents, unless an additional safeguard can be relied upon outside of the contractual option.

The implementation of the IDTA and UK Addendum marks a significant milestone in the UK establishing compliance requirements for international data transfer. It should be noted that the requirement to execute a Transfer Risk Assessment (TRA) for the jurisdiction where information is being sent remains; this continues to be required for any organisation relying on the EU SCCs.

A LOOK AHEAD

Data Privacy continues to be a critical issue for organisations. Looking ahead, organisations must pay attention to regulatory developments, build sound privacy governance functions, and better leverage technology to manage and enhance privacy operations.

Regulatory Developments

2023 will be a busy year for new privacy laws and regulations. For example, in the U.S. alone, the California Privacy Rights Act, which supersedes the California Consumer Privacy Act, will go into effect at the beginning of the new year. The Virginia Consumer Protection Act and the Colorado Privacy Act will also go into effect. With these and other pending global regulations, organisations will need to align their privacy compliance programmes to address these laws. Looking toward the future, as more states and countries pass new privacy laws, and the U.S. Congress likely makes another attempt at Federal privacy legislation, organisations need to decide whether to a) adjust their privacy programmes to address new regulations one at a time, or b) develop a global standard for privacy compliance resulting in fewer changes as new laws get passed.

Once the European Commission ratifies the agreement and issues a formal adequacy decision, the Trans-Atlantic Data Privacy Framework (TADPF) will also go into effect. Under TADPF, organizations that agree to certify to privacy principles, will be able to transfer data between the U.S. and EU without having to implement contractual language such as standard contractual clauses or binding corporate rules. However, there is a chance that privacy activists may choose to challenge the TADPF in court, which may limit TADPF adoption due to its uncertain future, requiring existing data transfer mechanisms to remain in place.

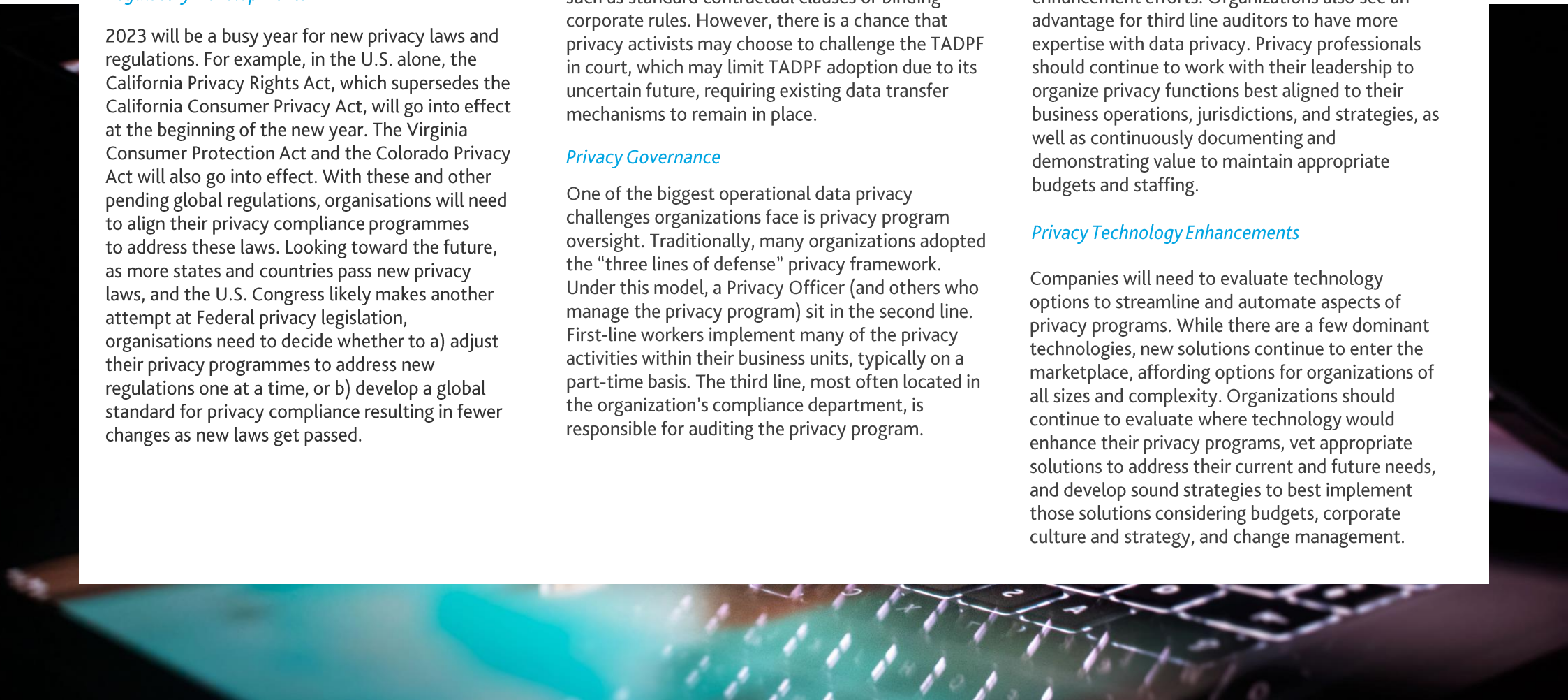
Privacy Governance

One of the biggest operational data privacy challenges organizations face is privacy program oversight. Traditionally, many organizations adopted the "three lines of defense" privacy framework. Under this model, a Privacy Officer (and others who manage the privacy program) sit in the second line. First-line workers implement many of the privacy activities within their business units, typically on a part-time basis. The third line, most often located in the organization's compliance department, is responsible for auditing the privacy program.

More recently, organizations are finding more operational success with enhanced full-time privacy expertise within their business units. More Chief Privacy Officers see themselves in hybrid roles, sitting in both the first and second lines, allowing them to manage their programs, but also closely oversee program implementation and enhancement efforts. Organizations also see an advantage for third line auditors to have more expertise with data privacy. Privacy professionals should continue to work with their leadership to organize privacy functions best aligned to their business operations, jurisdictions, and strategies, as well as continuously documenting and demonstrating value to maintain appropriate budgets and staffing.

Privacy Technology Enhancements

Companies will need to evaluate technology options to streamline and automate aspects of privacy programs. While there are a few dominant technologies, new solutions continue to enter the marketplace, affording options for organizations of all sizes and complexity. Organizations should continue to evaluate where technology would enhance their privacy programs, vet appropriate solutions to address their current and future needs, and develop sound strategies to best implement those solutions considering budgets, corporate culture and strategy, and change management.



BDO DATA PROTECTION ACADEMY

With the complexities of global data protection regulations, it is critically important to stay informed regarding the latest laws, processes, and guidance. Organisations that process data must be especially careful to ensure that the data they are processing follows the necessary data protection and privacy legislation. Failure to do so can result in allegations of fraud; negative press; and loss of revenue, productivity, and brand trust. Training is key to ensure that data protection and privacy components are understood and properly and handled by employees. Proper training drives a culture of awareness and compliance.

BDO's Data Protection Academy assists organisations in achieving these goals. As an authorised International Association of Privacy Professionals (IAPP) trainer, we offer courses delivered by highly credentialed instructors with real-world data privacy experience. The Data Protection Academy offers:

- IAPP certification courses
- Private, customised training based on an organisation's needs, global operating jurisdictions, and business strategies
- eLearning and Learning Management System (LMS) content development and delivery
- Complimentary webinars focused on recent data protection trends and topics
- Blockchain in Privacy courses

The Data Protection Academy's diverse training options will help organisations strengthen their privacy posture, providing privacy leaders, champions, and workers with key knowledge of privacy and data protection obligations. BDO's trainers are practitioners with experience as Data Protection Officers, CPOs, CISOs, CIOs, and have backgrounds in legal, technology, management, and business processes. We are versed in cultural and language nuances, as well as evolving regulatory changes. The Data Protection Academy currently offers the following IAPP courses:

- Certified Information Privacy Manager (CIPM)
- Certified Information Privacy Professional / US Private Sector (CIPP/US)
- Certified Information Privacy Professional / Europe (CIPP/E)
- Certified Information Privacy Technologists (CIPT)
- Foundations of Privacy and Data Protection

After attending the Academy, students are better prepared to influence and optimise their privacy programmes. Additionally, organisations have seen benefits from sponsoring the attendance of colleagues in privacy-adjacent roles.

For more information about upcoming courses, customised eLearning experiences and content development, contact:
The BDO Data Protection Academy

BDO DATA PROTECTION MANAGED SERVICES (DPMS)

With the growing number of global regulations, increased consumer privacy awareness, and the risks of data loss, it is more important than ever for organisations to enhance and maintain their data protection and privacy compliance programmes. While most organisations & recognise the importance of data privacy compliance, they struggle with limited staff, inadequate bandwidth, inability to scale, fragmented ownership of privacy tasks, and the reality of "just-in-time" privacy operations.

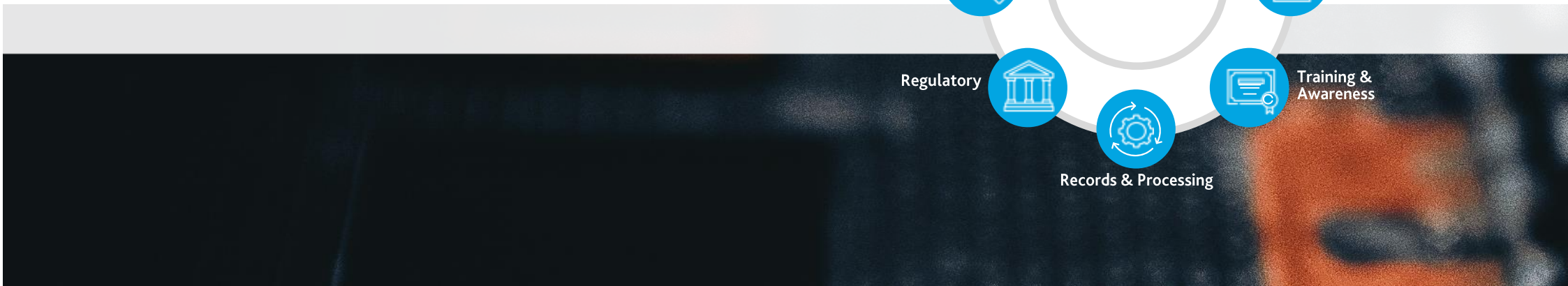
BDO's Data Protection Managed Services provide a holistic approach to data protection, drawing on local in-country intelligence and support across your global jurisdictions. Our expansive international team responds to meet each client's fluctuating needs, applies proven methodologies to various market-leading privacy platforms, and leverages experience with in-country regulators around the world. Our data protection team offers a one-stop, cost-effective solution for local and global data protection through managed services.

For more information about our Data Protection Managed Services, contact:
BDO DPMS

FROM MID-MARKET TO FORTUNE 50

A Fortune 50 company required a service that could offer the privacy expertise and scalability to fulfil their high volume of data subject requests. Since May 2018, BDO has fulfilled more than 1,000,000 of the company's data subject requests, managed responses to global regulators, and helped the client enable technology to automate their response processes.

With a lack of in-house privacy professionals, a client required assistance developing and managing their global privacy programme. Using BDO's Privacy Management Framework (PMF)®, and a global team of managed service professionals, BDO has successfully established the client's foundational privacy capabilities and continues to manage and enhance the programme through BDO's Data Protection Managed Services.

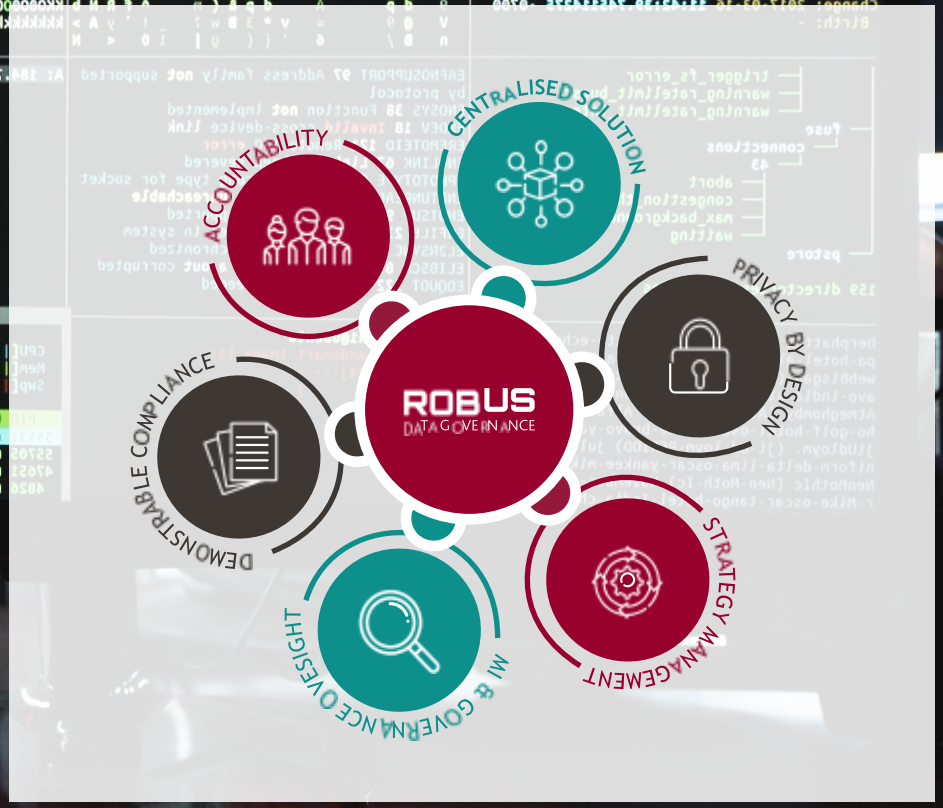


BDO ROBUS

ROBUS is a core platform used by BDO's Global Data Privacy team to manage privacy operations. ROBUS centralises an organisation's data protection programme, eliminating duplication of information and effort. ROBUS is built on the Microsoft Power Platform, seamlessly integrating with an organisation's existing technology stack.

ROBUS supports a comprehensive approach to data protection by formalising record keeping, Privacy-by-Design, Data Subject Requests, Privacy Impact Assessments, and breach response. It seamlessly links assets to activities, building relationship between data processing activities and records. The end-to-end product enables aggregated reporting of key privacy performance indicators that unify an enterprise view for privacy risk management.

Watch an introductory video for ROBUS here.
For more information about BDO ROBUS, visit www.bdo.je/robus.



RESOURCES: BDO GLOBAL DATA PROTECTION GUIDE & PRIVACYWATCH®

Staying updated and receiving timely and relevant information is time-consuming and resource intensive. BDO provides two resources to assist with that:

- BDO Global Data Protection Guide
- BDO PrivacyWatch

BDO's online Global Data Protection Guide is a no cost resource backed by a team of global privacy and data protection professionals who provide current, country-specific information to keep you informed regarding the privacy regulatory landscape.

PrivacyWatch is a weekly email digest that offers case law updates and data protection, security, and privacy industry trends. Each update includes important privacy and data protection highlights from worldwide jurisdictions.

Customised PrivacyWatch updates are available and tailored to your organisation's industry, applicable jurisdictions, and data processing activities.

Click here to request a snapshot of BDO's PrivacyWatch,

Click here to request a link to the most recent version of the BDO Global Data Protection Guide.

COUNTRY UPDATES

This year's BDO Global Data Privacy Whitepaper surveyed in-country BDO professionals to learn more about the changes within their jurisdictions. The table in the next section summarises the following information and the subsequent pages detail recent updates that will impact 2023 and beyond.

- Data Protection / Privacy Law
- Data Protection Regulator
- EU Adequacy Decision
- Other Related Laws

As noted in the regulatory updates on the following pages, legislators continue to modernise privacy and data protection legislation to remain current with technical trends, including cookie compliance and website consent mechanisms. Additionally, regulators are negotiating and instituting new data transfer mechanisms and guidance, as more countries enact or refine their data protection legislation.

With regulators continuing to impose hefty fines and penalties for a variety of privacy and data protection shortcomings, organisations should continue to assess and monitor their global privacy risk according to updated privacy legislation and revised guidance. They should seek to optimise their privacy programme structure and governance, aligned with growth and business strategy. Organisations should also look for ways to introduce or expand the use of technology to streamline and automate parts of their privacy compliance operations.

PRIVACY AND DATA PROTECTION SUMMARY BY COUNTRY (1/7)

Country	Data Protection/Privacy Law	Data Protection Regulator	EU Adequacy Decision	Other Related Laws	BDO Contact Member
Argentina	Personal Data Protection Act, Act NO. 25.326 of 200	National Directorate for Personal Data Protection	Yes	Argentenian Constitution & Regulatory Decree 1558/2001	Fabian Descalzo fdescalzo@bdoargentina.com +54 11 4106 7000
Australia	Privacy Act 1988 (No.119, 1988)(as amended) ('The Privacy Act')	The Office of the Australian Informaton Commissioner ("OAIC)	No	Treasury Laws Amendment (Consumer Data Right) Bill 2019	Leon Fouche +61 7 3237 5688 leon.fouche@bdo.com.au
Austria	GDPR	Austrian Data Protection Authority	N/A	Austrian Data Protection Act/Datenschutzgestez	Ewald Kager ewald.kager@bdo.at +43 1 53737
Belgium	GDPR	Belgian Data Protection Authorty	N/A	Act of 3 December 2017 Establishing the Data Protection Authority, Act of 30 July 2018 on the Protection of Natural Persons with Regard to the Processing of Personal Data	Alain Vanmeerhaeghe alain.vanmeerhaeghe@bdo.be +32497644213
Brazil	Law No. 13709 of 14 August 2018, General Personal Data Protection Law (as amended by Law No. 13.853 of 8 July 2015) ("LGPD")	Brazilian Data Protection Authority ('ANPD)	No		Toni Hebert toni.hebert@bdo.com.br +55 11 3848.5880
Bulgaria	GDPR	Commissioner for Personal Data Protection (CPDP)	N/A	The Protection of Personal Data Act 2002 (Amended 2019), Rules on the Activity of the Commission of Personal Data Protection and its Administration	Silvana Dzharkova-Aleksandrova s.dzharkova@murgova.com +35929898298
Canada	The Personal Information Protection and Electronic Documents Act (PIPEDA)	Office of the Privacy Commissioner of Canada (OPC)	Yes (Commercial Organisations)	Privacy Act 1985 ('The Privacy Act'), Bank Act of 1991, Canada's Anti-Spam Legislation, Proceeds of Crime (Money Laundering) and Terrorist Financing Act of 2000	Ziad Akkaoui Zakkaoui@bdo.ca 416.369.6048
Cayman Islands	Data Protection Regulations, 2018 (SL 17 of 2019), The Data Protection Act (2021 Revision)	Office of theOmbudsman (the Ombudsman)	No		Richard Carty rcarty@bdo.ky +13459281120

PRIVACY AND DATA PROTECTION SUMMARY BY COUNTRY (2/7)

Country	Data Protection/Privacy Law	Data Protection Regulator	EU Adequacy Decision	Other Related Laws	BDO Contact Member
China	Personal Information Protection Law (PIPL)	The Cyberspace Adminstration of China (CAC)	No	Cybersecurity Law 2016	Min Cai min.cai@bdo.com.cn 法证与网络安全咨询服务部 全国主管合伙人 Tel: +086 21 2328-2844
Colombia	Statutory Law1581 of 2012 (October 17)	Colombia Data Protection Authority (SIC)	No		Paula Giraldo Gutierrez pgiraldo@bdo.com.co +573173311331
Costa Rica	Law on the Protection of Persons Regarding the Processing of their Personal Data No. 8968 of 2011	Agencia de Protección de Datos de los Habitantes (Agency for the Protection of Inhabitants' Data) (PRODHAB)	No	Executive Decree No. 37554-JP of 30 October 2012 Regulating Law No. 8968	Carlos González cgonzalez@bdo.cr +506 22317060
Czech Republic	GDPR	Office for Personal Data Protection (UOOU)	N/A	Act No. 110/2019 Coll. on Personal Data Processing , Article 89(3) of the Act No. 127/2005 Coll. Of 22 February 2005 on Electronic Communications and on Amendment to Certain Related Acts	Stanislav Klika stanislav.klika@bdo.cz +420 604226734
Denmark	GDPR	Danish Data Protection Authority (Datatilsynet)	N/A	Act No. 502 of 23 May 2018 on Supplementary Provisions to the Regulation on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data	Mikkel Jon Larssen mla@bdo.dk +45 30 70 43 34
Finland	GDPR	Office of the Data Protection Ombudsman	N/A	The Data Protection Act (1050/2018)	Ossi Määttä ossi.maatta@bdo.fi +358503511453
France	GDPR	French Data Protection Authority (Commission Nationale de l'Informatique et des Libertés, "CNIL")	N/A	Federal Data Protection Act of 30 June 2017	Bruno Saucourt bruno.saucourt@bdo.fr +33686282959

PRIVACY AND DATA PROTECTION SUMMARY BY COUNTRY (3/7)

Country	Data Protection/Privacy Law	Data Protection Regulator	EU Adequacy Decision	Other Related Laws	BDO Contact Member
Georgia	Law of Georgia on Personal Data Protection of 28 December 2011 No. 5669 ('the Data Protection Act')	Office of the Personal Data Protection Inspector ('PDP')	No		Anzor Mekhrishvili amekhrishvili@bdo.ge +995598212007
Germany	GDPR	The Federal Commissioner for Data Protection and Freedom of Information (Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, "BfDI")	N/A	Federal Data Protection Act of 30 June 2017	Hans-Peter Toft Hans-peter.toft@bdolegal.de +49 40 30293-945
Guernsey	The Data Protection (Bailiwick of Guernsey) Law, 2017	The Office of the Data Protection Authority	Yes	The Data Protection (Commencement, Amendment and Transitional) (Bailiwick of Guernsey) Ordinance, 2018	Richard Searle +44 (0)1481 724561 Richard.Searle@bdo.gg
Hong Kong	Personal Data (Privacy) Ordinance (Cap. 486) as amended in 2012 ('PDPO') The Office of the Privacy Commissioner	The Office of the Privacy Commissioner for Personal Data ('PCPD')	No		Ricky Cheng Rickycheng@bdo.com.hk +852 2218 8266
India	Introduced the Personal Data Protection Bill	Once passed, the Data Protection Authority of India to be established	No	Information Technology Act, 2000, amended to address specific data protection concerns	Saumil G Shah saumilgshah@bdo.in +919900079563
Ireland	GDPR	Data Protection Commission ('DPC')	N/A	Data Protection Act 2018	David McCormick DMcCormick@bdo.ie or DPO@BDO.ie +353 1 4700000
Israel	Protection of Privacy Law, 5741-1981	Privacy Protection Authority ('PPA')	Yes	Protection of Privacy Regulations (Data Security) 5777-2017	Gali Sela galis@bdo.co.il
Italy	Personal Data Protection Code, Containing Provisions to Adapt the National Legislation to General Data Protection Regulation (Regulation (EU) 2016/679)	Italian data protection authority (Garante per la protezione dei dati personali, "Garante")	N/A		Stefano Minini stefano.minini@bdo.it +393346829871

PRIVACY AND DATA PROTECTION SUMMARY BY COUNTRY (4/7)

Country	Data Protection/Privacy Law	Data Protection Regulator	EU Adequacy Decision	Other Related Laws	BDO Contact Member
Japan	The Act on the Protection of Personal Information (Act No. 57 of 2003 as amended in 2015) ('APPI')	The Personal Information Protection Commission ('PPC')	Yes	Act on the Use of Numbers to Identify a Specific Individual in the Administrative Procedure ('My Number Act')	Gary Loh garyloh@bdo.com.sg
Jersey	Data Protection (Jersey) Law, 2018	Jersey Office of the Information Commissioner ('JOIC')	Yes	Data Protection Authority (Jersey) Law 2018	Damon Greber dgreber@bdo.je +44 (0) 1534 844 451
Latvia	GDPR	Data State Inspectorate ('DVI')	N/A	Personal Data Processing Law of 21 June 2018	Lasma Kramina lasma.kramina@bdo.lv +371 6722 2237
Malta	GDPR	Office of the Information and Data Protection Commissioner ('IDPC')	N/A	The Data Protection Act (Act XX 2018) ('the Act')	Ivan Spiteri ivan.spiteri@bdo.com.mt +356 23434201
Mauritius	Data Protection Act 2018 (the Data Protection Act)	Data Protection Office ('the Office')	No		Deepshi Hujoory deepshi.hujoory@bdo.mu +230 202 9562
Mexico	Federal Law on Protection of Personal Data Held by Private Parties ('FLPPDPP')	National Institute for Access to Information and Protection of Personal Data ('INAI')	No	Regulations to the Federal Law on Protection of Personal Data Held by Private Parties	Ramses Inzunza ramses.inzunza@bdomexico.com +52 (55) 8503-4200
Netherlands	GDPR	Dutch Data Protection Authority ("AP")	N/A	Act Implementing the GDPR	Robert Van Vianen robert.van.vianen@bdo.nl +31 30 284 98 00
Nigeria	Nigeria Data Protection Regulation 2019 ('NDPR')	National Information Technology Development Agency ('NITDA')	No	Freedom of Information Act (2011), National Health Act (2014), Cybercrimes (Prohibition, Prevention, etc.) Act (2015)	Ebenezer Olabisi eoolabisi@bdo-ng.com +234 1 448 3051
Norway	GDPR	Data Protection Authority ('Datatilsynet')	N/A	Law on the Processing of Personal Data (Personal Data Act) of 15 June 2018	Henrik Dagestad henrik.dagestad@bdo.no +47 901 77 117

PRIVACY AND DATA PROTECTION SUMMARY BY COUNTRY (5/7)

Country	Data Protection/Privacy Law	Data Protection Regulator	EU Adequacy Decision	Other Related Laws	BDO Contact Member
Panama	Law No. 81 on Personal Data Protection 2019	National Authority for Transparency and Access to Information ('ANTAI')	No		Simone Mitil smitil@bdo.com.pa +507 6070 7907
Phillipines	The Data Privacy Act of 2012 (Republic Act No. 10173) ('the Act')	The National Privacy Commission ('NPC')	No	An Act Providing for an Opt-In Mechanism for Telephone and Mobile Subscribers, protecting such Subscribers from Electronic Threats through the Misuse of Digital Technology, and Providing Penalties for Violations Thereof' ('SB 2460')	Ricky Cheng Rickycheng@bdo.com.hk +852 2218 8266
Poland	GDPR	Polish Data Protection Authority ("UODO")	N/A	Act of 10 May 2018 on the Protection of Personal Data	Tymoteusz Murzyn tymoteusz.murzyn@bdolegal.pl
Portugal	GDPR	Portuguese Data Protection Authority ("CNPD")	N/A	Law No. 58/2019, which Ensures the Implementation in the National Legal Order of the GDPR	Luís Crispim luis.crispim@bdo.pt +351937990341
Romania	GDPR	National Supervisory Authority for Personal Data Processing ('ANSPDCP')	N/A	Law No. 190/2018 Implementing the GDPR	Raluca Andrei raluca.andrei@tudor-andrei.ro +40755633856
Singapore	Personal Data Protection Act 2012 (No. 26 of 2012) ('PDPA')	Personal Data Protection Commission ('PDPC')	No	Cybersecurity Act 2018 (No. 9 of 2018)	Gary Loh garyloh@bdo.com.sg
Slovakia	GDPR	Office for Personal Data Protection of the Slovak Republic ('ÚOOÚ')	N/A	The Act No. 18/2018 Coll. on Protection of Personal Data and on Amendments to certain Acts	Marek Priesol priesol@bdoslovakia.com
South Africa	Protection of Personal Information Act, 2013 (Act 4 of 2013) ('POPIA')	The Information Regulator	No	Regulations Relating to the Protection of Personal Information (2018)	Carl Bosma cbosma@bdo.co.za

PRIVACY AND DATA PROTECTION SUMMARY BY COUNTRY (5/7)

Country	Data Protection/Privacy Law	Data Protection Regulator	EU Adequacy Decision	Other Related Laws	BDO Contact Member
South Korea	Personal Information Protection Act (PIPA) 2011	Personal Information Protection Commission ('PIPC')	Yes	The Use and Protection of Credit Information Act 2009 The Act on Promotion of Information and Communications Network Utilization and Information Protection 2001.	Mark Antalik mantalik@bdo.com +1 617-378-3653 Taryn Crane tcrane@bdo.com +1 301-354-2583
Spain	GDPR	Spanish Data Protection Authority ("AEPD")	N/A	Organic Law 3/2018, of 5 December 2018, on the Protection of Personal Data and Guarantee of Digital Rights	Albert Castellenos albert.castellanos@bdo.es
Sweden	GDPR	The Swedish Authority for Privacy Protection ('IMY')	N/A	The Swedish Data Act (1973 Revised), Swedish Personal Data Act, 1998, The Act with Supplementary Provisions to the GDPR (SFS 2018:218)	Hakan Skyllberg hakan.skyllberg@bdo.se +46 70 167 16 57
Switzerland	Federal Act on Data Protection 1992 ('FADP'); revised 2020	Federal Data Protection and Information Commissioner ('FDPIC')	Yes	Schweizer Datenschutzgesetz – Swiss Data Protection Act	Klaus Krohmann klaus.krohmann@bdo.ch +41 44 444 36 25
United Arab Emirates	Federal Decree-Law No. 45 of 2021 regarding the Protection of Personal Data ('the Law')	DIFC and Abu Dhabi Global Market (ADGM), UAE Data Office	No	DIFC data Privacy law ADGM Data Protection, Department of Health (DOH) Abu Dhabi's Abu Dhabi Healthcare Information and Cyber Security Standards (ADHICS)	Shivendra Jha shivendra.jha@bdo.ae +971 4 518 6666
United Kingdom	UK General Data Protection Regulation (Regulation (EU) 2016/679)	EU) 2016/679) The Information Commissioner's Office ("ICO")	Yes	Data Protection Act 2018	Christopher Beveridge christopher.beveridge@bdo.co.uk +44 795 699 1215

PRIVACY AND DATA PROTECTION SUMMARY BY COUNTRY (7/7)

Country	Data Protection/Privacy Law	Data Protection Regulator	EU Adequacy Decision	Other Related Laws	BDO Contact Member
United States	No Federal Law	Federal Trade Commission	No	FTC Act – Section 5, Gramm-Leach Bliley Act of 1999, Health Insurance Portability & Accountability Act of 1996, Children's Online Privacy Protection Act of 1998, Electronic Communications Privacy Act of 1986 Health Information Technology for Economic and Clinical Health Act of 2009 ('HITECH') Telemarketing and Consumer Fraud and Abuse Prevention Act of 1994 ('TCFAPA') Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 ('CAN-SPAM') Fair Credit Reporting Act of 1970 ('FCRA') Telephone Consumer Protection Act of 1991 ('TCPA') Privacy Act of 1974 Fair and Accurate Credit Transactions Act of 2003 ('FACTA') Video Privacy Protection Act of 1988 ('VPPA')	Mark Antalik mantalik@bdo.com +1 617-378-3653 Taryn Crane tcrane@bdo.com +1 301-354-2583

DETAILED COUNTRY UPDATES

ARGENTINA

Law: Personal Data Protection Act, Act No. 25.326 of 2000, Argentinian Constitution and Regulatory Decree 1558/2001

Regulator: National Directorate for Personal Data Protection

EU Adequacy Decision: yes

Fabian Descalzo
fdescalzo@bdoargentina.com
+54 11 4106 7000

The primary law in Argentina is Personal Data Protection Act, Act No. 25.326 of 2000. However, the Argentinian Constitution and Regulatory Decree 1558/2001 (DP Decree) and provisions issued by the National Directorate for Personal Data Protection (NDPDP) are also part of Argentina's data privacy landscape.

Notable Changes

In August 2022, the head of Argentina's Data Protection Authority presented the main guidelines for updating Law 25,326 on the protection of Personal Data and has published a draft bill that proposes to bring Argentina's 22-year-old data protection law more in line with the European Union's General Data Protection Regulation.

The bill modernises Argentina's data protection law to deal with more recent issues, including cloud computing, biometric, and genetic data. It provides greater scope for international transfers of information by allowing transfers under the sanction of adequate data protection guarantees in the absence of a decision by the Agency that the importing country has adequate data protection. The draft bill is now open for public comments.

Data Protection Authority Focus

President Alberto Fernández appointed Beatriz de Anchorena as the new director for the Argentinian data protection authority ('AAIP') on 10 March 2022. Of particular note, Anchorena was appointed after a transparent and open public hearing process and after she presented her work plan for the AAIP. [1]

The AAIP aims to fill in legislative gaps in the current Data Protection Act through disposition and resolutions. The Agency does not regularly take on enforcement actions. However, it periodically practices audits and imposes sanctions. Most of these sanctions are for failure to register or renew a Database registration. Others pertain to unauthorised data processing, not providing rectification, suppression of the personal data of the data subject, not providing notice of the purpose of data collection, and not following data protection rules.

[1] https://www.dataguidance.com/news/argentina-president-appoints-new-director-data

AUSTRALIA

Law: Privacy Act No. 119 1988 (as amended) ('the Privacy Act')

Regulator: The Office of the Australian Information Commissioner ("OAIC")

EU Adequacy Decision: no

Leon Fouche
leon.fouche@bdo.com.au
+61 7 3237 5688

Notable Changes

The Notifiable Data Breaches scheme commenced as part of the Privacy Act on 22 February 2018. The scheme requires notification to affected individuals and the OAIC when an entity subject to the Privacy Act experiences a data breach of personal information that poses a likely risk of serious harm to affected individuals.

The Minister for Trade and Tourism announced on 17 August 2022, in a joint press release with the Attorney General, that Australia joined the Global Cross-Border Privacy Rules CBPR Forum, the multilateral initiative which aims to better facilitate the flow of data across borders. The Global CBPR Forum builds on the APEC CBPR formed in 2011 and is open to participation by non-APEC members.

Data Protection Authority Focus

The Australian Attorney General is behind "urgent reforms" to the Privacy Act following an unprecedented breach involving Optus, Australia's second-largest wireless carrier. Australia expects enhanced data protection laws in place this year in response to the cyberattack where personal data of 9.8 million customers was compromised.

On 6 October 2022 the Australian Minister for Communications announced that, following extensive consultation with the financial services sector, telecommunications providers, the privacy commissioner, and others, a set of telecommunications amendments are going to be introduced to the Telecommunications Regulations 2021 that will:

- Enable telecommunications providers to better coordinate with financial institutions to detect and mitigate the risks of malicious activity, including ID theft and scams; and
- Allow organizations to share limited information about customers with government agencies, such as Services Australia, to assist in preventing fraud[1].

[1] https://www.dataguidance.com/news/australia-government-announces-changes-telecoms

AUSTRIA

Law: Austrian Data Protection Act / Datenschutzgesetz

Regulator: Österreichische Datenschutzbehörde / Austrian Data Protection Authority

EU Adequacy Decision: n/a

Ewald Kager
ewald.kager@bdo.at
+43 1 53737

Notable Changes

On 12 May 2022, the Council of Europe (CoE) announced that 22 Council of Europe Member States had signed the Second Additional Protocol to the Convention on Cybercrime on Enhanced Cooperation and Disclosure of Electronic Evidence (Second Additional Protocol to the Budapest Convention). In particular, the CoE outlined that the Second Additional Protocol aims to bring the Budapest Convention up to date with current technological challenges so that it remains the most relevant and effective international framework for combating cybercrime. More specifically, the CoE highlighted that the protocol responds to the need for greater and more efficient cooperation between States themselves and also between States and the private sector.

The Second Additional Protocol to the Budapest Convention has been signed by the following CoE Member States: Austria, Belgium, Bulgaria, Estonia, Finland, Iceland, Italy, Lithuania, Luxembourg, Montenegro, Netherlands, North Macedonia, Portugal, Romania, Serbia, Spain, and Sweden. In addition, the Second Additional Protocol was signed by the following non-CoE Member States: Chile, Colombia, Japan, Morocco, and the United States.[1]

On 29 September 2022, the European Commission announced that it had taken further steps in its infringement procedure against Austria, Belgium, Romania, and Slovenia, following its previous infringement action in July 2022. In particular, the Commission noted that the four member states had failed to fully transpose the Directive on the Protection of Persons who Report Breaches of Union Law (Directive (EU) 2019/1937) (the Whistleblowing Directive) before 17 December 2021. As such, the commission concluded that it had issued reasoned opinions, to which the four member states have two months to reply. Additionally, if the replies are not satisfactory, the commission indicated that it may refer the concerned member states to the Court of Justice of the European Union.[2]

Data Protection Authority Focus

On 25 May 2022, the Austrian data protection authority (DSB) published FAQs on cookies and data protection, aiming to clarify the legal framework around the use of cookies under EU and Austrian law. In particular, the FAQs outline that the use of cookies is generally subject to prior user consent unless cookies are strictly necessary, as stipulated by Article 5(3) of the Directive on Privacy and Electronic Communications (2002/58/EC) (as amended) (the ePrivacy Directive) and Section 165(3) of the Telecommunications Act 2021 (TKG), the conditions of which are regulated by the consent provisions of the General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR).[3]

1 https://www.dataguidance.com/news/eu-commission-issues-reasoned-opinions-against-four
2 https://www.dataguidance.com/news/international-22-states-sign-new-additional-protocol
3 https://www.dataguidance.com/news/austria-dsb-publishes-faqs-cookies-outlines-conditions

BELGIUM

Law: Act of 3 December 2017 Establishing the Data Protection Authority, Act of 30 July 2018 on the Protection of Natural Persons with Regard to the Processing of Personal Data ('the Act') and the GDPR

Regulator: Autorité de la protection des données - Gegevensbeschermingsautoriteit (APD-GBA) / Data Protection Authority ('Belgian DPA')

EU Adequacy Decision: n/a

Alain Vanmeerhaeghe
alain.vanmeerhaeghe@bdo.be
+32497644213

Notable Changes

The number of incoming complaints has skyrocketed in 2021, with 1928 complaints (up from 685 in 2020): a growth of 181.46% compared to 2020. 1120 of these relate to a data leak from the social network Facebook, and thus contribute to this unprecedented amount of incoming complaints. The DPA also received 142 mediation requests (+67.06% compared to 2020) and processed 4207 requests for information (+2.43%).

The DPA opened 1435 data leakage cases (it received 1432 data leakage notifications, and opened 3 initiative cases), compared to 1054 in 2020 (+36.15%). It also initiated 35 monitoring cases, compared to 30 in 2020 (+16.67%). Finally, DPA received 279 requests for advice (+87.25% compared to 2020), the highest number since DPA was created.

In terms of enforcement: the Inspection Service launched 142 investigations in 2021, compared to 152 in 2020 (-6.58%) . The DPA's Litigation Chamber issued 143 decisions in 2021, compared with 83 in 2020 (+72.29%). In total, the amount of fines imposed through these different decisions is 301,000 euros.

In February 2022, the Council of Ministers approved a draft law on the protection of persons notifying of violations of the law of the European Union or Belgian law within a public body: "the Whistleblowing Directive."

The draft law requires legal entities within the private sector with over 50 employees to implement reporting procedures and channels to ensure that employees may report violations. The draft bill law has been transmitted to the Council of State for its opinion.[1]
On 12 May 2022, The Council of Europe (CoE) announced that 22 Council of Europe Member States had signed the Second Additional Protocol to the Convention on Cybercrime on Enhanced Cooperation and Disclosure of Electronic Evidence (Second Additional Protocol to the Budapest Convention).[2]

Data Protection Authority Focus

On 4 April 2022, the Belgian DPA published its decision[3] in which it imposed administrative fines of €200,000 and €20,000 on Brussels Airport and Ambuce Rescue team, respectively, for the carrying out of temperature checks on passengers and for the processing of special categories of personal data (health data).

1 https://www.dataguidance.com/news/belgium-council-ministers-approves-draft-whistleblowing
2 https://www.dataguidance.com/news/belgium-council-ministers-approves-draft-whistleblowing
3 https://www.dataguidance.com/news/international-22-states-sign-new-additional-protocol

BELGIUM (CONTINUED)

Law: Act of 3 December 2017 Establishing the Data Protection Authority, Act of 30 July 2018 on the Protection of Natural Persons with Regard to the Processing of Personal Data ('the Act') and the GDPR

Regulator: Autorité de la protection des données - Gegevensbeschermingsautoriteit (APD-GBA) / Data Protection Authority ('Belgian DPA')

EU Adequacy Decision: n/a

Alain Vanmeerhaeghe
alain.vanmeerhaeghe@bdo.be
+32497644213

The Litigation Chamber states that, when taking this decision, it considered the difficult context of the COVID-19 crisis.[4] The Belgian DPA also fined Brussels South Charleroi Airport (BSCA) €100,000 for similar usage of thermal cameras.

In February 2022, IAB Europe, an advertising business trade organisation, was fined €250,000. The Data Protection Authority found that IAB Europe's Transparency & Consent Framework (TCF), which facilitates the capture of users' preferences to share them with advertisers, did not comply with certain *GDPR* provisions. Contrary to its allegations, IAB Europe was found to act as a *controller* with respect to the registration of users' consent and their preferences by means of a unique TCF string (linked to an identifiable user) and could therefore be held responsible for *GDPR* infringements.[5]

Additionally, the Roularta publishing company was fined €50,000 by the Belgian Data Protection Authority for how it handled cookies on two websites. According to the ADP, the business did not comply with the requirements of the EU General Data Protection Regulation for obtaining user consent for cookie placement. Hielke Hijmans, head of the DPA Litigation Chamber, stated that because cookies are so common on the internet, it is crucial for the security of user data that they are set by site editors in a clear and legal manner.

4 https://edpb.europa.eu/news/national-news/2022/temperature-checks-brussels-airport-belgium-part-fight-against-covid-19_en
5 https://www.linklaters.com/en/insights/data-protected/data-protected---belgium

BRAZIL

Lei n. 13.709/2018

Law: Lei Geral de Proteção de Dados Pessoais (LGPD)

Data Protection Authority: Autoridade Nacional de Proteção de Dados (ANPD)

EU Adequacy Decision: no

Toni Hebert
toni.hebert@bdo.com.br
+55 11 3848.5880

Notable Changes

On January 2021, the ANPD published the Technical Note no. 1/2021/CGN/ANPD, related and Report about the regulatory impacts for the application of LGPD in microbusiness and, additionally, it determined orientations such as: the need of a risk assessment in the information security area, an data protection awareness environment , training, contract management, access controlled (MFA/cryptography) and personal data security.

On 10 February 2022, the President of the National Congress, Senator Rodrigo Pacheco, promulgated EC 115, thereby creating Article 5 (LXXIX) in the Brazilian Constitution. The article includes the protection of personal data as a fundamental right as well as guaranteeing and granting the Union exclusive competence to legislate, organise, and supervise the protection and processing of personal data.[1]

On 28 January 2022, the ANPD launched International Data Protection Day, the Guidance on the Processing of Personal Data by the Public Power.

The purpose of the Guide is to assist in the challenge of establishing objective parameters capable of providing legal certainty to transactions with personal data carried out by public bodies and entities.[2]

On 11 October 2022 the Chamber of Deputies announced that it had approved a provisional measure that transforms the ANPD into an agency of a special nature, granting administrative autonomy to the body.[3]

On 23 August 2022, the Ministry of Justice and Public Security (MJSP) announced that its National Consumer Secretariat (Senacon) had issued a decision in which it imposed a fine of BRL 6.6 million (approx. €1,290,000) to Facebook, Inc. following the unlawful sharing of personal data of Brazilians. The MJSP stated that Senacon did not accept Facebook's position and imposed the fine.[4]

1 https://www.dataguidance.com/news/brazil-congress-issues-statement-enactment-amendment
2 https://www.gov.br/anpd/pt-br/assuntos/noticias/no-dia-internacional-da-protecao-de-dados-anpd-publica-guia-orientativo-sobre-tratamento-de-dados-pessoais-pelo-poder-publico
3 https://www.dataguidance.com/news/brazil-chamber-deputies-approves-provisional-measures
4 https://www.dataguidance.com/news/brazil-senacon-fines-facebook-brl-66m-cambridge

BRAZIL (CONTINUED)

Lei n. 13.709/2018

Law: Lei Geral de Proteção de Dados Pessoais (LGPD)

Data Protection Authority: Autoridade Nacional de Proteção de Dados (ANPD)
Adequacy Agreement with Adequacy

EU Adequacy Decision: no

Toni Hebert
toni.hebert@bdo.com.br
+55 11 3848.5880

New Data Privacy Legislation

On 14 March 2022, the Brazilian Centre for Prevention, Treatment, and Response to Government Cyber Incidents (CTIR) issued Alert No. 08/2022 on Virtual Private Networks (VPNs).[5]

On 22 March 2022, the Chamber of Deputies of the National Congress announced Bill No. 310/2022 to prohibit telemarketing companies from contacting users without prior consent.[6]

On 27 April 2022, the ANPD published the Version 2.0 of its Guidance for Personal Data Processing Agents and Data Protection Officers (DPO), which was initially published on 28 May 2021.[7]

On 4 January 2022, the Federal Senate of Brazil announced the enactment of Law No. 14.289 of 3 January 2022 on the confidentiality of persons with HIV, chronic hepatitis, leprosy, and tuberculosis.[8]

On 19 April 2022, the Ministry of Economy authorised the Federal Service for Data Processing (SERPRO) to provide third parties with access to data subject's personal data, under the management of the Special Secretariat of the Federal Revenue Service of Brazil (RFB).[9]

5 https://www.dataguidance.com/news/brazil-ctir-recommends-measures-vpn-use
6 https://www.dataguidance.com/news/brazil-bill-prohibiting-telemarketing-without-prior
7 https://www.dataguidance.com/news/brazil-anpd-publishes-updated-guidance-data-controllers
8 https://www.dataguidance.com/news/brazil-senate-approves-law-requiring-confidentiality
9 https://www.dataguidance.com/news/brazil-ministry-economy-publishes-ordinance-sharing

BULGARIA

Law: Personal Data Protection Act, National Personal Data Protection Act

Regulator: омисия за защита на личните данни / Personal Data Protection Commission (the 'Commission')

EU Adequacy Decision: n/a

Silvana Dzharkova-Aleksandrova
s.dzharkova@murgova.com
+35929898298

Notable Changes

On 25 March 2022, the CPDP published its annual report for 2021. The report contains sections on the CDPD's protection of data subjects' rights, control activity and international activity. In addition, the report notes that it had received 487 complaints related to violations of the General Data Protection Regulation (GDPR) in 2021. Furthermore, the report highlights that there were a total of 64 violations of the GDPR that had resulted in administrative action. Lastly, the report noted that the CPDP imposed fines amounting to BGN 319,000 (approx. €162,542) in 2021.[1]

Data Protection Authority Focus

The focus of the Bulgarian DP Authority, namely the CPDP, is mainly guidance and decisions regarding complaints.

On 10 June 2022, the CPDP announced that it had adopted, on 1 June 2022, a list of personal data processing operations for which prior consultation is mandatory under Article 65(3) of the Protection of Personal Data Act 2002 (the Act) (last amended in 2019).

The controllers and processors under Chapter Eight of the Act should consult the CPDP before starting to process personal data that will form part of a new personal data register in all cases where a particular type of processing is likely to result in a high risk to the rights and freedoms of data subjects, including in the cases referred to in Article 65(1) of the Act.[2]

1 https://www.dataguidance.com/news/bulgaria-cpdp-publishes-2021-annual-report
2 https://www.dataguidance.com/news/bulgaria-cpdp-publishes-list-personal-data-processing

CANADA

Law: The Personal Information Protection and Electronic Documents Act (PIPEDA), The Privacy Act

Regulator: Office of the Privacy Commissioner of Canada, Office of the Information and Privacy Commissioner of Alberta, Office of the Information and Privacy Commissioner for British Columbia, Commission d'accès à l'information du Québec

EU Adequacy Decision: yes (Commercial Organisations)

Ziad Akkaoui
Zakkaoui@bdo.ca
+1 (416) 369-6048

Notable Changes

On 3 March 2022, the OPC published its 2022-2023 Departmental Plan. The Departmental Plan provides information on how the OPC will:

- Contribute to the adoption of laws that improve privacy protection
- Prepare the OPC for the implementation of new responsibilities
- Continue to focus on its Departmental Results Framework (DRF) goals
- Invest in and support its employees.[1]

On 23 June 2022, the OPC announced the appointment of Philippe Dufresne as the new Privacy Commissioner of the OPC. Dufresne will begin his role on 27 June 2022.[2]

On 16 June 2022, Government Bill C-27 (An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act, and the Artificial Intelligence and Data Act), and to make consequential and related amendments to other Acts, was introduced and passed in its first reading in the House of Commons. Known as the Digital Charter Implementation Act, 2022, the bill is divided into three main parts: to enact the Consumer Privacy Protection Act, to enact the Personal Information and Data Protection Tribunal Act, and to enact the Artificial Intelligence and Data Act.[3]

On 29 September 2022, the OPC announced that it had released and tabled in Parliament its 2021-2022 annual report. The annual report highlights investigations under both the Privacy Act of 1985, which applies to the public sector, and PIPEDA, which is the federal private sector privacy law, the tabling of Bill C-27, the Digital Charter Implementation Act, and developments regarding the application of facial recognition technology. The annual report lays out the OPC's vision of privacy, which recognizes:

- Privacy as a fundamental right
- Privacy in support of the public interest and Canada's innovation and competitiveness
- Privacy as an accelerator of Canadians' trust in their institutions and a driver in their participation and contribution toward a robust digital economy.[4]

Data Protection Authority Focus

FINTRAC announced that it has imposed an administrative monetary penalty on Libro Credit Union Limited, also operating as Libro Credit Union. This credit union in London, Ontario, was imposed an administrative monetary penalty of $156,750 on 12 October 2021 for noncompliance with Part 1 of the Proceeds of Crime (Money Laundering) and Terrorist Financing Act and its associated regulations.

1 https://www.dataguidance.com/news/canada-opc-publishes-its-2022-2023-departmental-plan
2 https://www.dataguidance.com/news/canada-opc-announces-appointment-philippe-dufresne-new
3 https://www.dataguidance.com/news/canada-bill-digital-charter-implementation-act-2022
4 https://www.dataguidance.com/news/canada-opc-releases-annual-report-2021-2022

CANADA (CONTINUED)

Law: The Personal Information Protection and Electronic Documents Act (PIPEDA), The Privacy Act

Regulator: Office of the Privacy Commissioner of Canada, Office of the Information and Privacy Commissioner of Alberta, Office of the Information and Privacy Commissioner for British Columbia, Commission d'accès à l'information du Québec

EU Adequacy Decision: yes (Commercial Organisations)

Ziad Akkaoui
Zakkaoui@bdo.ca
+1 (416) 369-6048

Libro Credit Union Limited was found to have committed the following violations:

- Failure to submit suspicious transaction reports where there were reasonable grounds to suspect that transactions were related to a money laundering or a terrorist financing offence
- Failure to take prescribed special measures to mitigate its high risks.[5]

The Canadian Radio-television and Telecommunications Commission's (CRTC) chief compliance and enforcement officer announced penalties totalling $300,000 to four Canadians for their involvement in the dark web marketplace Canadian Headquarters (also known as Canadian HQ). The marketplace was taken offline following the execution of warrants by CRTC staff.[6]

Montecristo Jewellers Inc., a dealer of precious metals and precious stones in Vancouver, British Columbia, was imposed an administrative monetary penalty of $222,750 on 17 February 2022 for committing four violations. The violations were found during a compliance examination in 2019. Montecristo Jewellers Inc. has appealed the decision to the Federal Court.[7]

5 https://fintrac-canafe.canada.ca/pen/amps/pen-2022-01-13-eng
6 https://www.canada.ca/en/radio-television-telecommunications/news/2022/01/crtc-investigation-targets-dark-web-marketplace-vendors-and-administrator.html
7 https://fintrac-canafe.canada.ca/pen/amps/pen-2022-05-12-eng

CAYMAN ISLANDS

Law: The Data Protection Act (2021 Revision), and the Data Protection Regulations, 2018 (SL 17 of 2019), The Data Protection Law (DPL)

Regulator: Office of the Ombudsman

EU Adequacy Decision: no

Richard Carty
rcarty@bdo.ky
+13459281120

Notable Changes

On 31 March 2022, the Office of the Ombudsman (the Ombudsman) released its first quarter report for 2022. The report details the number of inquiries received by the Ombudsman and summarises various statistic relating to data protection. Of the 96 total inquiries received, 36 focused on data protection. The report notes that the Ombudsman dealt with 22 different cases and received 20 breach notification reports, 13 of which were resolved.[1]

The Ombudsman noted on 28 January 2022, International Data Protection Day, that data protection legislation is more crucial to privacy and information rights than ever, given the onset of the Omicron variant of COVID-19.

The Ombudsman's office saw a 15% increase in data protection queries from the public during 2021 and a more than 50% increase in the number of data breaches being reported in cases where the office was notified that personal data had been accessed, lost, altered, or disclosed in an unlawful or unauthorised manner.[2]

Data Protection Authority Focus

The Department of Children and Family Services (DCFS) did not reply when an individual made a subject access request to the DCFS under section 8 of the Data Protection Act (2021 Revision) (DPA) for her own and her child's personal data and related information within the statutory timescale of 30 days. After investigation of the matter, the Ombudsman concluded that DCFS failed to comply with its statutory duty under section 8 of the DPA. An enforcement order was issued, requiring DCFS to provide a comprehensive response no later than the end of business on 7 March 2022.

The Ombudsman also recommended that DCFS draft a comprehensive policy detailing how it will handle section 8 requests in accordance with the DPA in the future.[3]

1 https://www.dataguidance.com/news/cayman-islands-ombudsman-releases-first-quarter-report
2 https://ombudsman.ky/news
3 https://ombudsman.ky/images/pdf/decisions/dp_decisions/DP_Case_202200019_DCFS_Enforcement_ Order.pdf

CHINA

Law: Personal Information Protection Law, Data Security Law

Regulator: The Cyberspace Administration of China ('CAC')

EU Adequacy Decision: no

Min Cai
min.cai@bdo.com.cn
Partner, National Head of Forensic and Cyber Advisory Services
法证与网络安全咨询服务部
全国主管合伙人
Tel: +086 21 2328-2844

Notable Changes

On 14 January 2022, the State Council of the People's Republic of China released its 14th Five-Year Plan on Digital Economy Development. The plan highlights the current digital economy development strategy and outlines basic principles, general requirements, and main objectives.[1]

On 28 February 2022, the CAC announced the launch of the Internet Information Algorithm Filing Service. The CAC noted that the launch of the Filing Service fulfils the requirements of Article 24 of the Internet Information Service Algorithm Recommendation Management Regulations (the Regulations), which came into force on 1 March 2022. [2]

On 24 June 2022, the CAC announced that the Cybersecurity Review Office interviewed the person in charge of Tongfang CNKI (Beijing) Knowledge Network Technology Co., Ltd to prevent national data security risks, maintain national security, and protect public interests in accordance with the Cybersecurity Law 2016, the Data Security Law, and the Cybersecurity Review Measures.[3]

On 14 September 2022, the CAC released its draft Decision Amending the Cybersecurity Law of the People's Republic of China and is requesting public comments on it. The draft decision amends penalties associated with violations of the Cybersecurity Law, introducing fines of up to 5% of the annual turnover.[4]

Data Protection Authority Focus

On 5 July 2022, the CAC announced that it and the National Cybersecurity Office of Thailand had signed a memorandum of understanding (MoU) on cybersecurity cooperation. The CAC noted that the two sides agreed to further strengthen exchanges and cooperation in the field of cybersecurity and maintain cyberspace stability.[5]

On 29 July 2022, the CAC announced that it had signed a cooperation plan with the National Cyber and Cryptography Agency of Indonesia. The CAC noted that the plan aims to deepen cooperation in cybersecurity capacity building between China and Indonesia.[6]

1 https://www.dataguidance.com/news/china-state-council-releases-14th-five-year-plan
2 https://www.dataguidance.com/news/china-cac-announces-launch-internet-information
3 https://www.dataguidance.com/news/china-cac-announces-cybersecurity-review-cnki
4 https://www.dataguidance.com/news/china-cac-requests-public-comments-draft-decision
5 https://www.dataguidance.com/news/international-china-and-thailand-sign-mou-cybersecurity
6 https://www.dataguidance.com/news/china-cac-and-indonesian-cybersecurity-authority-sign.pdf

COLOMBIA

Disposiciones Generales para la protección de datos personales
n/a (we are part of the EU)

Law: Statutory Law 1581 of 2012, Decree 1377 of 2013

Regulator: Colombian Data Protection Authority ('SIC')

EU Adequacy Decision: no

Paula Giraldo Gutierrez
pgiraldo@bdo.com.co
+57 317 331 1331

Notable Changes

Decree No. 092 of 2022 was published on 24 January 2022. The Decree amends the structure and tasks of several SIC offices and also creates an additional office called the Habeas Data Office, which will carry out its functions inside the SIC.[1]

Data Protection Authority Focus

The SIC outlined that the resolution follows an appeal made by Google regarding Resolutions 53593 of 3 September 2020 and 60478 of 21 September 2021 concerning Google's data processing actives. The SIC ordered Google to implement certain measures such as to register their database, create a privacy policy, and implement a mechanism or procedure to comply with the special requirements related to the collection and processing of data of children and adolescents. Google appealed, noting that Google LLC and Google Colombia have a relationship of control and questioned the competence of the SIC and the lawfulness of its order.

On 28 January 2022, the SIC published Resolution No. 2389 of 2022, upholding Resolution 60478 of 21 September 2021. This was following an appeal by Google Colombia Limitada (Google Colombia) for violations of Article 2 Statutory Law 1581 of 2012 (October 17), which Issues General Provisions for the Protection of Personal Data (the Data Protection Law).[2]

On 22 March 2022, the SIC published Resolution No. 13874 of 2022, upholding its decision in Resolution No. 24840 of 28 April 2021 against Raigoza Villegas S.A.S for violations of Articles 8(1), 8(5), 8(8), and 8(10) of the Statutory Law 1266 of 2008 (December 31), which establishes general provisions of habeas data and regulates the management of information contained in personal databases, specifically financial, credit, commercial, and of services derived from third-countries and other provisions (the Law) where the SIC imposed a fine of COP 40 million (approx. €9,600).[3]

On 2 March 2022, the SIC published Resolution No. 9744 of 2022, in which it imposed a fine of COP 27,653,343 (approx. €6,530) to System Group S.A.S., for violation of Articles 8(1), 8(5), and 8(10) of Statutory Law 1266 of 2008 (December 31) which Establishes General Provisions of habeas data and regulated management of information contained in personal databases, specifically financial, credit, commercial, and of services derived from third-countries and other provisions (the Law), regarding failure to ensure the accuracy and quality of personal data, and lack of informed consent for processing personal data.[4]
On 23 March 2022, the SIC published Resolution No. 14242 of 2022, in which it upheld its decision in Resolution No. 20809 of 2021 to impose a fine of COP 50,032,424 (approx. €11,970) on Banco de Bogotá S.A. for violations of Articles 4(f), 4(g), and 17(d) of the Statutory Law 1581 of 2012 (October 17).

1 https://www.dataguidance.com/news/colombia-decree-amend-sic-structure-published
2 https://www.dataguidance.com/news/colombia-sic-upholds-resolution-requiring-google-0
3 https://www.dataguidance.com/news/colombia-sic-upholds-its-decision-fine-raigoza-cop-40m
4 https://www.dataguidance.com/news/colombia-sic-fines-systemgroup-cop-276m-unlawful

COSTA RICA

Law: Protection of Persons Regarding the Processing of their Personal Data No. 8968 of 2011
Regulator: Agency for the Protection of Inhabitants' Data) (PRODHAB)

EU Adequacy Decision: no

Carlos González
cgonzalez@bdo.cr
+506 2231 7060

Notable Changes

The law was approved on 5 September 2011. The corresponding regulation was approved on 5 March 2013. As of 5 June 2014, all extensions and transitory were fulfilled, for which its current application is mandatory.

This is a public order law that applies to both public and private entities.

The government agency that ensures the application of the law is the Agency for the Protection of Inhabitants' Data (PRODHAB), an entity of the Ministry of Justice.

The Law applies to personal data contained in automated or manual databases, public or private organisations, and any form of subsequent use of such data within the territory of Costa Rica, or where applicable to Costa Rican legislation by virtue of the conclusion of a contract or international law (Article 2 of the Law, and Article 3 of the Executive Decree).

Technically, the Law does not apply to any database held by individuals or legal entities for exclusively internal, personal, and/or domestic purposes. However, PRODHAB is able to apply the Law to any database even if it has not been used for internal, personal, or domestic purposes.

Data Protection Authority Focus

PRODHAB's main duties and responsibilities, among others, are (Article 16 of the Law):

- processing any claim related to a data protection matter;
- administrating the registration procedure of the databases that must comply with such requirements;
- requesting any information regarding the data processing made by any entity;
- creating awareness regarding data protection aspects;
- elaborating guidelines for any aspect regarding data protection; and
- if needed, issuing mandatory orders to the data controllers in order to comply with the data subjects' rights.

PRODHAB may initiate proceedings sue sponte, or upon request by a person with a legitimate interest or subjective right (Article 24 of the Law, and Article 58 of the Executive Decree). After receiving such a request, PRODHAB will grant data controllers three working days to reply and offer evidence considered relevant for their defense (Article 25 of the Law).

PRODHAB can also investigate and gather evidence and may issue any interim and provisional measures that it deems necessary. Proceedings end with a final judgment which is subject to appeal.

For an offence under the Law, PRODHAB can issue sanctions which can be minor (Article 29 of the Law), serious (Article 30 of the Law), or extremely serious (Article 31 of the Law). Accordingly, the penalty will vary depending on the seriousness of the offence and can range from a fine of approximately $3,000 to $18,000. In the most severe cases, the result could be the closure of the database for a period of one to six months (Article 28(c) of the Law).

1 https://www.dataguidance.com/notes/costa-rica-data-protection-overview

CZECH REPUBLIC

Law: Act No. 110/2019 Coll. on Personal Data Processing and the GDPR

Regulator: Office for Personal Data Protection ('UOOU')

EU Adequacy Decision: n/a

Stanislav Klika
stanislav.klika@bdo.cz
+420 604226734

Notable Changes

On 17 February 2022, the UOOU published its 2022 control plan, which focuses on compliance for emerging technologies. The plan includes inspection on legislative reform, such as the requirement of opt-in consent for cookies, electronic communications (and amending some related acts – the Electronic Communications Act), the dissemination of unsolicited SMS marketing, and its Smart Quarantine project.[1]

On 5 August 2022, an amendment to the Act on Cybersecurity was published in the Collection of Laws. The law was prepared by the National Office for Cyber and Information Security, with the aim of adapting the Czech legal system to the regulation of the European Parliament and the Council of the EU with the abbreviated name "Cyber Security Act." The new law states that the national cyber security certification authority is the National Office for Cyber and Information Security.[2]

On 22 August 2022, the National Cyber and Information Security Agency (NÚKIB) published a guide on asset and risk on security measures, cybersecurity incidents, reactive measures, cybersecurity reporting requirements, and data disposal.[3]

Data Protection Authority Focus

The UOOU found that the Czech National Police violated Section 79(3) of the Police Law, which stipulates that data on racial or ethnic origin, religious, philosophical or political beliefs, trade union membership, health status, sexual behaviour, or sexual orientation may only be collected if it is necessary for the purposes of investigating a specific crime or misdemeanour, or when providing protection of persons.

As a result of the violation, the UOOU imposed the fine of CZK 975,000 on the Ministry of Interior, clarifying that the fine was on the processing of personal data because the Police of the Czech Republic does not have legal personality.[4]

1 https://www.dataguidance.com/news/colombia-decree-amend-sic-structure-published
2 https://www.dataguidance.com/news/colombia-sic-upholds-resolution-requiring-google-0
3 https://www.dataguidance.com/news/colombia-sic-upholds-its-decision-fine-raigoza-cop-40m
4 https://www.dataguidance.com/news/colombia-sic-fines-systemgroup-cop-276m-unlawful

DENMARK

Law: The Danish Act on Supplementary Provisions, GDPR

Regulator: Danish Data Protection Authority ('Datatilsynet'), Centre for Cybersecurity, Danish Business Authority

EU Adequacy Decision: n/a

Mikkel Jon Larssen
mla@bdo.dk
+45 30 70 43 34

Notable Changes

On 7 February 2022, the Danish Business Authority (DBA) announced that it had updated the guidelines on ESG reporting so that companies can report their ESG figures more quickly and easily. The DBA stated that the guidelines relate to companies' ability to report their ESG figures in a corporate social responsibility statement in connection with their annual reports.[1]

On 24 February 2022, the DBA published guidance on the use of third-party cookies and similar technologies on government self-service solutions and national web portals used by citizens. The DBA stated that the guidance states that cookies may no longer be used on such solutions and portals if third parties can then use the collected data for their own purposes, thereby offering citizens greater protection of their personal data. In this regard, the guidance states that its purpose is to strengthen citizens' trust in authorities by ensuring third parties do not collect information about citizens on solutions and portals.[2]

Data Protection Authority Focus

On 8 June 2022, the Datatilsynet announced that it had published a short, informative note on the concept of "data exporters." The Datatilsynet specified that the note is primarily targeted at controllers that use European processors where one or more of its sub-processors are located outside the EU/EEA, as well as processors in the EU/EEA that provide services using sub-processors outside the EU/EEA. The Datatilsynet stated that with regards to data transfers, Article 44 of the General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) imposes an obligation on both controllers and processors, where both parties are required to ensure that an effective transfer basis is provided in the light of the circumstances of the transfer. [3]

On 7 July 2022, the DBA announced that it would be inspecting a number of websites aimed at children and young people, with a focus on different types of cookies and similar technologies that can be used to share information with third parties. The DBA stated the reason behind this inspection is children's vulnerability when using the internet. [4]

1 https://www.dataguidance.com/news/denmark-dba-announces-updated-guidelines-esg-reporting%C2%A0
2 https://www.dataguidance.com/news/denmark-dba-publishes-cookie-guidance-government-self
3 https://www.dataguidance.com/news/denmark-datatilsynet-issues-statement-concept-data
4 https://www.dataguidance.com/news/denmark-dba-announces%C2%A0cookie-inspections-websites

FINLAND

Law: The Data Protection Act (1050/2018), GDPR

Regulator: Office of the Data Protection Ombudsman

EU Adequacy Decision: n/a

Ossi Määttä
ossi.maatta@bdo.fi
+358503511453

Notable Changes

There have been no changes in legislation in Finland. Customer behaviour has begun to change due to the decisions of the Data Protection Authorities and because of data leaks published for the public interest.

On 24 March 2022, the Finnish government announced that it had submitted a proposal to Parliament to amend the Employment Data Protection Act (759/2004). The government noted that the proposal would clarify an employer's right to collect employees' personal data, stating[1] that the aim of the proposal would be to clarify the regulation with respect to the GDPR and employment practices.

On 30 September 2022, the Ombudsman published a Guide on the Processing of Social Welfare Customer Data. The Ombudsman stated the Guide contains instructions on making customer registrations, keeping social welfare information confidential, and implementing customers' data subject rights. The Guide also provides advice on control of user rights and the storage and disposal of customer data.[2]

Data Protection Authority Focus

The Ombudsman stated that it received 11 complaints between 2018 and 2021 concerning Otavamedia's processing of personal data, noting that the complainants had not received responses to their data subject requests or inquiries.

Otavamedia's explanation to the Ombudsman was that some of the data subject requests did not receive a response due to technical problems with email control in connection with the change of service provider, and during the error, messages received in the inbox reserved for data protection issues had not been forwarded to customer service.

As a result, the sanctions board imposed a fine of €85,000 to Otavamedia for failure to respond to data subject rights via the email channel. In addition, the Ombudsman ordered Otavamedia to correct its practices in compliance with data protection rules and.[3]

On 4 July 2022, the Ministry of Digital Economy and Society (MDES) renewed its memorandum of understanding (MoU) with Finland on Telecommunication and ICT Cooperation and Digital Technology. The MDES said that the renewal is meant to expand cooperation in ICT and digital technology and will cover areas including policies and regulations on telecommunication, ICT, and digital technology. According to the MDES, the renewal aims to develop and promote information communications and digital industries, such as hardware, software, digital content, and technology for services. Furthermore, the MDES stated the renewed MoU will look at cooperation in digital innovation, such as Big Data, Internet of Things (IoT), as well as artificial intelligence and digital ecosystems including smart cities.[4]

1 https://www.dataguidance.com/news/denmark-dba-announces-updated-guidelines-esg-reporting%C2%A0
2 https://www.dataguidance.com/news/denmark-dba-publishes-cookie-guidance-government-self
3 https://www.dataguidance.com/news/denmark-datatilsynet-issues-statement-concept-data
4 https://www.dataguidance.com/news/denmark-dba-announces%C2%A0cookie-inspections-websites

FINLAND (CONTINUED)

Law: The Data Protection Act (1050/2018), GDPR

Regulator: Office of the Data Protection Ombudsman

EU Adequacy Decision: n/a

Ossi Määttä
ossi.maatta@bdo.fi
+358503511453

On 31 May 2022, the Deputy Data Protection Ombudsman made a decision that the workstations of the personal data processor's registrar customers have systematically had the location data access function turned on by default. The processor of personal data is given an order by Article 58, paragraph 2, subparagraph d of the General Data Protection Regulation to ensure that the location information function is not unjustifiably turned on by default in the Windows 10 workstations of current customers. Pursuant to this regulation, the personal data processor must turn off the location data feature on customers' Windows 10 workstations by 8 August 2022, unless the controller has instructed the processor otherwise. To ensure the controller's position, the personal data processor must notify the controller's customers of future changes without delay, and these controller's customers must be given the actual opportunity to inform the processor that the location data function should not be disabled. By 19 August 2022, the personal data processor must provide the data protection commissioner's office with information about which data controllers have announced that the location data feature should not be turned off, as well as confirmation of the deactivation of the location data function from other workstations of the data controller's customers. The personal data processor is given an order by Article 58, paragraph 2, subsection d of the General Data Protection Regulation to delete the personal data generated by the use of the location information feature in those parts of Windows 10 workstations where the location information feature has been turned on without justification.

The personal data processor must submit to the data protection commissioner's office confirmation of the measures taken by 18 August 2022.

On 15 November 2022, the Data Protection Ombudsman issued a notice to the Tax Administration regarding excessively extensive requests for information. The investigation by the Office of the Data Protection Ombudsman revealed that the Tax Administration had requested information from banks on all account transfers that crossed the borders of Finland in the years 2015–2021. The information requests covered, among other things, purchases paid by bank card in foreign stores and online stores. In addition to the notice, the data protection commissioner ordered the Tax Administration to delete personal data processed in violation of the data protection regulation and to stop submitting excessively extensive information requests to banks.

The Tax Administration submitted requests for information on cross-border account transfers to banks operating in Finland. Cross-border bank transfers refer to outgoing and incoming payments where the payer's or recipient's bank is located elsewhere than in Finland. The information requests also covered cross-border payments made with payment cards related to the use of the account, such as purchases paid with a bank card during trips abroad or in foreign online stores. The Tax Administration asked the banks to provide, among other things, the payment amount, date and customer contact information. The data materials were requested for the purpose of tax supervision.

FINLAND (CONTINUED)

Law: The Data Protection Act (1050/2018), GDPR

Regulator: Office of the Data Protection Ombudsman

EU Adequacy Decision: n/a

Ossi Määttä
ossi.maatta@bdo.fi
+358503511453

The Tax Administration did not limit requests for information based on the size of account transactions, for example, or consider children as a group in need of special protection. The Data Protection Commissioner considered that the information requests covered a significant part of the banks' customer registers based on the nature of the information request and the number of account holders. For example, for 2018, the three largest datasets submitted by banks to the Tax Administration comprised a total of approximately 17,860,000 account transactions. In terms of the number of account holders, the three largest materials concerned approximately 880,000 account holders, of which approximately 85 percent have been private individuals.

The Data Protection Commissioner considers that the Tax Administration has not sufficiently taken into account the risks related to the processing of personal data. When the use of cash has moved more and more to payment traffic via a bank account, a more detailed picture of a person's private life can be obtained based on account transactions.

FRANCE

Law: Amended Law No 78-17 of 6 January 1978 relating to computing, files, and freedom of information, GDPR

Regulator: French Data Protection Authority ('CNIL')

EU Adequacy Decision: n/a

Bruno Saucourt
bruno.saucourt@bdo.fr

Notable Changes

On 1 September 2022, a law aimed at improving the protection of whistle blowers came into effect in France. The law transposes the Directive on the Protection of Persons who Report Breaches of Union Law (the Whistleblowing Directive) into French law and amends the legal framework for the protection of whistle blowers, as established by Law No. 2016-1691 of 9 December 2016, on Transparency, the Fight against Corruption, and the Modernization of Economic Life (Sapin II). Notably, the law expands the definition of a whistle blower, which is now defined as "a natural person who reports or discloses, without direct financial compensation and in good faith, information relating to a crime, an offence, a threat or harm to the general interest, a violation, or an attempt to conceal a violation of international or European Union law, law or regulation."[1]

On 20 September 2022, the CNIL launched a public consultation on its draft technical recommendations on the use of application programming interfaces (APIs) for the purposes of secure sharing of personal data.[2]

On 16 May 2022, the CNIL published guidance outlining criteria for assessing the legality of cookie walls, i.e., the practice of conditioning access to a service on the internet user's consent to the deposit of cookies or similar tracking technologies on their terminal device.[3]

Data Protection Authority Focus

The CNIL carried out an online investigation of the infogreffe.fr website,[4] which allows users to consult legal information on companies and order documents certified by the commercial court registries.

The Key findings were:

- Failure to comply with the obligation to keep data for a period proportionate to the purpose of the processing (Article 5.1.e of the GDPR)
- Failure to comply with the obligation to ensure the security of personal data (Article 32 of the GDPR)

Based on these findings, the restricted committee (the CNIL body responsible for imposing sanctions) issued a fine of €250,000 on Infogreffe and decided to make it public. This decision was taken in cooperation with the other European authorities concerned, as user accounts were created from all EU Member States.[5]

The CNIL outlined that it and various other European data protection authorities had received complaints regarding challenges encountered when exercising data subject rights with Accor, a hotel company.
After investigating, the CNIL announced on 3 August 2022 that it had issued a fine of €600,000 to Accor SA for violations of Articles 12, 13, 15, 21, and 32 of the GDPR and Article L. 34-5 of the Postal and Electronic Communications Code.[6]

1 https://www.dataguidance.com/news/france-whistleblowing-law-enacted
2 https://www.dataguidance.com/news/france-cnil-launches-public-consultation
3 https://www.dataguidance.com/news/france-cnil-publishes-criteria-assessing-legality
4 https://www.dataguidance.com/news/france-cnil-fines-gie-infogreffe-250000-data-retention
5 https://edpb.europa.eu/news/national-news/2022/french-sa-fines-economic-interest-group-infogreffe-eur-250000_en
6 https://www.dataguidance.com/news/france-cnil-fines-accor-600000-various-direct-marketing

FRANCE (CONTINUED)

Law: Amended Law No 78-17 of 6 January 1978 relating to computing, files, and freedom of information, GDPR

Regulator: French Data Protection Authority ('CNIL')

EU Adequacy Decision: n/a

Bruno Saucourt
bruno.saucourt@bdo.fr

The Hellenic Data Protection Authority (HDPA) stated that it had received complaints at the same time as four others before the supervisory authorities of Austria, France, Italy, and the U.K. The complainants claimed that Clearview AI violated their access right under Article 15 of the GDPR. The HDPA reminded Clearview AI that the provisions under Article 3(2) and 27 of the GDPR related to the territorial scope of the GDPR and the controller's obligation to appoint a representative where the same is not established in the EU, which Clearview AI contradicted, noting that it does not provide products or services to data subjects within the EU, nor monitor their behaviour and that it only provides its services to law enforcement agencies outside the EU.

On 14 July 2022, the HDPA published its decision, imposing a fine of €20 million on Clearview AI, Inc. for violations of Articles 5(1)(a), 6, 9, 12, 14, 15, and 27 of the GDPR, following a complaint submitted by Homo Digitalis on behalf of the data subject.[7]

7 https://www.dataguidance.com/news/greece-hdpa-fines-clearview-ai-20m-lawfulness-and

GEORGIA

Law: Law of Georgia on Personal Data Protection of 28 December 2011 No. 5669

Regulator: Office of the Personal Data Protection Inspector ('PDP')

EU Adequacy Decision: No

Anzor Mekhrishvili
amekhrishvili@bdo.ge
+995598212007

Notable Changes

The European Parliament announced, on 23 June 2022, that it had adopted, on the same date, a resolution calling on heads of state or Government to grant EU candidate status to Ukraine and the Republic of Moldova without delay, with Georgia to follow, once certain reforms are delivered.

On 17 August 2021, PDP published a statement, in which it imposed a fine of GEL 1,000 (approx. €284), setting out its findings following an investigation into the lawfulness of the disclosure of patient's health data on social media by a doctor.

On 24 September 2021, PDP published its decision in which it imposed a fine of GEL 2,000 (approx. €570) to the Ministry of Internal Affairs of Georgia, for violations of Articles 43(2) and 44(2) of the Law of Georgia on Personal Data Protection of 28 December 2011 No. 5669 and also a fine of GEL 500 (approx. €140) to a medical institution for violations of Articles 43(1), 44(1), and 46(1) of the Law, following the PDP's inspection into the legality of disclosing video recordings of the movement of Alexander (Lexo) Lashkarava.

Data Protection Authority Focus

In May 2019 the PDP announced the draft law on Personal Data Protection, which aims at bringing Georgian legislation on personal data protection into closer alignment with the GDPR. According to the state of Georgia's website, 'GDPR applies only to the extent Georgia governmental entities have a physical location within Europe, monitor consumer behaviour in Europe (such as through electronic data collection or analysis), or offer goods and services into Europe. The Georgian State Inspector's Service outlines the interest of Georgian companies and when they must comply with GDPR. The Georgia State Inspector's Service is providing guidance to Georgian companies with relevant recommendations.

When the draft law passes it will provide further guidance on the principles of data processing, data subjects rights, children's consent, deceased persons data processing, monitoring, direct marketing, data controller and data processor obligations, data transfers, enforcements, and penalties for noncompliance.

GERMANY

Law: Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG), GDPR

Regulator: Germany does not have one central Data Protection Authority. There are 16 Data Protection Authorities for each German state. German Federal Commissioner for Data Protection and Freedom of Information (Bundesbeauftragte für Datenschutz und Informationsfreiheit – 'BfDI')

EU Adequacy Decision: n/a

Hans-Peter Toft
Hans-peter.toft@bdolegal.de
+49 40 30293-945

Notable Changes

On 4 May 2022, the German Data Protection Conference (DSK) published its resolution calling for an employee data protection law, as issued on 29 April 2022. The DSK called on the legislature to create legal regulations in the use of algorithmic systems, including artificial intelligence (AI), as part of an independent employee data protection law. In addition, the DSK noted that intrusive data processing should be prohibited and called for profiling to be subject to the prohibition and exceptions under Article 22 of the GDPR, including in the context of employment.[1]

On 6 May 2022, the Federal Office for Information Security (BSI) announced that it had expanded the scope of its IT security label and that, from May 2022, manufacturers of smart cameras, smart speakers, smart cleaning and garden robots, smart toys, and smart television products will be able to apply for the same.[2]

On 29 September 2022, the BSI published a guide on the use of attack detection systems, which provides guidance on the requirements for operators of critical infrastructures, operators of energy plants and energy supply networks, and auditing bodies. The BSI explained that the operators are obliged to take appropriate organizational and technical precautions to avoid disruptions as well as being required to operate their information technology systems, components, or processes in accordance with the principles of integrity, authenticity, and confidentiality.[3]

On 13 June 2022, the BSI announced that it had published a new draft guidance on the use of attack detection systems. The draft guidance provides pointers on the requirements that operators of critical infrastructures, operators of energy systems and energy supply networks, and testing bodies must abide by.[4]

On 16 December 2022 the first chamber of the German parliament, Bundestag, passed the proposed Whistle blower Protection Act (HinSchG) to transpose the Directive on the Protection of Persons who Report Breaches of Union Law (Directive (EU) 2019/1937) (the Whistleblowing Directive) into German law. The proposed act, will likely be passed by the second chamber of the German parliament, the Bundesrat in mid-February.[5]

1 https://www.dataguidance.com/news/germany-dsk-issues-resolution-calling-employee-data
2 https://www.dataguidance.com/news/germany-bsi-expands-scope-it-security-label-includes
3 https://www.dataguidance.com/news/germany-bsi-publishes-guidance-use-attack-detection
4 https://www.dataguidance.com/news/germany-bsi-publishes-draft-guidance-use-attack
5 https://www.bundestag.de/dokumente/textarchiv/2022/kw50-de-hinweisgeber-926806

GERMANY (CONTINUED)

Law: Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG), GDPR

Regulator: Germany does not have one central Data Protection Authority. There are 16 Data Protection Authorities for each German state. German Federal Commissioner for Data Protection and Freedom of Information (Bundesbeauftragte für Datenschutz und Informationsfreiheit – 'BfDI')

EU Adequacy Decision: n/a

Hans-Peter Toft
Hans-peter.toft@bdolegal.de
+49 40 30293-945

Data Protection Authority Focus

On 12 May 2022, the Berlin Data Protection Authority (the Berlin Commissioner) announced its guidance on data transfers to third countries, addressing what applies after the Court of Justice of the European Union's (CJEU) judgment in *Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems* (C-311/18) (Schrems II) and the audits it has initiated in this regard. The guidance provides a breakdown of data export requirements under the GDPR and notes that the concept of transmitting data abroad is large in scope, requiring organisations to consider their entire service/value chain. The guidance also gives an overview of the current legal situation with regards to international transfers and particularly those that concern the U.S., highlighting the legal opinion that the German Data Protection Conference had commissioned and outlining the implications of Scherms II.[6]

On 1 September 2022, the BfDI announced via its Mastodon account that it had published an article on the destruction of data mediums.
The BfDI stated that data protection requirements must be considered when destroying data mediums. The BfDI specified that the destruction of data mediums is a technical and organisation measure to ensure data security and that, as such, the technical requirements described in the DIN standard 66399 "Office and data technology - Destruction of data carriers" (the Standard) must be observed.[7]

On 24 November 2022 the German Data Protection Conference (DSK) published their assessment of the use of Microsoft 365 as data processing service.[8] The DSK found Microsoft not in compliance with the transparency and accountability requirements under Art. 5 GDPR particularly regarding Microsoft's own use of data. The DSK's assessment was based on the Microsoft Products and Services Data Protection Addendum ("DPA") of September 2022. The DSK assessment gained major media attention. Microsoft reacted stating that the DSK is exceeding the requirements of GDPR.[9]

As a reaction to President Biden's Executive Order 14086 and the implementation of the proposed EU-US Privacy Framework and the expected adequacy decision, the Hamburg DPA is taking a balanced view of the U.S. Executive Order on "Enhancing Safeguards for United States Signals Intelligence Activities" by pointing at the positive aspects of the executive order while at the same time not losing sight of remaining challenges. The Hamburg DPA stated that the legal protection procedure might lack transparency and bulk collection of data by U.S. government agencies is continued, and that it is therefore not clear from the text to what extent the new proportionality clause specifically changes bulk collection.

6 https://www.dataguidance.com/news/germany-bsi-publishes-draft-guidance-use-attack
7 https://www.dataguidance.com/news/germany-federal-cabinet-passes-draft-whistleblowingA066399-requirements
8 https://datenschutzkonferenz-online.de/media/dskb/2022_24_11_festlegung_MS365_zusammenfassung.pdf; https://datenschutzkonferenz-online.de/media/dskb/2022_24_11_festlegung_MS365_abschlussbericht.pdf
9 https://news.microsoft.com/wp-content/uploads/prod/sites/40/2022/11/2022.11_Stellungnahme-MS-zu-DSK_25NOV2022_FINAL.pdf

GUERNSEY

Law: The Data Protection (Bailiwick of Guernsey) Law, 2017 (the Law) and The Data Protection (Commencement, Amendment and Transitional) (Bailiwick of Guernsey) Ordinance, 2018, (the Ordinance)

EU Adequacy Decision: yes

Richard Searle
Richard.Searle@bdo.gg
+44 (0)1481 724561

Notable Changes

New guidelines of data transfer were published by the ODPA on 21 June 2022 to help organisations navigate the complex legal framework of data transfer.[1]

On 6 May 2022, the Office of the Data Protection Authority (ODPA) announced a cybersecurity checklist. The ODPA also urged the companies and individuals to take steps to reduce the risk of becoming a target.[2]

The ODPA has also released a factsheet that would impact the process of collection and usage of personal data about potential, new, and existing employees as currently followed by organisations. This is against the backdrop of the introduction of discrimination legislation in Guernsey.[3]

A data protection guidance for employers was also published by the ODPA. This guidance would help the employers make decisions on their employees' data and manage employment relationships.[4]

Data Protection Authority Focus

The 2021 annual report released by the ODPA said that is has received 180 personal data breach reports and has assessed 35 complaints about the local data controller. Further, the ODPA conducted 17 investigations and one inquiry.[5]

The ODPA has also issued reprimands to companies for cases such as failure to adequately respond to DSAR,[6] for unlawful disclosure of sensitive personal data,[7] and the unlawful processing of data.[8]

Proper data protection measures are important for any company handling data. To help maintain an adequate level of cybersecurity, the ODPA published a cybersecurity checklist and highlighted to the companies the need to take steps to reduce the risk of becoming a target. [9]

1 https://www.dataguidance.com/news/guernsey-odpa-publishes-new-guidance-data-transfers
2 https://www.dataguidance.com/news/guernsey-odpa-publishes-cybersecurity-checklist
3 https://www.dataguidance.com/news/guernsey-odpa-publishes-factsheet-employers-lawful-data
4 https://www.dataguidance.com/news/guernsey-odpa-publishes-data-protection-guidance
5 https://www.dataguidance.com/news/guernsey-odpa-publishes-2021-annual-report
6 https://www.dataguidance.com/news/guernsey-odpa-issues-reprimand-bwci-pension-failure
7 https://www.dataguidance.com/news/guernsey-odpa-issues-reprimand-and-compliance-order
8 https://www.dataguidance.com/news/guernsey-odpa-issues-reprimand-hsbc-unlawful-processing
9 https://www.dataguidance.com/news/guernsey-odpa-publishes-cybersecurity-checklist

HONG KONG

Law: Personal Data (Privacy) Ordinance (Cap. 486) as amended in 2012 ('PDPO')

Regulator: The Office of the Privacy Commissioner for Personal Data ('PCPD')

EU Adequacy Decision: no

Ricky Cheng
Rickycheng@bdo.com.hk
+852 2218 8266

Notable Changes

In October 2021, changes were introduced to the PDPO by The Personal Data (Privacy) (Amendment) Ordinance (Amendment Ordinance). New offenses of doxing and corresponding penalties were also introduced. The Amendment also gave the Privacy Commissioner power to carry out criminal investigations and prosecute for doxing and related offenses.[1]

Data Protection Authority Focus

A guidance on recommended model clauses and its implications and comparison against EU SCCs was also released by the PCPD in 2022. This guidance supplements the previous PCPD 2014 Guidance on Cross-Border Data Transfer and updates the Recommended Model Contract Clauses previously annexed to the 2014 Guidance.[2]

Personal data security risks are also exacerbated due to increased digitisation. A good data security system is critical in the present day and age. Keeping this in mind, the PDPC released a guidance note in August 2022 that would provide data users with recommended data security measures.[3]

On 6 October 2022, the Shatin Magistrates' Court convicted a 27-year-old male of charges relating to the new doxing offense. This is the first conviction under the new anti-doxing law introduced by the 2021 Ordinance.[4] Several arrests have also been made by the PCPD for suspected doxing offenses.[5]

1 https://www.dataguidance.com/opinion/hong-kong-amendments-hong-kong-privacy-law-combat
2 https://www.dataguidance.com/opinion/hong-kong-pcpd-guidance-recommended-model-clauses
3 https://www.pcpd.org.hk/english/resources_centre/publications/files/guidance_datasecurity_e.pdf
4 https://www.pcpd.org.hk/english/news_events/media_statements/press_20221006.html
5 https://www.dataguidance.com/news/hong-kong-pcpd-announces-arrest-suspected-doxxing-2
https://www.dataguidance.com/news/hong-kong-pcpd-announces-arrest-suspected-doxxing-1
https://www.dataguidance.com/news/hong-kong-pcpd-announces-arrest-suspected-doxxing-0

INDIA

Law: (Pending) Personal Data Protection Bill, 2019

Regulator: None

EU Adequacy Decision: no

Saumil G Shah
saumilgshah@bdo.in
+919900079563

Notable Changes

The Indian government withdrew its long-awaited Personal Data Protection Bill (PDPB) on 3 August 2022, and it is no longer being considered by Parliament.[1] In its place would be a fresh bill that will take up all the recommendations made by the Joint Committee of Parliament.[2]

Data Protection Authority Focus

After shelving the Personal Data Protection Bill (PDPB) 2018-2019, the Ministry of Electronics and IT (MeitY) released the Digital Personal Data Protection Bill in November 2022 (DPDP Bill). The Bill was introduced 3 months after the withdrawal of the Data Protection Bill. The new Bill is noticeably shrunken version from the previous draft bill. The number of clauses has gone from 90 to 30 and levies heavy penalties for data breaches and non-compliance with the law. The newly released DPDP was open for public feedback until 17 December 2022. The Government is hopeful of introducing this Bill in the upcoming Budget session of Parliament in February 2023.

The government is now working on a new bill that will be unveiled soon.[3] The Minister for Telecom and IT has hinted that the draft bill will be soon released for consultation and will be presented to the Parliament during the budget session of 2023.[4]

1 https://www.dataguidance.com/jurisdiction/india
2 https://www.thehindu.com/opinion/interview/ashwini-vaishnaw-interview-new-draft-data-protection-bill-to-be-out-soon-for-consultatioN/Article65822798.ece
3 https://techcrunch.com/2022/08/03/india-government-to-withdraw-personal-data-protection-bill/
4 https://www.thehindu.com/opinion/interview/ashwini-vaishnaw-interview-new-draft-data-protection-bill-to-be-out-soon-for-consultatioN/Article65822798.ece

IRELAND

Law: Data Protection Act 2018, GDPR

Regulator: Data Protection Commission ('DPC')

EU Adequacy Decision: n/a

David McCormick
DMcCormick@bdo.ie or DPO@BDO.ie
+353 1 4700000

Notable Changes

The DPC is the national supervisory authority tasked with monitoring the application of the GDPR in Ireland and is also the lead authority for regulating big tech companies that are based in Ireland but operate across the European Union.

In October 2022, the DPC released guidance on data subject rights for data controllers.[1] Due to an amendment in the Communications (Retention of Data) Act, the retention of communication and location data in a general and indiscriminate manner can only be done on national security grounds, where approved by the designated judge.[2]

Data Protection Authority Focus

The DPC has also provided a final decision about whether WhatsApp, owned by Facebook, has discharged its GDPR transparency obligations regarding the provision of information and the transparency of that information to users and non-users of WhatsApp's services. In the decision, the DPC concluded that the users were not properly informed. WhatsApp was consequently fined an amount of €225 million.[3]

Despite its efforts regulating large tech businesses, the DPC has been criticised by some for the slow pace of progress. The European Parliament's Civil Liberties Committee has expressed concerns that the DPC, as the lead authority in the EU, has failed to regulate the big tech companies headquartered in Dublin. In its defence, the DPC has highlighted the complexity and significant resources necessary for each inquiry underway and pointed to the EU's own consultation process as a factor slowing the finalisation of DPC decisions.

Irish Council for Civil Liberties (ICCL) also sued DPC in 2022 over failure to act on the biggest data breach by Google.[4]

On 6 October 2022, a report on the handling of cross-border complaints under GDPR was published by the DPC. The report provided an overview of the complaint handling process used by the DPC and said that nearly 20,000 complaints were received post-GDPR, out of which 17,000 had been resolved.[5]

1 https://www.dataprotection.ie/sites/default/files/uploads/2022-10/20221005%20Subject%20Access%20Requests%20A%20Data%20Controller%27s%20Guide.pdf
2 https://www.dataguidance.com/news/ireland-president-signs-communications-data-retention
3 https://www.twobirds.com/en/insights/2021/uk/irish-data-protection-commission-whatsapp-decision#:~:text=The%20DPC%20concluded%20that%20WhatsApp,as%20required%20by%20GDPR%20Art.
4 https://www.iccl.ie/news/iccl-sues-dpc-over-failure-to-act-on-massive-google-data-breach/
5 https://www.dataguidance.com/news/ireland-dpc-publishes-updated-statistical-report

ISRAEL

Law: Protection of Privacy Law, 5741-1981 (the Privacy Law), and the Privacy Protection (Data Security) Regulations

Regulator: Privacy Protection Authority (PPA)

EU Adequacy Decision: yes

Gali Sela
galis@bdo.co.il

Notable Changes

The Privacy Protection Authority (PPA) is Israel's data privacy authority and is the regulating and enforcing authority for personal digital information.[1] The legal framework regarding data privacy is mainly governed by the Protection of Privacy Law, and the Privacy Protection (Data Security) Regulations. There are also regulations regarding transfer of data abroad, as well as regulations regarding transfer of data between public entities.[2]

On 5 January 2022, a draft bill clarifying the terms of the privacy law and increasing the PPA enforcement powers was submitted to the Israeli Parliament and is currently in discussion in the Parliamentary committee.[3] The bill would partly align the data privacy framework of Israel with the GDPR.[4]

Data Protection Authority Focus

The PPA has released many guidelines on topics such as right to access, workplace surveillance, and use of outsourcing services for personal data processing. Guidelines are used to clarify the interpretation of the Privacy Protection Law and to remove uncertainties and ambiguities.[5]

In January 2022, it released DPO guidelines to explain the process of appointment of the DPO and their roles and responsibilities in the organisation.[6]

In 2022, the PPA signed an agreement with the Data Protection Authority of Abu Dhabi for enhanced cooperation between the two authorities and mutual learning of their respective legislations.[7]

Under the current regulatory framework, the PPA has limited power to impose fines, i.e., only for cases of data use for non-consented purpose. It cannot impose fines for the cases of data security violations. The recently introduced bill seeks to change this by giving the PPA power to impose fines of USD $1 million for unauthorised use of data and violating purposeful processing principles, and a fine of up to USD $100,000 for other violations under DSR 2017.[8]

1 https://www.gov.il/en/departments/the_privacy_protection_authority/govil-landing-page#:~:text=The%20Privacy%20Protection%20Authority%20is,information%20held%20in%20digital%20databases.
2 https://www.gov.il/en/Departments/legalInfo/legislation
3 https://iapp.org/news/a/a-turning-point-for-privacy-laws-in-israel/
4 https://resourcehub.bakermckenzie.com/en/resources/data-privacy-security/emea/israel/topics/key-data-privacy-and-security-laws
5 https://www.gov.il/en/Departments/General/guidelines_ppa
6 https://www.gov.il/he/departments/publications/reports/dpo_doc_kit
7 https://www.gov.il/en/departments/news/mou_abu_dhabi
8 https://iapp.org/news/a/a-turning-point-for-privacy-laws-in-israel/

ITALY

Law: Personal Data Protection Code, Containing Provisions to Adapt the National Legislation to General Data Protection Regulation (Regulation (EU) 2016/679) ('the Code'), Legislative decree n. 196/03 integrating GDPR provisions, GDPR

Regulator: Italian Data Protection Authority ('Garante')

EU Adequacy Decision: n/a

Stefano Minini (partner)
stefano.minini@bdo.it
+393346829871

Notable Changes

The GDPR was implemented in Italy by amending the parts of Personal Data Protection Code and repealing those parts that were conflicting with the GDPR. The two laws are working in harmony to govern the data privacy framework in Italy. The Garante has also issued a guide on the application of the GDPR as well as an FAQ, which approves of all the guidelines and opinions issued by Article 29 Working Party.[1]

The Legislative Decree No. 101 of 10 August 2018 (with provisions for the Adaptation of the National Legislation to the Provisions of the General Data Protection Regulation 2016/679) ('the Decree') amended the former Code (Legislative decree n. 196/03) to implement the provisions of the GDPR. The Decree, which was published in the Italian Official Gazette on 4 September 2018 and came into effect on 19 September 2018, repealed those sections of the Code deriving from the implementation of the previous Data Protection Directive (Directive 95/46/EC) and directly conflicting with the GDPR. Furthermore, the Decree introduced new provisions to apply a number of rules introduced by the GDPR.[2]

On 10 July 2021, the Garante announced that it had released guidelines on cookies and similar tracking technologies. The guidelines make distinctions between active and passive identifiers, where active consist of identifiers such as cookies and passive consist of identifiers such as fingerprinting.[3]

Data Protection Authority Focus

The Garante has imposed numerous fines on the concerns and complaints regarding unsolicited telemarketing calls, transparency, lack of security measures, not handling data subject requests, etc. In October 2022, a company was fined €10,000 for failing to properly handle a data subject request. The data subject's request for deletion was not handled, even after a warning letter was sent to the company.[4] Another company was fined €15,000 for lack of appropriate security measures.[5] Recently (2022) a famous telephone company was also fined € 500,000, following a complaint filed by an elderly woman who witnessed the transfer, against her will, of her telephone service from another operator[6].

On an international cooperation front, the Garante has recently signed a cooperation agreement on data protection with Georgian Personal Data Protection Service (PDPS). The agreement aims to spread awareness pertaining to data privacy, to share information and best practices, and to allow the exchange of experts between the two authorities.[7]In September 2022, the Garante issued a negative opinion on the draft decree regarding creation of a database called Ecosistema Dati Sanitari (EDS). In August 2022, it had similarly issued an opinion on a decree implementing a national level Electronic Health Record. The Garante outlined that the draft decrees were in violation of the regulations regarding protection of personal data.[8]

1 https://www.dataguidance.com/notes/italy-data-protection-overview
2 https://www.dataguidance.com/notes/italy-data-protection-overview
3 https://www.dataguidance.com/opinion/italy-garantes-finalised-guidelines-cookies-and
4 https://www.dataguidance.com/news/italy-garante-fines-bper-banca-10000-failing-satisfy
5 https://www.dataguidance.com/news/italy-garante-fines-servizio-idrico-integrato-15000-0
6 https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9826417
7 https://www.dataguidance.com/news/international-garante-signs-cooperation-agreement-data
8 https://www.dataguidance.com/news/italy-garante-issues-negative-opinion-establishment-e

ITALY (CONTINUED)

Law: Personal Data Protection Code, Containing Provisions to Adapt the National Legislation to General Data Protection Regulation (Regulation (EU) 2016/679) ('the Code'), Legislative decree n. 196/03 integrating GDPR provisions, GDPR

Regulator: Italian Data Protection Authority ('Garante')

EU Adequacy Decision: n/a

Stefano Minini (partner)
stefano.minini@bdo.it
+393346829871

The Garante, in an emergency measure adopted on July 7 (2022), warned a popular social networking platform that it is unlawful to use personal data stored in users' devices to profile them and send them personalised advertising in the absence of explicit consent. The Garante had initiated an investigation after the company informed its users that, as of July 13, people over the age of 18 would be reached by "personalised" advertising, i.e., based on profiling of their browsing behaviour on the aforementioned social network[9].

The Garante announced on June 23, 2022, that it published Order No. 224, issued on June 9, 2022, in which it imposed an administrative fine on a society following a complaint filed by a person. The company in question among other violations, was guilty of transferring the complainant's personal data to Google LLC, based in the United States, using Google Analytics, in the absence of an adequate level of safeguards. (provided by Chapter V of the GDPR). In imposing the sanction, the Garante specified that "The website using the Google Analytics (GA) service, without the safeguards provided by the EU Regulation, violates data protection law because it transfers user data to the United States, a country without an adequate level of protection. [10]"

The Garante, in a resolution Oct. 6, 2022, published in the Official Gazette, accredited the new Monitoring Body to protect consumers from problems with credit information systems and gave final approval to the code of conduct for operators in the sector[11].

On October 20, 2022, the Data Protection Authority sanctioned a well-known perfume chain to the payment of € 1,400,000 for violating several provisions of the personal data protection regulations. Specifically, during the inspection, carried out with the Special Unit for Privacy Protection and Technological Fraud of the Guardia di Finanza, it was found that the perfumery chain kept the data of about three million three hundred thousand customers of the previous three companies incorporated without requesting their consent[12].

The Garante has expressed a positive opinion about the request by the Ministry of Economy and Finance to novate Legislative Decree No. 231 of November 21, 2007, on "prevention and use of the financial system for the purpose of money laundering and financing of terrorism." The main object of the amendment is the establishment of a centralised computer database for the aforementioned prevention purposes. In particular, the decree introduces a new provision (Art. 34-bis), entitled "Computer databases at self-regulatory bodies," which, in providing for the establishment of specific archives, stipulates that they will be fed by the acts, useful for the purposes of money laundering risk assessments, sent by professionals, such as accountants, lawyers, notaries, labour consultants, in the exercise of their activities[13].

9 https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9788429
10 https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9782874
11 https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9818201
12 https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9825667
13 https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9799609

JAPAN

Law: Act on the Protection of Personal Information (Act No. 57 of 2003 as amended in 2015) (APPI)

Regulator: Personal Information Protection Commission (PPC)

EU Adequacy Decision: yes

Gary Loh
garyloh@bdo.com.sg

Notable Changes

Japan's Data Privacy framework is governed by the Act on the Protection of Personal Information (Act No. 57 of 2003 as amended in 2015) (APPI), while its data protection authority is called the Personal Information Protection Commission (PPC). Japan is also a part of the Asia-Pacific Economic Cooperation Cross Border Privacy Rules system (APEC CBPR), which has been recognised by the European Commission as having an adequate level of personal data protection.

In April 2022, the PPC released guidance and a case study on the processing of anonymous and pseudo-anonymous information. The guidance clarifies these concepts and outlines restrictions on the handling of the same.[1]

The PPC also updated the procedures for personal information protection organisations regarding notifying the change of important matters without delay (i.e., when an authorised personal information protection organisation creates a personal information guideline, the PPC must be immediately notified[2]).

Data Protection Authority Focus

A toolkit was released by the PPC for data mapping on 13 October 2022. The toolkit was provided by the PPC to clarify what data mapping encompasses and the importance of following the compliance programme. Furthermore, it explains the procedure to be used to carry out data mapping.[3]

A 2021 annual report published by PPC indicated that most data breaches occurred due to the conveyance of incorrect documents and emails, as well as the loss of documents and electronic media.[4] The Ministry of Internal Affairs and Communications (MIC) has published the ICT cybersecurity measures for 2022. The measures provide guidance for enhancing cybersecurity in areas such as IoT, smart cities, and cloud services.[5]

Japan is also focusing on international cooperation for data privacy. Japan recently signed a memorandum of cooperation with Thailand in the field of information and communication digital technology.[6] A joint statement with Singapore has also been released to extend and strengthen cooperation in relation to digital economies, artificial intelligence governance, and cybersecurity.[7]

1 https://www.dataguidance.com/news/japan-ppc-updates-guidance-and-case-studies-anonymous
2 https://www.dataguidance.com/news/japan-ppc-updates-procedures-authorised-personal
3 https://www.dataguidance.com/news/japan-ppc-releases-data-mapping-tool-kit
4 https://www.dataguidance.com/news/japan-ppc-releases-2021-annual-report
5 https://www.dataguidance.com/news/japan-mic-publishes-ict-cybersecurity-measures-2022
6 https://www.dataguidance.com/news/international-japan-and-thailand-sign-moc-ict
7 https://www.dataguidance.com/news/international-singapore-and-japan-further-cooperate

JERSEY

Law: Data Protection (Jersey) Law 2018 ('DPLJ'), Data Protection Authority (Jersey) Law 2018 ('the Authority Law')

Regulator: Jersey Office of the Information Commissioner (JOIC)

EU Adequacy Decision: yes

Damon Greber
dgreber@bdo.je
+44 (0) 1534 844 451

Notable Changes

The Jersey Office of the Information Commissioner (JOIC) has published multiple blog posts that serve as guidelines. A September 2022 post highlighted the importance of transparency at the time of data collection from data subjects, stressing the need to explain what information is being collected and the purpose of such collection.[1] The JOIC also published a blog highlighting recommendations concerning basic data protection principles, training and awareness, data management and data storage, and access for new small-business owners.[2]

The JOIC also highlighted data security of the blog posts, which included recommendations to reduce security risks such as introducing multifactor authentication.[3]

Data Protection Authority Focus

The JOIC published its statistics report for 2021, which listed the number of complaints and self-reported data breaches. The report showed a culture of high-level of reporting and compliance within the finance and professional services sectors, but also that a high percent of complaints and self-reported breaches were from the public authorities.[4]

The Jersey Data Protection Authority has also issued a reprimand to the Children's Services of the Government of Jersey in October 2021 for contravening the Data Protection Law, as it had disclosed the complainant's extremely sensitive information to a previously unaware family member.[5] A reprimand was also issued to the Planning and Building Control Department, as it was found to be responsible for two data breaches.[6]

International Cooperation is also in focus, with the JOIC and the Abu Dhabi Global Market (ADGM) signing a memorandum of understanding (MoU) that aims to facilitate the cooperation between both jurisdictions in the matter of data privacy and protection.[7]

1 https://www.dataguidance.com/news/jersey-joic-issues-blog-post-transparency-requirements
2 https://www.dataguidance.com/news/jersey-joic-publishes-blog-post-data-protection
3 https://www.dataguidance.com/news/jersey-joic-publishes-blog-post-addressing-importance
4 https://www.dataguidance.com/news/jersey-joic-publishes-2021-activity-report
5 https://www.dataguidance.com/news/jersey-jdpa-issues-childrens-services-government-jersey
6 https://www.dataguidance.com/news/jersey-jdpa-issues-planning-and-building-control
7 https://www.dataguidance.com/news/international-adgm-and-joic-sign-mou-data-protection

LATVIA

Law: Personal Data Processing Law of 21 June 2018 ('the Law'), GDPR

Regulator: Data State Inspectorate ('DVI')

EU Adequacy Decision: n/a

Lasma Kramina
lasma.kramina@bdo.lv
+371 6722 2237

Notable Changes

The Data State Inspectorate (DVI) has published guidance covering a range of topics, including the role of the data protection officer, in which it highlighted the main functions of the DPO;[1] guidance on the process to exercise the right to deletion;[2] and guidance regarding anonymised and pseudo-anonymised data.[3] A cookie guideline was also released that describes cookie consent, transparency, obligations pertaining to usage of cookies, and different types of cookies.[4]

A data protection impact assessment guide was also published by the DVI. The guide explains the processes involved in a data protection impact assessment and the need for conducting one.[5]

Data Protection Authority Focus

The DVI has stated in its enforcement and breach statistics that it has released almost 1,000 complaints from citizens of the country, 88 notifications from data controllers, and 19 notifications from other persons, such as public institutions, organisations, and associations, regarding actual or possible data protection violations. The DVI carried out 1,080 personal data processing inspections in total.[6]

1 https://www.dataguidance.com/news/latvia-dvi-publishes-guidance-dpo-role
2 https://www.dataguidance.com/news/latvia-dvi-publishes-guide-right-deletion
3 https://www.dataguidance.com/news/latvia-dvi-publishes-guide-pseudonymised-and-anonymised
4 https://www.dvi.gov.lv/lv/media/1517/download
5 https://www.dataguidance.com/news/latvia-dvi-publishes-dpia-guide
6 https://www.dataguidance.com/news/latvia-dvi-announces-2021-enforcement-and-breach

MALTA

Law: Data Protection Act (CAP 586) ('the Act')

Regulator: Office of the Information and Data Protection Commissioner ('IDPC')

EU Adequacy Decision: n/a

Ivan Spiteri
ivan.spiteri@bdo.com.mt
+356 23434201

Notable Changes

No new legislative changes.

Data Protection Authority Focus

In 2022 a survey was conducted by the Information and Data Protection Commissioner (IDPC) among 259 SMEs (small and medium size entities) found that knowledge about GDPR-related issues was found to be medium to high among most SMEs. The survey, conducted together with the Malta Chamber of SMEs and the Malta Employers' Association, was commissioned by the IDPC as part of a wider project to increase GDPR awareness among the public and the business community, particularly SMEs. [1]

The IDPC issued two fines in 2022. A fine of €65,000 to a Controller who infringed principles of security regarding personal and special categories of data of many data subjects and a fine €2,500 to a Controller who has unlawfully disclosed the complainant's personal data. [2]

The IDPC also announced in October 2022 that it has signed sign memorandum of understanding with the Gibraltar Regulatory Authority the aim of enhancing bilateral cooperation. The GRA and the IDPC, which are both members of the BIIDPA (British, Irish and islands data protection authorities) network, enjoy a longstanding relationship which the recently signed memorandum will strengthen even further, in the interest of businesses and individuals. [3] Similarly, in 2022, the IDPC and Albanian Office of the Information and Data Protection Commissioner (IDP) also signed a cooperation agreement to deepen knowledge and cooperation in personal data protection.

1 https://timesofmalta.com/articles/view/icon-completes-nationwide-gdpr-platform-smes.969977
2 https://idpc.org.mt/decisions/
3 https://idpc.org.mt/idpc-publications/idpc-and-gpa-gibraltar-mou/

MAURITIUS

Law: Data Protection Act 2017 ('the Data Protection Act')

Regulator: Data Protection Office ('the Office')

EU Adequacy Decision: no

Deepshi Hujoory
deepshi.hujoory@bdo.mu
+230 202 9562

Notable Changes

No new legislative changes.

Data Protection Authority Focus

In 2021, Mauritius signed the Administrative Arrangement for the transfer of personal data between European Economic Area (EEA) Authorities and non-EEA Authorities. This will help demonstrate Mauritius's commitment to adhere to international data protection standards.[1]

1 https://www.dataguidance.com/news/mauritius-fsc-publishes-communique-signing

MEXICO

Law: The Federal Law on the Protection of Personal Data held by Private Parties 2010 and Regulations to the Federal Law on the Protection of Personal Data Held by Private Parties 2011.[44]

Regulator: National Institute for Access to Information and Protection of Personal Data ('INAI')

EU Adequacy Decision: no

Ramses Inzunza
ramses.inzunza@bdomexico.com
+52 (55) 8503-4200

Notable Changes

The law that governs the data privacy and protection in Mexico is called Federal Law on Protection of Personal Data Held by Private Parties (FLPPDPP). It is supplemented by the regulations called Regulations to the Federal Law on Protection of Personal Data Held by Private Parties. They establish basic standards for the processing of personal data. Under the current legal framework, there are some key components missing, such as a lack of requirement to inform the authority of a data breach, but future amendments are in the works to make such requirements part of the legal framework.[1]

In April 2022, the INAI released a bulletin containing recommendations to protect the personal data of children who use toys that are connected to the internet.[2]

The INAI released Recommendations for the Processing of Personal Data derived from the use of AI in May 2022. The recommendations include topics such as AI and privacy by design, personal information protection in massive data analysis for AI, and protection of personal data in the technologies of virtual and augmented reality.[3]

Data Protection Authority Focus

The INAI has reported instances of privacy violations in a report published with statistics from 1 January 2022 to 30 June 2022. The report stated the INAI had issued fines of MXN 18 million (approx. €928,874) for privacy law violations. The INAI has also received 820 complaints for improper use of data in the private sector and 47 such complaints in the public sector.[4]

A summary of 2021 enforcement activity was also released on 9 January 2022. It showed fines of MXN 90 million (approx. €3,877,709) imposed on individuals who misused personal data. There were also a total of 1,930 complaints against individuals and legal entities within the private sector and 83 within the public sector received by the INAI.[5]

With the rise in cyber incidents, the Ministry of Security and Citizen Protection (SSPC) announced that it is in creating a National Registry for Cyber Incidents. The registry will allow the government to measure the occurrence and impact of internet crimes.[6]

1 https://www.dataguidance.com/jurisdiction/mexico
2 https://www.dataguidance.com/news/mexico-inai-issues-bulletin-toys-connected-internet
3 https://www.dataguidance.com/news/mexico-inai-publishes-recommendations-ai
4 https://www.dataguidance.com/news/mexico-inai-publishes-enforcement-statistics-first
5 https://www.dataguidance.com/news/mexico-inai-publishes-summary-2021-enforcement-activity
6 https://www.dataguidance.com/news/mexico-sspc-announces-creation-national-registry-cyber

THE NETHERLANDS

GDPR and Dutch Implementation Law ("UAVG")

Law: Act Implementing the GDPR, GDPR

Regulator: Dutch Data Protection Authority ('AP')

EU Adequacy Decision: n/a

Robert Van Vianen
robert.van.vianen@bdo.nl
+31 30 284 98 00

Notable Changes

There have not been significant changes in legislation (as the GDPR continues to apply), but new case law sheds more information on data subjects, such as processing for purposes of legitimate interests pursued by the controller.

In 2021, the AP received 24,866 data breach notifications. This is nearly a 4% increase from 2020.[1]

Data Protection Authority Focus

The AP has expressed its concerns about the continuous change of society due to digitisation and technological innovation, leading to more data which are also more diverse, specific, and personal.

DPG Media will receive an AVG fine of 525,000 euros for incorrectly asking for ID. Publisher DPG Media has been fined € 525,000 for GDPR because it asked customers for proof of identity if they wanted to access their data. DPG has thus 'raised unnecessary barriers to the implementation of GDPR rights'. The fine will be borne by DPG Media, the parent company of Tweakers and publisher of major newspapers and magazines such as de Volkskrant and Autoweek. The Dutch Data Protection Authority imposes a fine of €525,000 on the publisher for violating the General Data Protection Regulation. The violations took place at DPG Magazines, which was known as Sanoma Media until it was acquired by DPG in April 2020.

Customers who wanted to know from Sanoma and later DPG what data the publisher collected about them had to send their proof of identity digitally. Customers also had to do this if they wanted to cancel or change their subscription. DPG also did not point out to them the possibility of shielding their data

The AP has recommended amendments to a proposed act on the accountancy sector. It has highlighted how the proposed act does not provide adequate protection to the personal data of accountants.[2]

On 30 April 2021, the AP released different methods of anonymisation in the form of a guidance, to help organisations better handle the anonymisation,[3] which can be useful for protecting private and sensitive information.

Data controllers may face difficulties in complying with the GDPR requirements, so the AP released a tool to help with the process. The tool would provide tailored advice to organisations on how to comply with the GDPR.[4]

Amendments to the law regarding government personal data have been proposed, as the current draft law does not set proper limits, and there is a potential risk of data being shared without proper permission.5 In April 2022, the AP published its 2021 annual report. The report highlights number of opinions and advice issued by the body. It also notes that the AP has imposed 11 fines.[6]

1 https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/datalekkenrapportage_ap_2021.pdf
2 https://www.dataguidance.com/news/netherlands-ap-issues-advice-publishing-accountants
3 https://www.dataguidance.com/news/netherlands-ap-addresses-anonymisation-techniques
4 https://www.dataguidance.com/news/netherlands-ap-releases-interactive-gdpr-compliance
5 https://www.dataguidance.com/news/netherlands-ap-recommends-amendments-use-government
6 https://www.dataguidance.com/news/netherlands-ap-publishes-2021-annual-report

NIGERIA

Law: Nigerian Data Protection Regulation (NDPR)

Regulator: National Information Technology Development Agency ('NITDA')

EU Adequacy Decision: no

Ebenezer Olabis
eoolabisi@bdo-ng.com
+234 1 448 3051

Notable Changes

Nigeria currently has a variety of laws, regulations, and guidelines in place which together form one of the most comprehensive data protection regimes in Africa. Notable laws include the NDPR, the Freedom of Information Act, 2011, the National Health Act, 2014, and the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015. The most significant recent development has been the passing and entry into force of the NDPR, which was issued by NITDA and has the force of law. While the NDPR sets out data subject rights, prescribes the development of security measures to protect data, and strengthens the supervisory powers of NITDA, it does not include explicit requirements for the processing of sensitive data and is silent on data breach notifications. The NDPR applies to natural persons residing in Nigeria as well as Nigerian citizens abroad. Following the issuance of the NDPR, NITDA published its Draft Data Protection Implementation Framework in July 2019. In November 2020, a second draft of the Implementation Framework was released. Although not yet enforceable, this framework would provide important supplementary information for interpreting the NDPR and would establish requirements for data breach notifications.[1]

On 14 January 2022, NITDA announced that it had launched a visitors book designed to comply with the 'NDPR. In particular, NITDA explained that the booklet's pages are duplicates and work by making personal details on the visitor's book invisible on the first page, while capturing the data on the duplicate page.

Further to the launch of the booklet, NITDA highlighted that the NDPR applies to all acts of personal data collection and processing, no matter how and where it takes place, e.g., including visitor data and employee personal data, and sought to debunk the common misconception that the NDPR only applies in the online environment.[2]

On 22 February 2022, Olumide Babalola, Managing Partner at Olumide Babalola LP, said that the Nigeria Data Protection Bureau (NDPB) had been established by the federal government, following a request made by the Minister of Communications and Digital Economy, Professor Isa Pantami.[3]

Data Protection Authority Focus

On 4 October 2022, the NDPB released the draft Data Protection Bill, 2022. The bill outlines principles and lawful bases for the processing of personal information, including the conducting of Data Protection Impact Assessments (DPIAs); the appointment of a data protection officer (DPO); and data subject rights, including the rights to object, withdraw consent, data portability, and not to be subject to a decision based solely on automated processing of personal data.[4]

1 https://www.dataguidance.com/jurisdiction/nigeria
2 https://www.dataguidance.com/news/nigeria-nitda-reveals-ndpr-compliant-visitors-booklet
3 https://www.dataguidance.com/news/nigeria-nigeria-data-protection-bureau-established
4 https://www.dataguidance.com/news/nigeria-ndpb-releases-draft-data-protection-bill

NORWAY

Law: Law on the Processing of Personal Data (Personal Data Act) of 15 June 2018 and GDPR

Regulator: Data Protection Authority (Datatilsynet)

EU Adequacy Decision: n/a

Henrik Dagestad
henrik.dagestad@bdo.no
+47 901 77 117

Notable Changes

Datatilsynet has been active in enforcement and in publishing guidelines on data privacy issues, such as code of conduct, direct marketing, software development, and privacy by design.[1]

In June 2022, the Datatilsynet provided advice for safeguarding personal data protection within organizations. The advice provides for how personal data should be processed and the aspects organisations should keep in mind when engaging in a processing activity.[2]

A new Credit Information Act entered into force on 1 July 2022. Under the act, it is no longer necessary to apply for permits from Datatilsynet to conduct credit information activities. Compliance with the regulations will be checked by Datatilsynet through inspections instead of a preapproval process through license application.[3]

Data Protection Authority Focus

Datatilsynet has conducted planned supervision with several companies and organizations, including a large telecom company, a large electronics retailer, and the Norwegian Correctional Service.

Datatilsynet recently conducted a survey on monitoring and control of employees' digital activities.

On subsequent publication of the result, it was found out that most employees do not have a clear overview of the information collected by their employers and that employers collect large amounts of information about employees' digital rights. [4]

A report on the status of privacy by the Privacy Commission showed that digitisation is coming at the expense of privacy. The commission came up with proposals to improve the situation and strengthen privacy in Norway. Datatilsynet has acknowledged the report and plans to analyse and provide concrete feedback on it.[5]

Datatilsynet has made (informal) objections towards the proposal of a new Norwegian intelligence law, that will allow the Norwegian Police Security Service to increase their surveillance of statements made online.

Datatilsynet has made several reports from projects where Datatilsynet and companies/organisations have explored the possibility to use artificial intelligence in line with the requirements in GDPR. Several reports are available in English.[6]

Datatilsynet has also issued fines to numerous companies and organisations for violations of the personal data protection law. The Norwegian Labour and Welfare Administration and a private company were both fined 5 MNOK (approx. € 475 144) for violations of GDPR in two separate cases.[7]

1 https://www.dataguidance.com/jurisdiction/norway
2 https://www.dataguidance.com/news/norway-datatilsynet-provides-nine-rules-safeguarding
3 https://www.dataguidance.com/news/norway-datatilsynet-announces-new-credit-information
4 https://www.dataguidance.com/news/norway-datatilsynet-publishes-report-monitoring-and
5 https://www.dataguidance.com/news/norway-privacy-commission-issues-report-status-privacy
6 https://www.datatilsynet.no/regelverk-og-verktoy/sandkasse-for-kunstig-intelligens/ferdige-prosjekter-og-rapporter/
7 https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2022/endelig-vedtak-om-overtredelsesgebyr-til-nav/ https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2022/gebyr-til-trumf/

PANAMA

Law: Law No. 81 on Personal Data Protection 2019

Regulator: National Authority for Transparency and Access to Information ('ANTAI')

EU Adequacy Decision: no

Simone Mitil
smitil@bdo.com.pa
+507 6070 7907

Notable Changes

The Law No. 81 on Personal Data Protection 2019 along with the Executive Decree No. 285 of 18 May 2021, which regulates the Law No. 18, together govern the privacy landscape in Panama. According to the law, the rights and obligations pertaining to the protection of personal data apply to natural and legal persons, as well as for-profit and non-profit organisations. The law also has an extra-territorial effect, as it also targets foreign companies operating in Panama. The law entered into force on 29 March 2021.[1]

The law contains provisions for governing the data subject rights, namely the right to access, rectification, cancellation, opposition, and portability.[2] The Executive Decree contains provisions against the automated processing of data in case it creates a negative legal effect and prejudices the rights of the data subject. Data subjects are to be provided with information regarding automated processing, and they also have a right to object based solely on automated processing.[3]

Data Protection Authority Focus

The ANTAI is responsible for ensuring that the protocols for data management and transfer are followed by data managers. It also determines which data is noncompliant and applies punishments as a result of noncompliance. Based on the seriousness of the offence, the ANTAI sets the amount of fine. ANTAI provides guidance and clarifications for further issues that may arise in relation to data processing or transfer.[4]

1 https://www.dataguidance.com/news/panama-data-protection-law-enters-effect
2 https://www.dlapiperdataprotection.com/index.html?t=law&c=PA
3 https://www.dataguidance.com/notes/panama-data-protection-overview#:~:text=On%2028%20May%202021%2C%20Panama,principle%20of%20personal%20data%20protection.
4 https://www.dataguidance.com/notes/panama-data-protection-overview#:~:text=On%2028%20May%202021%2C%20Panama,principle%20of%20personal%20data%20protection.

PHILIPPINES

Law: The Data Privacy Act of 2012

Regulator: National Privacy Commission (NPC)

EU Adequacy Decision: no

Ricky Cheng
Rickycheng@bdo.com.hk
+852 2218 8266

Notable Changes

On 1 December 2021, the Senate of the Philippines filed Senate Bill No. 2460, "An Act Providing for an Opt-In Mechanism for Telephone and Mobile Subscribers, protecting such subscribers from electronic threats through the misuse of digital technology, and providing penalties for violations thereof" (SB 2460).[1]

The NPC is conducting on-site compliance check visits to personal information controllers (PICs) and personal information processors (PIPs) to verify compliance documents submitted and to determine whether there are substantial findings of noncompliance with the Data Privacy Act of 2012 and NPC's issuances. Upon the conclusion of the on-site visits, the NPC personnel present their findings and determine whether the PIC or PIP has deficiencies that need to be addressed[2].

On 20 April 2022, the NPC held its virtual launching of the Data Breach Notification Management System (DBNMS), an interface that facilitates tracking and submission of personal data breach notifications and annual security incident reports. The DBNMS is a standardised, automated, system, making it easier for PICs to submit personal data breach notifications, as required by NPC Circular No. 16-03, and annual security incident reports. With the launch of the DBNMS, the NPC will no longer accept breach notification and annual security incident report submissions except through the DBMNS online platform.

Thus, submissions through email, personal filing, ordinary mail, licensed courier service, and any other mode of physical submission shall not be considered as valid.[3]

On 4 March 2022, the NPC announced Joint Administrative Order No. 2022-01, "Guidelines for Online Businesses Reiterating the Laws and Regulations Applicable to Online Businesses and Consumers," (the JAO) to provide guidance so that e-commerce businesses inform consumers of their rights and the mechanisms for redress.[4]

Data Protection Authority Focus

On 28 February 2022, the NPC issued NPC Advisory Opinion No. 2022-06, "Request for Customer's Personal Data and Transaction History with a Private Courier." The Advisory Opinion outlines the request for personal data by the Philippines Drug Enforcement Agency (DPEA).

On 4 March 2022, the NPC issued guidelines regarding the certification of registration for Data Protection Officers (DPOs). The NPC stated that the validity of all existing certificates of registration for DPOs issued in 2021 have been extended until 8 March 2023, and for those issued before 2021, PICs and PIPs have been directed to renew DPO registration with the NPC.[5]

1 https://www.dataguidance.com/news/philippines-senate-files-anti-spam-act
2 https://www.privacy.gov.ph/2022/05/npc-conducts-on-site-compliance-checks-to-determine-level-of-compliance-with-the-dpa/
3 https://www.privacy.gov.ph/2022/04/npc-launches-user-friendly-online-system-for-faster-and-easier-data-breach-notification-management-and-reporting/
4 https://www.dataguidance.com/news/philippines-npc-announces-joint-administrative-order
5 https://www.dataguidance.com/news/philippines-npc-issues-guidelines-dpo-registration

PHILIPPINES (CONTINUED)

Law: The Data Privacy Act of 2012

Regulator: National Privacy Commission (NPC)

EU Adequacy Decision: no

Ricky Cheng
Rickycheng@bdo.com.hk
+852 2218 8266

On 2 March 2022, the NPC issued NPC Advisory Opinion No. 2022-08, "Obtaining Employment Record or Certification from the Social Security System." The NPC said that in requesting records or proof of employment, any record may contain personal information and sensitive personal information of the employee concerned. It added that while legal basis for such a request exists under Sections 12 and 13 of Republic Act No. 10173, the principle of proportionality must be adhered to.[6]

On 24 November 2021, the NPC issued NPC Advisory Opinion No. 2021-041, "Posting of Names of Passport Applicants on the Website of the Office of Consular Affairs of the Department of Foreign Affairs ('Advisory Opinion')." The NPC stated that Republic Act No. 10173 (the Act) applies to all types of personal information and any natural and judicial person involved in personal information processing. However, the NPC noted that the processing of personal information based on legitimate interest, provided under Section 12(f) of the Act, does not apply to processing carried out by government agencies.[7]

On 12 August 2022, the NPC issued the Circular No. 2022-01 on guidelines on administrative fines for data privacy infractions committed by PICs and PIPs. The NPC noted that the circular is essential for the public interest to impose administrative fines that are proportionate and dissuasive of data privacy infractions.[8]

On 5 July 2022, the NPC published Advisory Opinion No. 2022-016, "Request for Personal Information of overseas Filipino workers (OFWs) Deployed in the Middle East and Other Muslim Countries." The NPC stated that the advisory opinion concerns the request for sensitive religious personal data of OFWs by the National Commission on Muslim Filipinos (NCMF) from the Department of Labour and Employment (DOLE) and other government departments. However, the NPC clarified that while the processing of the personal data of Muslim OFWs may fall within the mandate of the NCMF, this would not apply to the personal data held by non-Muslim OFWs, and there may be a need to gain the consent of non-Muslim OFWs prior to the collection of their personal data.[9]

6 https://www.dataguidance.com/news/philippines-npc-issues-advisory-opinion-obtaining
7 https://www.dataguidance.com/news/philippines-npc-issues-advisory-opinion-legitimate
8 https://www.dataguidance.com/news/philippines-npc-issues-circular-administrative-fines
9 https://www.dataguidance.com/news/philippines-npc-issues-advisory-opinion-processing

POLAND

Law: Act of 10 May 2018 on the Protection of Personal Data ('the Act'), GDPR

Regulator: Polish Data Protection Authority ('UODO')

EU Adequacy Decision: n/a

Tymoteusz Murzyn
tymoteusz.murzyn@bdolegal.pl

Notable Changes

In 2022, the draft act on combating abuses in electronic communication was released by the Minister of Digitisation. The draft act obliges organisations working in telecommunications to put technical and organisational measures in place to counteract potential abuses that may arise.

Also in 2022, an updated whistleblowing bill was released by the Ministry of Family and Social Policy and introduces provisions for data retention in relation to the personal data processed regarding the acceptance of notification.[1]

Data Protection Authority Focus

The UODO released a report on secure personal data processing, stating that most people do not know who should deal with the negative consequences of a data breach.[2]

Guidelines regarding the circumstances surrounding financial institutions making copies of identity documents were published, stating that copies may only be made when required to apply security measures for anti-money laundering and counter terrorist financing purposes.[3]

The UODO issued a fine of PLN 60,000 (approx. €12,500) to the surveyor general of Poland[4] and a fine of PLN 10,000 (approx. €2,120) the Medical University of Warsaw[5] for breach of notification obligations under GDPR.

A memorandum of understanding regarding cyber protection was signed between Poland and Ukraine. The memorandum aims to improve the flow of information regarding cyber incidents faster and more efficiently.[6]

A data protection agreement was also signed between the UODO and National Centre for the Protection of Personal Data (NCPDP) of Moldova. The agreement aims to develop cooperative relations in the field of personal data protection.[7]

1 https://www.dataguidance.com/news/poland-ministry-family-and-social-policy-publishes-0
2 https://www.dataguidance.com/news/poland-uodo-releases-report-secure-personal-data
3 https://www.dataguidance.com/news/poland-uodo-opines-when-financial-institutions-can-make
4 https://www.dataguidance.com/news/poland-uodo-fines-surveyor-general-pln-60000-failure
5 https://www.dataguidance.com/news/poland-uodo-fines-medical-university-warsaw-pln-10000
6 https://www.dataguidance.com/news/international-ukraine-and-poland-sign-mou-cyber
7 https://www.dataguidance.com/news/international-moldova-and-poland-sign-data-protection

PORTUGAL

Law: No. 58/2019, which Ensures the Implementation in the National Legal Order of the GDPR on the Protection of Individuals with Regards the Processing of Personal Data and the Free Movement of Such Data ('Law No. 58/2019'), GDPR

Regulator: Portuguese Data Protection Authority ('CNPD')

EU Adequacy Decision: n/a

Luís Crispim
luis.crispim@bdo.pt
+351937990341

Notable Changes

In June 2022, the CNPD published the Whistleblowing Law, which transposes the Directive on the Protection of Persons who Report Breaches of Union Law (Directive (EU) 2019/1937) into a national law of Portugal. The act has not yet come into force.[1]

Several EU Directives were transposed by the Electronic Communications Law that was published by the National Regulatory Authority for Communications. The Electronic Communications Law contains provisions primarily governing the organisation of the electronic communications market and the provision of services and resources.[2]

An opinion on the draft law to ensure consumer rights in the purchase of goods, content, and services has also been released by the CNDP. CNDP recommended changes in the draft law that would guarantee data subjects' rights and ensure that data subjects have sufficient redressal mechanisms.[3]

Data Protection Authority Focus

The CNPD issued new direct marketing guidance clarifying the obligations on companies for such communications.[4]

The CNPD announced incoming guidelines on the use of cookies and released a note that would address concerns related to the use of cookies for private companies.[5]

The CNPD ordered telecom providers to delete data stored under retention law. The law had previously allowed providers to store a wide range of data for the purpose of investigation, detection, and prosecution of serious crime.[6]

1 https://www.dataguidance.com/news/portugal-whistleblowing-law-comes-force
2 https://www.dataguidance.com/news/portugal-anacom-announces-publication-new-electronic
3 https://www.dataguidance.com/news/portugal-cnpd-issues-opinion-draft-consumer-rights-law
4 https://www.dataguidance.com/news/portugal-cnpd-issues-new-direct-marketing-guidance-and
5 https://www.dataguidance.com/news/portugal-cnpd-issues-note-use-cookies-announcing
6 https://www.dataguidance.com/news/portugal-cnpd-orders-telecoms-providers-delete-data

ROMANIA

Law: Law No. 190/2018 Implementing the General Data Protection Regulation (Regulation (EU) 2016/679) ('the Law'), GDPR

Regulator: National Supervisory Authority for Personal Data Processing ('ANSPDCP')

EU Adequacy Decision: n/a

Raluca Andrei
raluca.andrei@tudor-andrei.ro
+40755633856

Notable Changes

The National Directorate of Cyber Security (DNSC) and ISACA Romania have published a cybersecurity guide for operators of essential services. The guide is meant to be an educational resource for organisations in the field of cybersecurity governance within organisations.[1]

Data Protection Authority Focus

The National Supervisory Authority for Personal Data Processing issued multiple fines for instances of insufficient security measures that led to data breaches,[2] failure to exercise the right to object,[3] and other issues of noncompliance.

The Romanian National Authority for Management and Regulation in Communications (ANCOM) signed a memorandum of understanding with the U.S. Federal Communications Commission (FCC) agreeing to collaborate on issues such as supply chain security, cybersecurity, and equipment authorisation procedures.[4]

A fine of €10,000 was imposed on a company for violation of Article 32 of the GDPR for not implementing appropriate technical and organisational measures, as well as a warning for violating Article 39 of the GDPR.[5]

Another company was fined €8,000 for violating Article 32 of the GDPR.[6]

1 https://www.dataguidance.com/news/romania-dnsc-and-isaca-romania-publish-cybersecurity
2 https://www.dataguidance.com/news/romania-anspdcp-fines-curtea-veche-publishing-5000; https://www.dataguidance.com/news/romania-anspdcp-fines-realmedia-network-8000-violating;
3 https://www.dataguidance.com/news/romania-anspdcp-fines-sephora-cosmetics-romania-2000
4 https://www.dataguidance.com/news/international-fcc-signs-mou-ancom-and-anatel
5 https://www.dataguidance.com/news/romania-anspdcp-fines-enel-energie-muntenia-10000
6 https://www.dataguidance.com/news/romania-anspdcp-fines-realmedia-network-8000-violating

SINGAPORE

Law: Personal Data Privacy Act 2012 (No. 26 of 2012) ('PDPA')

Regulator: Personal Data Protection Commission ('PDPC')

EU Adequacy Decision: no

Gary Loh
garyloh@bdo.com.sg

Notable Changes

The Singapore Government launched the Whole-Of-Government (WOG) Data Loss Protection (DLP) Suite in May 2022. The WOG DLP Suite works to prevent the accidental loss of sensitive data.

Amendments to the PDPA entered into force on 1 February 2021, including mandatory data breach notification requirements, amendments to the consent obligation, penalties for egregious mishandling of personal data, prohibitions relating to the use of dictionary attacks and address-harvesting software, and the PDPC's power to accept voluntary undertakings as part of its enforcement regime.[1]

In an effort to capitalize on the surging digital wave that occurred during the COVID-19 pandemic, the Singapore Parliament desires the Committee of Supply proposed a review of the Cybersecurity Act 2018 (No. 9 of 2018) (the Cybersecurity Act), with the intention of modernising it to consider recent developments in an ever-changing and complex world of cyber threats. The Cybersecurity Act, passed in March 2018, was originally established with the central aim of launching a legal basis for Singapore to supervise and sustain its national cybersecurity across numerous key sectors. At the moment, an evaluation of the legislation is being carried out to empower Singapore and various shareholders to better avert, achieve, and respond to cybersecurity threats and occurrences. The assessment of the law is poised to be accomplished by 2023, following discussions with industry and the public.

This analysis is particularly appropriate given the frequency of cyberattacks in the aftermath of the COVID-19 pandemic, which is likely to increase as the trend of digitalisation gains traction.[2]

Data Protection Authority Focus

The PDPA provides personal data protection requirements and contains provisions on data subject rights, the appointment of a data protection officer, and obligations for organisations and data intermediaries.

Organisations are required to notify both the PDPC and the affected individuals as soon as possible upon discovering a data breach. Companies with an annual turnover in Singapore exceeding S$10 million can now be fined up to 10% of this turnover.

The PDPA has issued several fines to companies for data breaches and noncompliance. Most recently, the PDPA imposed a fine of S$60,000 (approx. €42,660) on MyRepublic Limited for a violation of the Personal Data Protection Act 2012 (No. 26 of 2012) (PDPA), following a security incident.[3]

1 https://www.dataguidance.com/jurisdiction/singapore
2 https://www.dataguidance.com/opinion/singapore-plans-secure-singapores-digital-future
3 https://www.dataguidance.com/news/singapore-pdpc-fines-myrepublic-sgd-60000-data-security

SLOVAKIA

Law: Act No. 18/2018 Coll. on Protection of Personal Data and on Amendments to certain Acts ('the Act'), GDPR

Regulator: Office for Personal Data Protection of the Slovak Republic ('ÚOOÚ')

EU Adequacy Decision: n/a

Marek Priesol
priesol@bdoslovakia.com

Notable Changes

No significant changes.

Data Protection Authority Focus

On 11 July 2022, the ÚOOÚ published its 2021 report on the state of personal data protection, stating that from 1 January to 31 December 2021, 61 inspections were completed on the processing of personal data, 19 of which were initiated in 2021 and 42 in the previous period. The most frequent violation noted was around the legal foundation of processing, contradictory to the principle of integrity and confidentiality, which was connected to the failure to take appropriate security measures by processors.

The first coordinated enforcement action under the backing of the European Data Protection Board (EDPB) has begun in the Slovak Republic. The ÚOOÚ, together with 21 other administrative authorities in the European Economic Area (EEA), will be involved in the joint mapping of cloud-based services use by the public sector. This action is the effect of the EDPB's decision in October 2020 to establish a Coordinated Enforcement Framework (CEF), which seeks to modernise enforcement and cooperation among administrative authorities.

SOUTH AFRICA

Law: Protection of Personal Information Act, 2013 (Act 4 of 2013) ('POPIA'), Commencement of Section 1, Part A of Chapter 5 and Sections 112 and 113 of POPIA (April 2014), and Regulations Relating to the Protection of Personal Information (2018) ('the Regulations')

Regulator: The Information Regulator ('the Regulator')

EU Adequacy Decision: no

Carl Bosma
cbosma@bdo.co.za

Notable Changes

In accordance with POPIA, South Africa appointed an enforcement committee for the first time. The Regulator will now be able to enforce its powers and provide an effective remedy to complaints it receives.[1]

On 28 July 2022, the Regulator announced that it had established an enforcement committee in agreement with POPIA, which will be managed by Advocate Helen Fourie Senior Counsel. The Regulator stated that the Committee comprises 14 independent experts from diverse professional backgrounds, including data security, accounting, forensics, and criminal investigations.

Furthermore, the Regulator stated that pursuant to POPIA, the Committee must study all matters referred to it by the Regulator regarding a complaint, an inquiry of a complaint, a discovery in respect of a complaint or other matter, or a recommendation in respect of the proposed action to be taken by the Regulator, and complaints regarding the Promotion of Access to Information Act (PAIA). The Regulator noted that the committee is mandated to make findings in matters referred to it and make recommendations to the Regulator in relation to the provisions of POPIA, an information officer, or head of a private body.

Data Protection Authority Focus

The Regulator met with Transunion officials after a data breach that exposed the personal information of an undisclosed number of data subjects. POPIA requires all private or public bodies that have experienced a security breach to inform the Regulator and the affected parties following such an event. The Regulator required Transunion to submit specific details of the incident, procedures taken that will prevent a future security breach, and risk assessments that Transunion will conduct to strengthen security.[2]

1 https://www.dataguidance.com/news/south-africa-information-regulator%C2%A0establishes
2 dataguidance.com/news/south-africa-regulator-dissatisfied-trans-union

SOUTH KOREA

Law: Personal Information Protection Act (PIPA);
Related Laws: The Use and Protection of Credit Information Act 2009 and The Act on Promotion of Information and Communications Network Utilization and Information Protection 2001.

Regulator: Personal Information Protection Commission ('PIPC');

EU Adequacy Decision: yes

Mark Antalik
mantalik@bdo.com
+1 617-378-3653

Notable Changes

The PIPC has introduced a statement regarding combination and pseudo-anonymisation of personal information relating to driving, behaviour, location, and routes. The individual data held by local governments and the private sector may be used for the analysis and prediction of optimal location for electric vehicle charging facilities through the combination of pseudonymous information.[1]

In March 2022, the PIPC released guidelines stating that organisations should ensure consent is provided and that data subjects should not be deprived of products and services in case they refuse to provide consent to the processing of their data. The guidelines also address privacy notices, stating that privacy notices should clearly explain the types of processing activities involved.[2]

Data Protection Authority Focus

Google and Meta were fined KRW 69.2 billion (approx. €50 million) and KRW 30.8 billion (approx. €22 million), respectively, for violations of PIPA. Both Google and Meta had failed to properly inform or verify consent from data subjects when analysing their behaviour data.[3] The PIPC has also fined numerous other companies for PIPA violations, showing its proactive approach.[4]

South Korea is increasing international cooperation by signing a memorandum of understanding with the U.K. This MoU will seek to enhance cooperation and sharing of best data privacy practices.[5] A data adequacy agreement was also reached between South Korea and the U.K. for cross-border data transfer. This would allow U.K. organisations to securely transfer data to South Korea without restrictions.[6]

MyData programme, which is currently used for financial services and the public sector, will be used for all fields where general personal information is being transmitted for the facilitation of transactions and disclosure.[7]

1 https://www.dataguidance.com/news/south-korea-pipc-publishes-statement-use-and
2 https://www.dataguidance.com/news/south-korea-pipc-publishes-guidelines-consent-and-easy
3 https://www.dataguidance.com/news/south-korea-pipc-fines-google-and-meta-total-krw-100
4 https://www.dataguidance.com/news/south-korea-pipc-fines-gangwon-do-krw-45m-pipa; https://www.dataguidance.com/news/south-korea-pipc-fines-daejeon-technology-park-krw-78m
5 https://www.dataguidance.com/news/international-ico-and-pipc-sign-memorandum
6 https://www.dataguidance.com/news/international-uk-and-south-korea-reach-data-adequacy
7 https://www.dataguidance.com/news/south-korea-pipc-announces-plans-introduce-mydata-all

SPAIN

Law: Organic Law 3/2018, of 5 December 2018, on the Protection of Personal Data and Guarantee of Digital Rights and GDPR

Regulator: Spanish Data Protection Authority ('AEPD')

EU Adequacy Decision: n/a

Albert Castellenos
albert.castellanos@bdo.es

Notable Changes

There have been no key legislative changes in privacy in the last year, but the AEPD has initiated a GDPR risk assessment tool that empowers organisations to rapidly carry out a non-exhaustive assessment of intrinsic risks stemming from data processing activities, indicating the necessity of performing a data protection impact assessment (DPIA), and enabling remaining risk management by proposing procedures and precautions to minimise alleged risks.[1]

Furthermore, the AEPD has launched the '*Asesora Brecha*' advisory tool to help data controllers decide whether they should notify a personal data breach to the supervisory authority[2]. This tool is free, easy to use and is organised in sections, in order that it is not necessary to complete the entire form in all cases. Once completed, the data provided during the process is deleted, so the AEPD cannot know the information provided.

Data Protection Authority Focus

The AEPD is one of the most active data protection authorities in Europe when it comes to issuing enforcement actions and responding to data subjects' complaints and requests. Since 2021, the AEPD has sent out over 300 fines for GDPR Violations.[3]

Year	Count of Fines	Penalties (EUR/USD)
2022	158	€20.470.941 (early July)[4]
2021	277	€31,910,900
2020	133	€8,152,710
2019	38	€1,318,100
2018	0	0

On 18 May 2022, the AEPD issued a decision against Google, imposing a fine of €10 million for GDPR violations, including the unlawful processing of data, and the "right to be forgotten."

Google made it difficult for users to submit requests for the removal of content. Google required its data subjects to follow a multipart process that included selecting which Google service it wanted data removed from; the base upon which the request was being made (defamation, infringement, harassment, personally identifying information), and then only routed users who designated certain defined grounds for deletion to a web form.[5]

The AEPD found that Google processed the data subjects' data without a valid legal basis, due to the lack of possibility to object to the transfer of the Lumen Project. It also found that Google did not sufficiently enable the data subjects to exercise their right to erasure of their data. In addition, this affected many individuals, and, in some cases, sensitive data was processed[6].

1 https://www.dataguidance.com/news/spain-aepd-launches-gdpr-risk-assessment-tool
2 https://www.dataguidance.com/news/spain-aepd-launched-advisory-tool-data-breach
3 https://www.enforcementtracker.com/
4 https://cincodias.elpais.com/cincodias/2022/07/14/legal/1657790945_321207.html#:~:text=La%20cuant%C3%ADa%20de%20las%20multas,2021%2C%2035%20millones%20de%20euros.
5 https://www.scmagazine.com/native/incident-response/data-privacy-alert-spanish-dpa-fines-google-e10-million
6 https://www.enforcementtracker.com/ETid-1176

SWEDEN

Law: he Swedish Data Act (1973 Revised), Swedish Personal Data Act, 1998, GDPR, The Act with Supplementary Provisions to the GDPR (SFS 2018:218)

Regulator: Swedish Authority for Privacy Protection (IMY)

EU Adequacy Decision: n/a

Hakan Skyllberg
hakan.skyllberg@bdo.se
+46 70 167 16 57

Notable Changes

Sweden has a long history of safeguarding personal integrity and was the first country to adopt data protection legislation with the Swedish Data Act, enacted in 1973. With the implementation of the 1973 Data Act, the Swedish Data Protection Authority was established.[1]

On 7 April 2022, the IMY published a press release concerning the Trans-Atlantic Data Privacy Framework. The IMY noted that the European Data Protection Board (EDPB) had discussed the agreement in principle on a new Trans-Atlantic Data Privacy Framework for the protection of personal data when transferred to the U.S. at its last plenary meeting, noting that the EDPB had welcomed the agreement in principle but warning that much work remains to be done before a new system for transfers is in place.[2]

On 18 July 2022, the IMY announced that it is possible for individuals to whistle blow to the IMY if they have information that their employer, previous employer, or prospective employer does not follow the data protection rules. The IMY noted that the government considered the IMY to be a supervisory authority that is required to implement external whistleblowing channels under the Protection of Persons Reporting Irregularities (2021:890) (the Whistleblowing Act). [3]

Data Protection Authority Focus

Region Uppsala has reported two personal data breaches to the Swedish Authority for Privacy Protection (IMY). Sensitive personal information communicated to receivers inside and outside of Sweden without encryption is the subject of the data breaches.

Following the notification of the data breach, IMY started an investigation into the region (both the regional board and the hospital board), and it states in its two decisions that the region has not incorporated enough organisational and technical safeguards to maintain an appropriate security level in relation to the risks associated with the processing of personal data.

For the identified shortcomings in this investigation, IMY issues an administrative fine of SEK 1.6 million (approx. €144,000) against the hospital board in the Uppsala Region.

The Swedish Authority for Privacy Protection (IMY) noted that that it had completed an audit on Klarna and examined how Klarna informs users on its websites about how it processes personal data in accordance with the GDPR. Furthermore, the IMY stated that during the audit, Klarna had continuously changed the information it provided on how the company handles personal data. As a result, the IMY imposed a fine of SEK 7.5 million (approx. €725,513) against Klarna for the deficiencies discovered during the audit. Furthermore, the IMY stated that Klarna may appeal the decision by writing to the IMY and the IMY must receive the appeal no later than three weeks from the date on which Klarna received the decision.[4]

1 https://www.dataguidance.com/notes/sweden-data-protection-overview
2 https://www.dataguidance.com/news/sweden-imy-publishes-press-release-trans-atlantic-data
3 https://www.dataguidance.com/news/sweden-imy-implements-whistleblowing-channels
4 https://www.dataguidance.com/news/sweden-imy-fines-klarna-sek-75m-breaches-gdpr

SWITZERLAND

Schweizer Datenschutzgesetz - Swiss Data Protection Act

Law: Federal Act on Data Protection 1992 ('FADP'), revised in 2020

Regulator: Federal Data Protection and Information Commissioner ('FDPIC')

EU Adequacy Decision: yes

Klaus Krohmann
klaus.krohmann@bdo.ch
+41 44 444 36 25

Notable Changes

The Swiss Parliament ratified a total modification of the Swiss Data Protection Act (DPA) in the fall of 2020.[1] The Swiss Federal Council issued also a totally revised executing ordinance[2] on data protection and a new ordinance on data protection certifications,[3] which will all enter into force on 1 September 2023. The new act and its new sanctions will become effective and enforceable that date without any further grace period.

The totally revised Swiss DPA is based on principles analogous to the GDPR, however, has material deviations.

Although the DPA is overall slightly less stringent than the GDPR, compliance with the GDPR does not entirely cover the requirements of the Swiss DPA; additional actions will be required.

The terms in the new DPA deviate from the GDPR; associated compliance documentation and frameworks may need revision.

Data Protection Authority Focus

In its annual report for 2021, the Federal Data Protection and Information Commissioner (FDPIC) expressed concern that COVID-19 control measures have severely restricted citizens' freedom and privacy.

The FDPIC furthermore found that a Transfer Impact Assessment (TIA) similar to the concept of the EU is also required under Swiss data protection legislation. In particular, a documented assessment is required prior the transfer of personal data in a jurisdiction which is not recognised to have an equivalent level of data protection compared with Switzerland.[4]

1 SR 235.1 - Bundesgesetz vom 25. September 2020 über den Datenschutz (Datenschutzgesetz, DSG) (admin.ch)
2 SR 235.11 - Verordnung vom 31.August 2022 über den Datenschutz (Datenschutzverordnung, DSV) (admin.ch)
3 SR 235.13 - Verordnung vom 31. August 2022 über Datenschutzzertifizierungen (VDSZ) (admin.ch)
4 https://www.edoeb.admin.ch/dam/edoeb/de/dokumente/2021/Anleitung%20f%C3%BCr%20die%20Pr%C3%BCfung%20von%20Daten%C3%BCbermittlungen%20mit%20Auslandbezug%20DE.pdf.download.pdf/Anleitung%20f%C3%BCr%20die%20Pr%C3%BCfung%20von%20Daten%C3%BCbermittlungen%20mit%20Auslandbezug%20DE.pdf

SWITZERLAND (CONTINUED)

Schweizer Datenschutzgesetz - Swiss Data Protection Act

Law: Federal Act on Data Protection 1992 ('FADP'), revised in 2020

Regulator: Federal Data Protection and Information Commissioner ('FDPIC')

EU Adequacy Decision: yes

Klaus Krohmann
klaus.krohmann@bdo.ch
+41 44 444 36 25

Changes by the Reform

- The new Swiss DPA foresees penal sanctions against the responsible persons of the organisation. In a Swiss Ltd this is in first line the board of directors and the top management.
- Thus, board members and members of the management of Swiss companies face in future personal fines up to CHF 250'00 and criminal record entries, if their company is incompliant with the Swiss DPA. Such personal liability cannot be insured.
- Data Subject Access Rights are strengthened.
- New information duties for the processing of personal data are stipulated, various exceptions apply.
- Data Incident Reporting is introduced: Reporting duty "as soon as possible".
- Exterritorial scope beyond the boundaries of the Territory of Switzerland.
- Duty to appoint a representative in Switzerland for foreign companies acting in Switzerland or monitoring people in Switzerland, subject to specific requirements.
- Although a "principle of accountability" is not explicitly stated in the Swiss DPA, a reliable documentation of compliance will also be required to demonstrate in penal proceedings that you acted diligent in privacy matters.
- Legal entities are no longer protected by the DPA.
- Further types of personal data are covered by the special categories of personal data.
- The terms used by the Swiss DPA are not identical with the terms in the GDPR. Thus, a transformation of GDPR documentation is required in any case. Swiss specialties must be respected.

UNITED ARAB EMIRATES (UAE)

Law: Federal Decree-Law No. 45 of 2021 regarding the Protection of Personal Data (the Law)

Regulator: UAE Data Office

EU Adequacy Decision: no

Shivendra Jha
shivendra.jha@bdo.ae
+971 4 518 6666

Notable Changes

In 2021, the UAE enacted the Law regarding the protection of personal data. The Law covers the processing of personal data belonging to data subjects within the UAE, regardless of the location of the data controller or data processor.

Additionally, the Law details the conditions for consent, data subject rights, and extensive requirements for controllers and processors. Amongst these requirements are mandatory breach notifications, appointments of data protection officers, and the enactment of technical and organisational safeguards to support data security.[1]

Data Protection Authority Focus

In the last year, two Data Protection laws were significantly updated (Dubai International Financial Centre (DIFC) Data Protection Law and Abu Dhabi Global Market (ADGM) Data Protection Regulation). Additionally, standards for the healthcare sector were updated – the Department of Health (DOH) Abu Dhabi's Healthcare Information and Cyber Security Standards (ADHICS). These legislations cover both data protection and data privacy. UAE to have country-wide data privacy and protection legislation within the next few years.

Jurisdiction-specific data privacy and protection laws tend to incorporate the learnings from various legislations implemented elsewhere in the world, including EU's GDPR and have specific articles related to needs of the UAE. Consensus to meet global requirements drove the ADGM to become the first in the gulf country to join the Global Privacy Assembly's International Enforcement Cooperation Working Group (IECWG).

Much effort has been put in by the authorities to educate organisations and the public about the legislation in force and how to comply. Further, specific guidance materials have also been made available to organisations and individuals who can implement the controls specific to the legislation. This guidance material also incorporates some self-service questionnaires to clarify any topics.

Fines vary in number. For example, DIFC Data Protection Law has a maximum fine of USD 100,000 for an administrative breach and scope for more considerable (unlimited) fines for more serious violations. For ADGM Data Protection Law, the penalties are capped at USD 28 Million for significant data breaches.

1 https://www.dataguidance.com/jurisdiction/uae

UNITED KINGDOM

Law: UK Data Protection Act 2018 (DPA 2018), UK GDPR

Regulator: The Information Commissioner's Office ('ICO')

EU Adequacy Decision: yes

Christopher Beveridge
christopher.beveridge@bdo.co.uk
+44 795 699 1215

Notable Changes

The U.K. data protection regime is regulated by the Data Protection Act 2018, and the EU GDPR has been written into U.K. law and tailored to become the "U.K. GDPR." The European Commission published two adequacy decisions for the U.K., one for transfers under the EU GDPR (Commission Implementing Decision of 28 June 2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council) and one for transfers under the Law Enforcement Directive (Data Protection Directive with Respect to Law Enforcement (Directive (EU) 2016/680) (Commission Implementing Decision of 28 June 2021 pursuant to Directive (EU) 2016/680 of the European Parliament and of the Council on the Adequate Protection of Personal Data by the United Kingdom)). The U.K. GDPR and the Data Protection Act 2018 establish that the ICO is the supervisory authority in the U.K. and detail its functions, including an obligation to prepare codes of practice. The ICO is a particularly active authority and regularly issues guidance on a wide range of topics.

The most notable change for the U.K. in 2022 was the introduction of the new U.K. International Data Transfer rules. On 21 March 2022, the data transfer landscape changed in the U.K. for any organisation who had an exposure to international data transfer outside of the U.K. Following on from Brexit and the removal of the U.K. from the EU, the use of the newly drafted EU Standard Contractual Clauses as an international data transfer safeguard was never an viable option for UK organisations.

As a result, in February 2022, a number of changes were laid before U.K. parliament:

- The new UK International Transfer Agreement (IDTA);
- The new International Data Transfer U.K. Addendum to the EU's new Standard Contractual Clauses (UK Addendum); and
- The relevant transitional provisions

From 21 March 2022, any U.K. organisation relying on contractual safeguards to transfer personal information outside of the U.K. must ensure they sign the IDTA or the new UK Addendum linked to the new EU version of the Standard Contractual Clauses. These documents supersede all other contractual safeguards the U.K. were previously reliant on i.e., the old EU version of the Standard Contractual Clauses pre-dating the Schrems II decision. Other key dates to be aware of include the 22 September 2022 which was the date U.K. based organisations are no longer able to rely on the old EU SCC's and from this date U.K. organisations must ensure the new U.K. International Data Transfer documents are in place for any new international data transfers entered into. The other key date is 21 March 2024 which represents the date that U.K. based organisations are no longer able to rely on the use of the old EU Standard Contractual Clauses for any pre-existing (so agreements entered into before 22 September 2022) or legacy exposures to international data transfers.

UNITED KINGDOM (CONTINUED)

Law: UK Data Protection Act 2018 (DPA 2018), UK GDPR

Regulator: The Information Commissioner's Office ('ICO')

EU Adequacy Decision: yes

Christopher Beveridge
christopher.beveridge@bdo.co.uk
+44 795 699 1215

On 10 May 2022, it was announced in the late Queen's Speech at the state opening of U.K. Parliament that the U.K. government will be introducing a Data Reform Bill of which the purpose of the bill will be to reform the existing U.K. data protection regime that has been inherited from the EU following Brexit, namely the EU GDPR. In June 2022, the U.K. government published its long awaited response to the September 2021 consultation 'Data: a new direction' which outlined plans to reduce burdens on business by enabling organisations to create flexible and proportionate compliance regimes and on 18 July 2022 the Data Protection and Digital Information Bill was introduced to Parliament where currently the U.K. are still waiting on a decision on when the bill might be introduced into U.K. law.

Data Protection Authority Focus

On 3 October 2022, the U.S. Department of Justice (DoJ) announced that the agreement between the government of the United States of America and the government of the United Kingdom of Great Britain and Northern Ireland on Access to Electronic Data for the Purpose of Countering Serious Crime entered into force. The DoJ outlined that the agreement, as authorized by the Clarifying Lawful Overseas Use of Data Act of 2018 (the CLOUD Act), is the first of its kind and will allow investigators from both countries to gain access to data relating to serious crimes in a way which respects privacy and civil liberties.[1]

On 7 October 2022, the U.K. Secretary of State for Digital, Culture, Media and Sport and the U.S. Secretary of Commerce issued a joint statement to address the launch of a U.K.-U.S. Comprehensive Dialogue on Technology and Data and the progress on U.K. - U.S. data adequacy. In relation to data adequacy, the statement noted that both countries had accelerated and broadened discussions on promoting bilateral and globally interoperable cross-border data flows, agreeing to conclude such adequacy work in the weeks ahead.[2]

On the enforcement front, the U.K. regulator (Information Commissioners Office) has been reasonably active across 2022 issuing 57 enforcement actions made up of 33 monetary penalties, 23 enforcement notices and 1 individual prosecution. The focus of the U.K. supervisory authority in 2022 has been on marketing, finance and retail organisations where 45 of the 57 enforcement actions related to an organisation involved within one of these sectors.

1 https://www.dataguidance.com/news/international-uk-us-data-access-agreement-enters-force
2 https://www.dataguidance.com/news/international-uk-and-us-agree-conclude-data-adequacy

UNITED STATES

Various

Regulator: The Federal Trade Commission (FTC)

EU Adequacy Decision: no

Mark Antalik
mantalik@bdo.com
+1 617-378-3653

Taryn Crane
tcrane@bdo.com
+1 301-354-2583

Notable Changes

Federal Privacy and Data Protection Laws

The U.S. does not currently have a comprehensive privacy law. Instead, privacy is governed by a number of sectoral laws including:

- The Health Insurance Portability and Accountability Act of 1996 which governs the privacy and security of personal health data collected by covered health entities;
- The Gramm-Leach-Bliley Act of 1999 which governs the collection of personal data by financial institutions used in consumer transactions; and
- The Children's Online Privacy Protection Act of 2000 which governs the collection of personal data from individuals under the age of 13.

Debate over a Federal U.S. privacy law has grown in the past 10 years. In the 117th Congress (2021-2022), the House of Representatives introduced the American Data Privacy and Protection Act (ADPPA) which provided a federal framework governing the collection and processing of U.S. residents' personal data. Additionally, the ADPPA required that businesses provide individuals a way to opt-out of targeted advertising and provide legal rights including the ability for individuals to access, correct, and delete their personal data.

The ADPPA never received a vote in either house of Congress and therefore the legislation expired at the end of the last session. Another version of the bill will likely be introduced in the new Congress that began in January 2023.

Federal Authority

The Federal Trade Commission (FTC) is the most prominent Federal agency that can issue enforcement actions to organisations for violating consumers' rights to privacy under Section 5 of the FTC Act of 1914.[1] The FTC brings civil action against organisations that may have seriously harmed consumers by misrepresenting or failing to protect consumers' personal data. The FTC also prosecutes businesses for unfair and deceptive business practices and upholds other Federal laws pertaining to the safety and privacy of consumers. Two prominent FTC enforcement actions from this past year include:

Chegg: The FTC took action against the educational technology provider for deficient data security procedures that exposed consumers' personal data. The FTC required Chegg to 1) limit the personal data it can collect and process, 2) provide consumers with multifactor authentication to protect their accounts, and 3) allow consumers to access and erase their data.

Twitter: The FTC took action against Twitter when the company sold individual account security data to its advertisers. The FTC required Twitter to pay a $150 million fine and prohibited them from making money from the data it fraudulently collected.

Other Federal agencies including the Department of Health and Human Services, Department of Treasury, and the Federal Communications Commission also can enforce privacy-related regulations against organisations within those departments' jurisdictions.

1 https://www.dataguidance.com/news/international-uk-us-data-access-agreement-enters-force

UNITED STATES (CONTINUED)

Various

Regulator: The Federal Trade Commission (FTC)

EU Adequacy Decision: no

Mark Antalik
mantalik@bdo.com
+1 617-378-3653

Taryn Crane
tcrane@bdo.com
+1 301-354-2583

There were 368 breaches regarding healthcare data reported to the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) in the first half of 2021, which is 21 fewer breaches than in the same period in 2022. That reflects a decrease in reported breaches of 5.71%.[2]

Data Transfers

The European Union is expected to ratify the TransAtlantic Data Privacy Framework in 2023 which will reinstitute transfers personal data between the U.S. and EU without the need for mechanisms such as standard contractual clauses or binding corporate rules. The Framework replaces the Privacy Shield, invalidated by the EU High Court in 2020. Furthermore, the US participates in the Asia Pacific Cross-Border Privacy Rules system and the Privacy Shield Framework with Switzerland, both of which permit the transmission of data to other jurisdictions.

State Privacy and Data Protection Laws

California, Colorado, Connecticut, Utah, and Virginia are the five states that currently have comprehensive laws to protect the privacy of individual personal data. These laws share many key aspects of the GDPR including 1) requiring businesses to provide privacy notices to individuals; 2) providing the right for individuals to access and delete their personal data; and 3) providing right to opt- out of the sale or sharing of personal data.

Current U.S. State Privacy Laws

State	Law	Regulator	Date Effective
California	California Consumer Protection Act/ California Privacy Rights Act	California Privacy Protection Agency	Jan. 1, 2020
Colorado	Colorado Privacy Act	Colorado Attorney General	Jan. 1, 2023
Connecticut	Connecticut Act Concerning Personal Data Privacy and Online Monitoring	Connecticut Attorney General	July 1, 2023
Virginia	Virginia Consumer Data Protection Act	Virginia Attorney General	Jan. 1, 2023
Utah	Utah Consumer Privacy Act	Utah Attorney General	Dec. 31, 2023

2 https://www.hipaajournal.com/1h-2022-healthcare-data-breach-report/

Karen A. Schuler
kschuler@bdo.com

In addition to this whitepaper, a new BDO website with up-to-date information on data privacy per country, will be available soon. Via this website, you will also be able to subscribe to regular updates by e-mail on data privacy legislation per country.