AN OFFERING FROM BDO'S
DATA PRIVACY PRACTICE

PRIVACY INSIGHTS 2021

BDO

FOREWORD

This whitepaper focuses on data privacy regulatory insights around the globe and how BDO helps our clients solve those challenges.

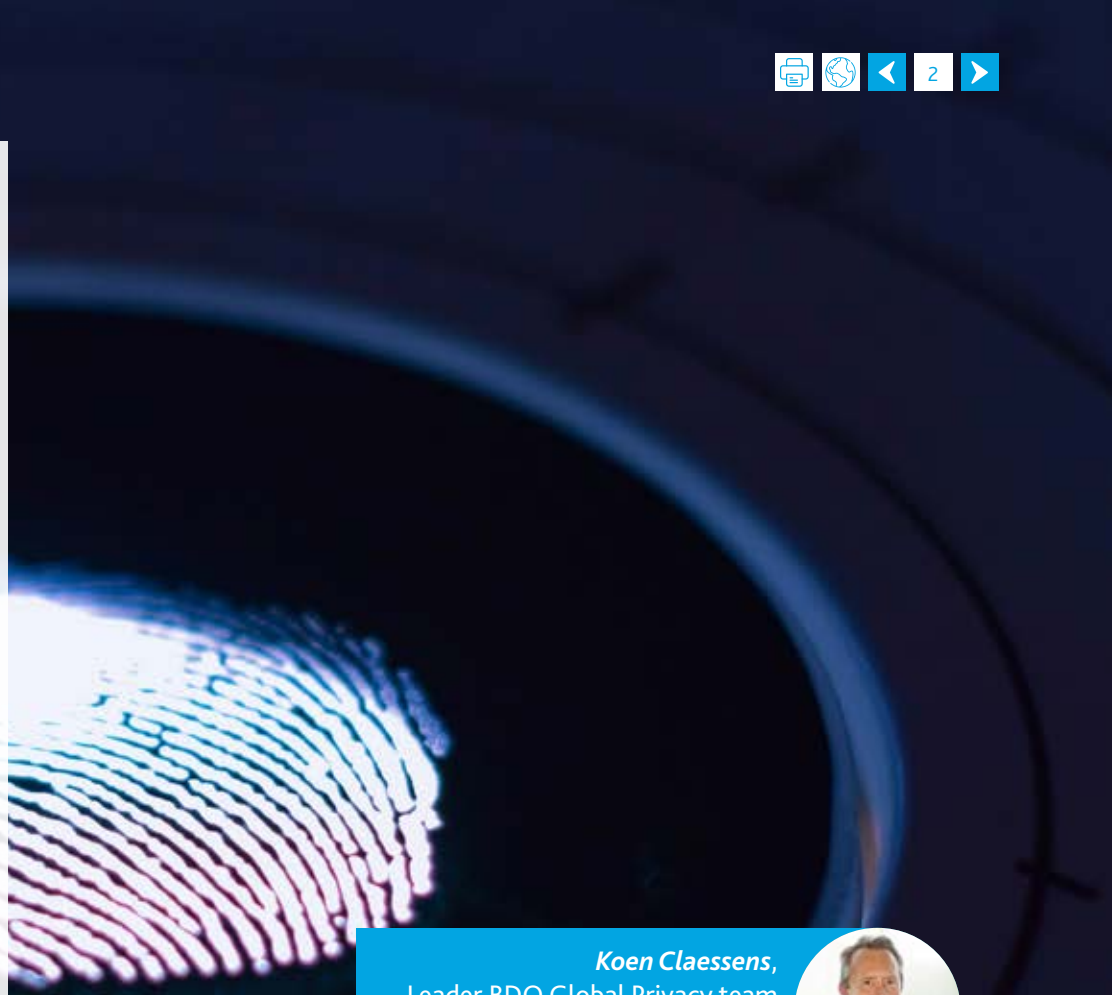
Privacy and data protection legislation continue to evolve. Recent evolutions, like the EU-US Privacy Shield, Swiss-US Privacy Shield, and Brexit have proven this. Organisations of all sizes struggle with staffing, process, and technology to manage their global privacy and data protection programmes.

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

Over the last 18 months, companies have shifted their models from in-person to remote operations. In many cases, privacy and data protection policies and procedures have not caught up to prevent data leakage, data misuse, and the increase in Data Protection Authority inquiries and investigations.

While most organisations recognise the importance of data privacy compliance, they struggle with limited staff and insufficient global coverage. Therefore, it is more important than ever for organisations to enhance and maintain their data protection and privacy compliance programmes. Our **Global DPO-as-a-Service** and **Data Protection Managed Services (DPMS)** can assist with this.

Privacy professionals require critical knowledge and a network of trained peers to manage privacy obligations effectively. **BDO's Global Data Protection Academy** enables professionals to meet 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 privacy professionals.



Koen Claessens,
Leader BDO Global Privacy team
Managing partner Risk Advisory
BDO Belgium

Karen A. Schuler,
co-leader BDO Global Privacy team,
Governance, Risk & Compliance
(GRC), National Leader, BDO USA

INTRODUCTION

It's been quite a year once again regarding privacy and data protection developments around the globe. Several jurisdictions implemented data protection and privacy legislation, most notably California and the California Consumer Privacy Act (CCPA), which came into force in January 2020, and Brazil's Lei Geral de Protecao de Dados (LGPD) was passed into force in September 2020.

These trends continue:

- China published the first draft of its General Data Protection Regulation ("GDPR"), the Personal Information Protection Law (PIPL)
- Singapore updated its Personal Data Protection Act (PDPA)
- Australia is due to undertake a full review of their Privacy Act this year
- U.S. states continue to update individual state data protection and privacy legislation

And, much more data protection and legislative privacy updates are in the pipeline regarding jurisdictions around the globe.

Privacy and data protection legislation is complex and evolving. In addition to international legislation updates we are experiencing, there were two other significant developments in 2020.

Invalidation of EU-US Privacy Shield

In July 2020, Europe's highest court, the European Courts of Justice, delivered their verdict in the 'Schrems II' case and invalidated the EU-US Privacy Shield. Previously the European Union ("EU") recognised the EU-US Privacy Shield as an adequate safeguard to transfer data across the Atlantic. However, this judgment caused several issues for organisations relying on it.

In the last five years, this is the second time that the European Union invalidated an EU-US data transfer safeguard, invalidating the predecessor to the EU-US Privacy Shield, 'Safe Harbor,' in 2015. The decision to invalidate Privacy Shield hinged on two factors:

1. Surveillance techniques used by U.S. authorities at the time information arrived in the United States ("US") from the EU, and
2. EU data subjects were unable to remedy misuses of personal data.

In practice, what does the decision mean? Organisations that data transfer between the EU and the US relied on the EU-US Privacy Shield. However, under the EU General Data Protection Regulation ("GDPR") this ruling requires that companies identify an alternative legal basis to transfer personal data. Options afforded to companies include:

a) Articles 46(2)(b) and 47, Binding Corporate Rules ("BCRs")

b) Article 49, derogations

c) Article 28, Data Processing Agreements

d) Standard Contractual Clauses

Binding Corporate Rules

Binding Corporate Rules are data protection policies adhered to by companies established in the EU for "transfers of personal data outside of the EU" within a group of enterprises. The procedures must include data protection principles and enforceable rights to ensure appropriate safeguards for data transfers. They must be legally binding by every member of the concerned group[1].

The process to approve BCRs is lengthy and costly. However, there are documents and assistance provided by the European Data Protection Board ("EDPB"), titled Working Document Setting Forth a Co-Operation Procedure for the approval of "Binding Corporate Rules" for controllers and processors under the GDPR to assist companies with developing their BCRs.

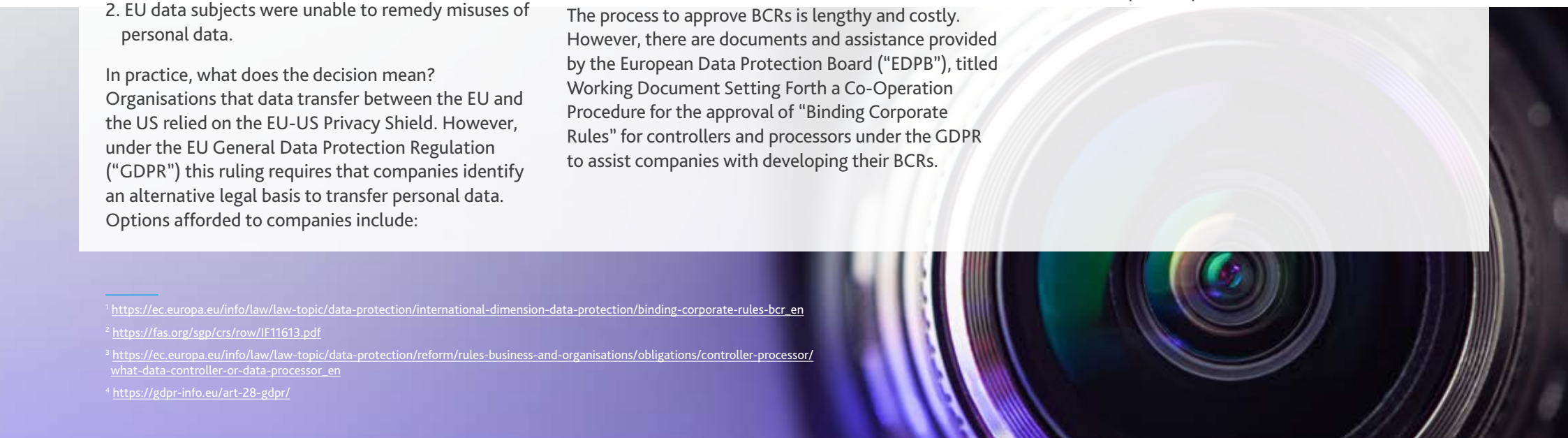
Derogations

Under EU law, specific derogations[2] are allowed for the transfer of personal data. Common derogations include, but are not limited to:

- Performance of a contract
- Explicit consent by a data subject

Data Processing Agreements

Global organisations are no stranger to Data Processing Agreements to transfer personal data between the data controller and the data processor[3]. Under the GDPR Article 28, Data Processing Agreements are a 'contract or other legal act under Union or Member State law'[4] that requires the implementation of technical and organisational measures to protect personal data.



[1] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en

[2] https://fas.org/sgp/crs/row/IF11613.pdf

[3] https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_en

[4] https://gdpr-info.eu/art-28-gdpr/

Invalidation of EU-US Privacy Shield (continued)

Standard Contractual Clauses

Despite the extension of Standard Contractual Clauses (SCCs) upheld by the Court, complications exist.

In practice, the judgment suggests that a data exporter and the data recipient analyse each case individually where they plan to rely on SCCs. Each case must meet a certain level of due diligence to demonstrate that the third country recipient ensures adequate data protection under EU law for any personal data transferred. If sufficient data protection is not possible, then the data exporter must consider additional safeguards. If those other safeguards are not attainable, then the data transfer must cease immediately.[5]

Furthermore, it is also important to note that the Supervisory Authorities now have the power to suspend transfers where they view that the third country will not have an adequate level of protection in place required by EU law.

It remains unknown how this affects the transfer of personal data to the US. By virtue that the EU-US Privacy Shield has been invalidated, predominantly due to the lack of protection surrounding government access to the information, the European Courts view of the US to have sufficient protections in place is somewhat lacking. The ruling is a challenge for any EU organisation relying on SCCs to transfer personal data to the US.

And, of course, the invalidation of SCCs negatively impacts any organisation that is transferring personal data to a third country and is currently relying on SCCs as the lawful remedy to do this.

[5] https://www.bdo.co.uk/en-gb/insights/advisory/risk-and-advisory-services/european-courts-of-justice-invalidates-eu-us-privacy-shield

Finalisation of Brexit Deal

On **24 December 2020**, the United Kingdom ("UK") agreed on a deal with the European Union ("EU") and signed the UK-EU Trade and Cooperation Agreement ("the Trade and Cooperation Agreement"). How did this impact data protection and the flow of information from the European Union to the United Kingdom, and vice versa?

The primary data protection concern for organisations surrounded data transfers after the initial Brexit transition period on **31 December 2020**. Before the Brexit deal and in the absence of an EU-UK adequacy agreement, **1 January 2021** onward, data transfers into the United Kingdom from an EU-based jurisdiction would have been deemed a transfer to a third country by the European Union. Any such transfer would have needed to use appropriate data transfer safeguards stated in Chapter V of the GDPR.

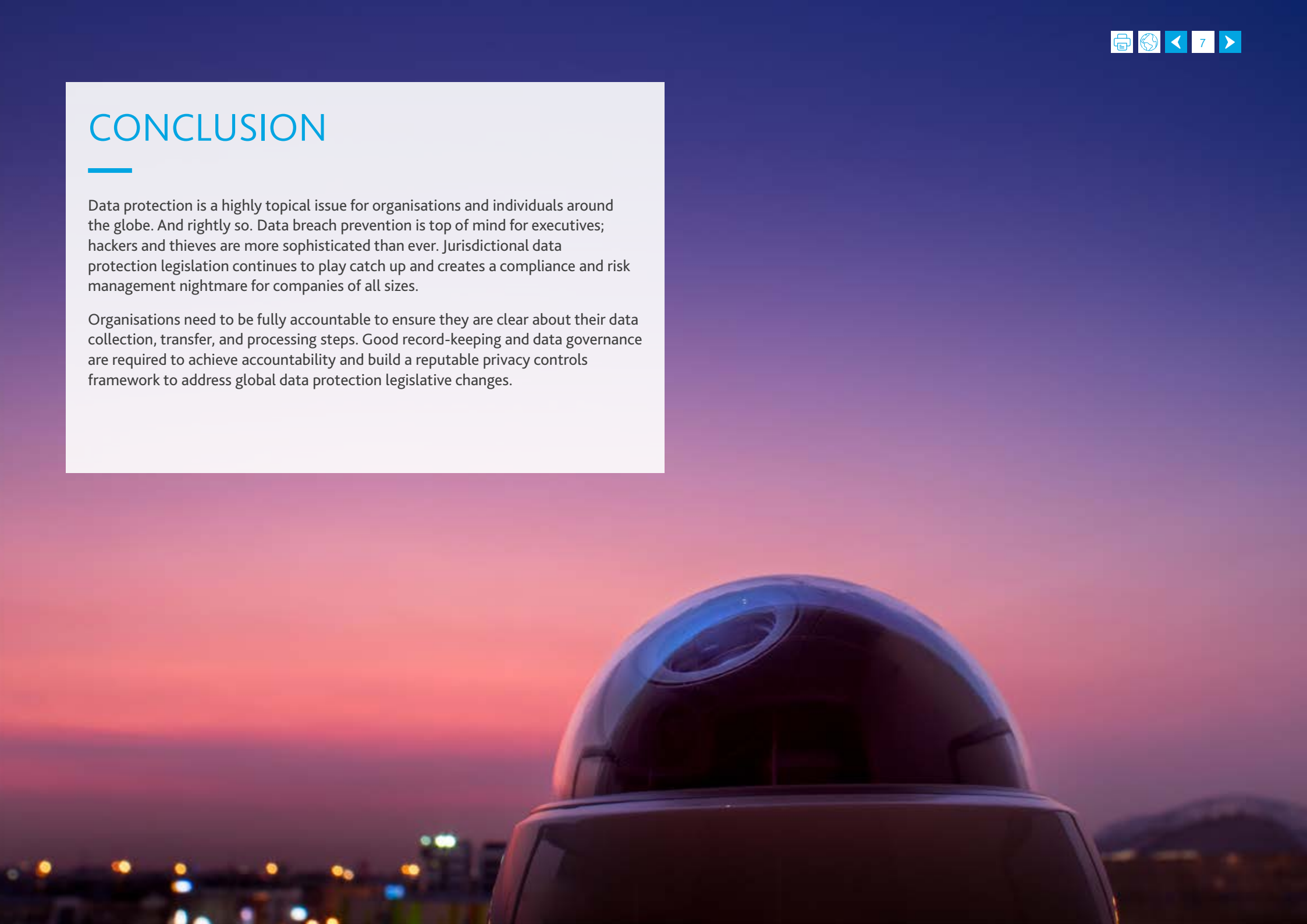
The Trade and Cooperation Agreement provides an interim period potentially lasting six months. During this time, data transfers from the EU to the UK can continue during the transition period. It's important to note that the Trade and Cooperation Agreement states that the interim period is initially four months to **1 May 2021** with an automatic extension of two months to 1 July 2021 (unless the EU or the UK objects).

The interim period provided enough time to finalise the EU-UK adequacy agreement. After executing the Trade and Cooperation Agreement, the European Commission published the draft UK adequacy decisions in February 2021. Two decision drafts include: (1) commercial data flows and (2) law enforcement data flows. On 28 June 2021, just before the deadline of the post-Brexit grace period under the Trade and Cooperation Agreement, the EU Commission adopted both adequacy decisions addressing the transfers of personal data to the UK under the GDPR and the Law Enforcement Directive (e.g., together known as the UK Adequacy Decisions).

CONCLUSION

Data protection is a highly topical issue for organisations and individuals around the globe. And rightly so. Data breach prevention is top of mind for executives; hackers and thieves are more sophisticated than ever. Jurisdictional data protection legislation continues to play catch up and creates a compliance and risk management nightmare for companies of all sizes.

Organisations need to be fully accountable to ensure they are clear about their data collection, transfer, and processing steps. Good record-keeping and data governance are required to achieve accountability and build a reputable privacy controls framework to address global data protection legislative changes.



BDO GLOBAL DATA PROTECTION ACADEMY

Data and disruptive technologies are crucial elements in this highly interconnected global economy. Organisations that process and store data must protect and mitigate potential risks associated with the data they manage and store, following data protection and privacy legislation worldwide. Failure to do so can result in fraud, negative press, and loss of revenue, productivity, and brand trust. At the foundation of data protection and privacy is training, as it allows companies to retain professionals, develop awareness, and communicate more effectively to the organisation.

BDO's Data Protection Academy assists organisations in achieving those goals and provides training from anywhere at any time. As an authorised International Association of Privacy Professionals (IAPP) trainer, we offer various courses delivered with trainers with global experience. Additionally, we provide our clients with:

- Private, customised training for organisations;
- eLearning and Learning Management System (LMS) content development and delivery services;
- complimentary webinars focused on hot topics; and
- a BDO Blockchain in Privacy Course which launches in January 2022.

Our team annually trains more than 10,000 professionals, in over 50 countries, and provides customised training for the Global 500. BDO's trainers are practitioners with experience as the Data Protection Officer, CPO, CISO, CIO, and have backgrounds in legal, technology, disruptive technologies, management, and business processes. We are well versed in cultural and language nuances, as well as evolving regulatory changes. The Data Protection Academy currently offers the following International Association of Privacy Professionals ("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)

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)

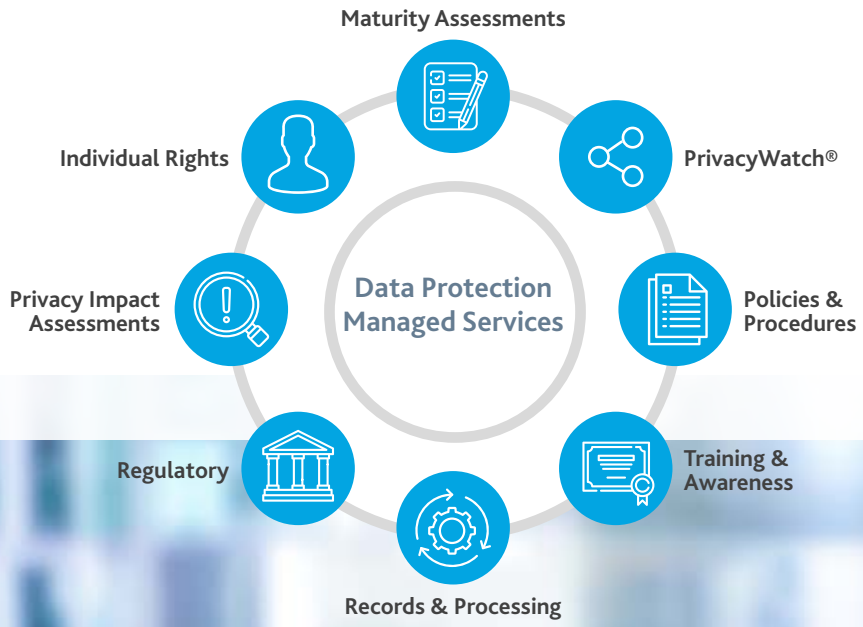
With the growing number of global regulations, increased consumer privacy awareness, and the risks of data loss, it is more important than ever for organisations to enhance and maintain their data protection and privacy compliance programmes. While most organisations & recognise the importance of data 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 10

- A Fortune 50 company required a service that could offer the privacy expertise and scalability to fulfill their high volume of data subject requests. Since May 2018, BDO has fulfilled nearly 500,000 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 proprietary Privacy Management Framework (PMF)® and a team of managed service professionals worldwide, BDO has successfully established the client's foundational privacy capabilities and continues to manage and enhance the programme on an ongoing basis.



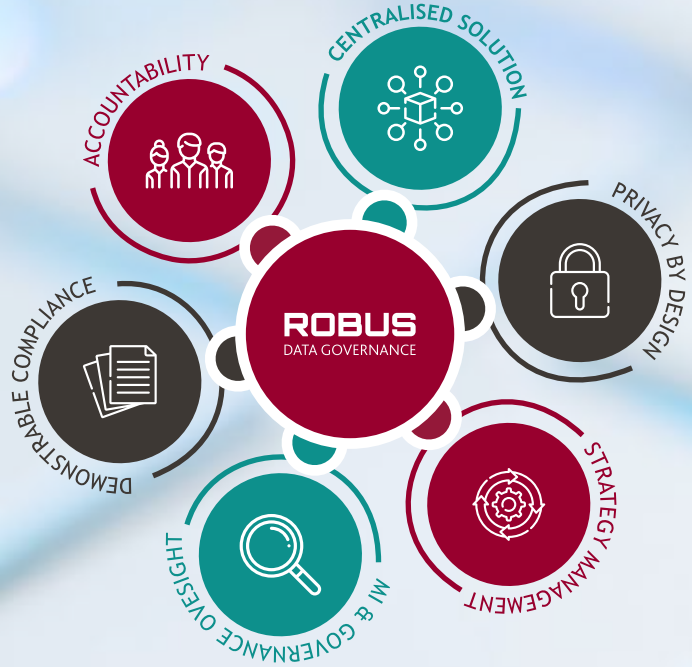
BDO ROBUS

Businesses often struggle with demonstrating compliance with data protection regulations, attempting to manage privacy activities manually[6]. However, the complexities of tracking processing activities, assets, third parties, data subject access requests, and data transfers across siloed functions are highly inefficient, duplicative, and costly.

BDO's ROBUS tool provides a comprehensive approach to data protection by formalising Privacy-by-Design, Data Subject Requests, Privacy Impact Assessments, and breach response. The tool's automated controls and real-time information flows provide a framework to facilitate informed decisions. The end-to-end product enables aggregated reporting of key performance indicators that unify an enterprise view for data risk management. ROBUS is flexible to adapt and be customised to various environments and enhances client efficiencies and insights.

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

Kimberley Lockley
klockley@bdo.je



[6] IAPP Annual Privacy Governance Report 2019

BDO GLOBAL DATA PROTECTION OFFICER AS A SERVICE (DPO-AS-A-SERVICE)

As an organisation's outsourced Global Data Protection Officer ("DPO"), BDO helps companies to:

- Understand their regulatory obligations,
- Identify and close gaps of non-compliance with regulatory obligations
- Fulfill the statutory position of DPO where required,
- Liaise with Data Privacy Authorities and respond to potential data breaches as required,
- Establish their privacy and data protection processes,
- Monitor and respond to individual rights requests,
- Increase user awareness on data privacy obligations and their role in this,
- Provide in-country support, and
- Provide executive updates and strategy.

Through our oversight and management, from readiness to ongoing support, our professionals work with organisations across the globe to remediate risks and help effectively manage your DPO needs. Additionally, our professionals are well versed in privacy laws and regulations to ensure that you remain in compliance across the globe.

BDO GLOBAL DATA PROTECTION OFFICER AS A SERVICE (DPO-AS-A-SERVICE) (CONTINUED)

BDO's three step process allows for an easy and methodical onboarding process.

Asses & Onboard

- Define jurisdictional obligations
- Establish privacy process and escalation procedures
- Identify privacy compliance risks and gaps
- Plan communications cadence
- Onboard local DPO team

Support

- Respond to regulatory and data subject inquiries
- Track and measure privacy initiatives
- Support local privacy awareness and enablement activities
- Complete Data Protection Impact Assessments and jurisdictional obligations

Improve

- Conduct quarterly and annual reviews
- Continuously refine privacy processes
- Provide feedback and present to executives on the current state

For more information about our Global Data Protection Officer services, contact:

Gregory Reid
greid@bdo.com
or BDO DPO Team

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 another no cost 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 the BDOBDO's PrivacyWatch.,

Click here for 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 jurisdiction. We asked each country the following questions, summarised on the next page and then detailed out for each country on the subsequent pages.

- **What is the name your country's data privacy law?**
- **Does your country have an adequacy decision in place with the EU?**
- **What critical data privacy and data protection legislative changes have been announced or implemented within your country during the last 12 months?**
- **What is the focus of your country's Data Protection Authority regarding fines, judgments, case law, public comments, or other guidance?**

Generally, legislators are:

- Updating privacy laws to reflect its country's values
- Implementing new regulations and measures to combat personal data misuse, loss and theft from the increased sharing of health data in response to COVID-19
- Modernising privacy and data protection legislation to remain current (e.g., technology, remote workforce)
- Instituting new privacy and data protection laws in countries that have had difficulties passing comprehensive laws
- Negotiating third-country adequacy agreements

Regulators continue to:

- Focus on a requirement for companies to build and manage Data Governance practices, processes, and policies
- Monitor and investigate data breaches that impact personal data theft
- Follow up on individual rights requests and complaints to ensure companies continue to resolve issues promptly

Based on BDO's observations, we predict that countries will continue to evolve their privacy and data protection legislation to remain current with the ever-growing workforce and the introduction of disruptive technologies (e.g., blockchain, cryptocurrency).


Cayman Islands
Hong Kong
Singapore
Mauritius
Guernsey
Jersey
Malta
Clickable

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

Country	Data Protection / Privacy Law	Data Protection Regulator	EU Adequacy Decision[7]	Other Related Laws
 Argentina	Personal Data Protection Act, Act No. 25.326 of 2000	National Directorate for Personal Data Protection	Yes[8]	Argentinian Constitution and Regulatory Decree 1558/2001
 Australia	Privacy Act 1988 (No. 119, 1988) (as amended) ('the Privacy Act')	The Office of the Australian Information Commissioner ("OAIC")	No	Treasury Laws Amendment (Consumer Data Right) Bill 2019
 Austria	GDPR	Austrian Data Protection Authority	N/A	Austrian Data Protection Act / Datenschutzgesetz
 Belgium	GDPR	Belgian Data Protection Authority	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,
 Brazil	Law No. 13.709 of 14 August 2018, General Personal Data Protection Law (as amended by Law No. 13.853 of 8 July 2019) ("LGPD")	Brazilian Data Protection Authority ("ANPD")	No	
 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 for Personal Data Protection and its Administration

[7] European Commission, Adequacy Decisions

[8] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

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

Country	Data Protection / Privacy Law	Data Protection Regulator	EU Adequacy Decision	Other Related Laws
Canada	The Personal Information Protection and Electronic Documents Act (PIPEDA)	Office of the Privacy Commissioner of Canada ('OPC')	Yes	Privacy Act 1985 ('the Privacy Act'), Bank Act of 1991, Canada's Anti-Spam Legislation, Proceeds of Crime (Money Laundering) and Terrorist Financing Act, 2000
Cayman Islands	Data Protection Regulations, 2018 (SL 17 of 2019), The Data Protection Act (2021 Revision)	Office of the Ombudsman ('the Ombudsman')	No	
China	Personal Information Protection Law ("PIPL")	The Cyberspace Administration of China ("CAC")	No	Cybersecurity Law 2016
Colombia	Statutory Law 1581 of 2012 (October 17)	Colombia Data Protection Authority ("SIC")	No	
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
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

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

Country	Data Protection / Privacy Law	Data Protection Regulator	EU Adequacy Decision	
Finland	GDPR	Office of the Data Protection Ombudsman	N/A	The Data Protection Act (1050/2018)
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
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	
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
Guernsey	The Data Protection (Bailiwick of Guernsey) Law, 2017	The Office of the Data Protection Authority	Yes	

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

Country	Data Protection / Privacy Law	Data Protection Regulator	EU Adequacy Decision	Other Related Laws
Hong Kong	Personal Data (Privacy) Ordinance (Cap. 486) as amended in 2012 ('PDPO')	The Office of the Privacy Commissioner for Personal Data ('PCPD')	No	
India	Introduced the Personal Data Protection Bill, 2019	Once passed, the Data Protection Authority of India to be established	No	Information Technology Act, 2000, amended to address specific data protection concerns
Ireland	GDPR	Data Protection Commission ('DPC')	N/A	Data Protection Act 2018
Israel	Protection of Privacy Law, 5741-1981	Privacy Protection Authority ('PPA')	Yes	Protection of Privacy Regulations (Data Security) 5777-2017
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	
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')
Jersey	Data Protection (Jersey) Law, 2018	Jersey Office of the Information Commissioner ('JOIC')	Yes	Data Protection Authority (Jersey) Law 2018
Latvia	GDPR	Data State Inspectorate ('DVI')	N/A	Personal Data Processing Law of 21 June 2018

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

Country	Data Protection / Privacy Law	Data Protection Regulator	EU Adequacy Decision	Other Related Laws
Malta	GDPR	Office of the Information and Data Protection Commissioner ('IDPC')	N/A	The Data Protection Act (Act XX 2018) ('the Act'
Mauritius	Data Protection Act 2017 ('the Data Protection Act')	Data Protection Office ('the Office')	No	
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
The Netherlands	GDPR	Dutch Data Protection Authority ("AP")	N/A	Act Implementing the GDPR
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)
Panama	Law No. 81 on Personal Data Protection 2019	National Authority for Transparency and Access to Information ('ANTAI')	No	
Poland	GDPR	Polish Data Protection Authority ("UODO")	N/A	Act of 10 May 2018 on the Protection of Personal Data
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

PRIVACY AND DATA PROTECTION SUMMARY BY COUNTRY (6/7)

Country	Data Protection / Privacy Law	Data Protection Regulator	EU Adequacy Decision	Other Related Laws
Romania	GDPR	National Supervisory Authority for Personal Data Processing ('ANSPDCP')	N/A	Law No. 190/2018 Implementing the GDPR
Russia	Federal Law of 27 July 2006 No. 152-FZ on Personal Data	The Federal Service for Supervision of Communications, Information Technology, and Mass Media ('Roskomnadzor')	No	Federal Law of 27 July 2006 No. 149-FZ on Information, Information Technologies and Protection of Information ("Law on Information"), Federal Law of 21 July 2014 No. 242-FZ ('the Data Localisation Law')
Singapore	Personal Data Protection Act 2012 (No. 26 of 2012) ('PDPA')	Personal Data Protection Commission ('PDPC')	No	Cybersecurity Act 2018 (No. 9 of 2018)
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
South Africa	Protection of Personal Information Act, 2013 (Act 4 of 2013) ('POPIA')	The Information Regulator (not fully operational)	No	Regulations Relating to the Protection of Personal Information (2018)
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

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

Country	Data Protection / Privacy Law	Data Protection Regulator	EU Adequacy Decision	Other Related Laws
Switzerland	Federal Act on Data Protection 1992 ('FADP')	Federal Data Protection and Information Commissioner ('FDPIC')	Yes	
United Arab Emirates (UAE)	No country wide legislation	DIFC and Abu Dhabi Global Market (ADGM)	No	DIFC data Privacy law ADGM Data Protection Department of Health (DOH) Abu Dhabi's Abu Dhabi Healthcare Information and Cyber Security Standards (ADHICS)
United Kingdom	UK General Data Protection Regulation (Regulation (EU) 2016/679)	The Information Commissioner's Office ("ICO")	Yes	Data Protection Act 2018
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')

Detailed Country Updates for those where there have been notable changes or areas of specific Data Protection Authority focus

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

Adequacy Agreement with GDPR: Yes

Greg Reid
greid@bdo.com
+1 617 456-2582

Joelys Gonzalez-Mendez
jgonzalezmendez@bdo.com
+1 404 979-7108

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') also are part of Argentina's data privacy landscape.

Notable Changes

Legislatively, there have not been any substantial changes made to Argentina's current data privacy laws. Argentina attempted to draft a new data protection law following the passage of the GDPR, however, sweeping legislative changes are yet to occur.

In 2018, the Argentine Executive Branch proposed a draft privacy bill to replace the current Personal Data Protection Act, Act Not. 25.326 of 2000.[9] The purpose of the Bill was to update the current legislation to align with contemporary international standards. This bill would be an important tool for the country to maintain its adequacy standard. In 2020, the Bill lost its parliamentary status, and therefore, Congress cannot discuss it.[10]

Even with the loss of parliamentary status, the Argentinian Data Protection Authority ('AAIP') has not been discouraged regarding updating Argentina's data privacy landscape. The AAIP regularly updates the practical application and interpretation of the Data Protection Act through several dispositions and resolutions.

Data Protection Authority Focus

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 every week[11]. Most of these sanctions are for failure to register or renew a Database registration. Others pertain to unauthorised data processing, to not provide access, rectification, or suppression of the personal data of the data subject, not provide notice of the purpose of data collection, and not follow data protection rules.

[9] https://www.theworldlawgroup.com/writable/documents/news/Argentina-Data-Protection-Bill-2020.pdf

[10] https://www.lexology.com/library/detail.aspx?g=4451c1f8-53dc-49bc-8115-0fae0d65ca94, https://thelawreviews.co.uk/title/the-privacy-data-protection-and-cybersecurity-law-review/argentina

[11] https://www.linklaters.com/en/insights/data-protected/data-protected---argentina

AUSTRALIA

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

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

Adequacy Agreement with GDPR: No

Faith Page
faith.page@bdo.com.au
+61416207294

Since 22 February 2018, the 'notifiable data breaches' provisions of the Privacy Act require mandatory notification of all 'eligible data breaches to the OAIC and affected individuals. Ransomware and impersonation fraud are the leading concerns for Australia. From January to June 2021, there were 446 data breaches, of which 43% resulted from cybersecurity incidents[12].

Notable Changes

In December 2020, the OAIC called for several changes to the Privacy Act to ensure they remain "consistent with Australian values" and suitable for an increasingly digital world. The regulator stopped short of supporting GDPR style data regulation and consent management, as the government considers the most significant reforms to Australian privacy law in decades.

Australian Information Commissioner and Privacy Commissioner released the regulator's submission to the ongoing review of Australia's Privacy Act which includes 70 recommendations[13]. Primarily, the OAIC review includes:

- the scope and application of the Privacy Act, including the definition of 'personal information,' exemptions, and general permitted situations to collect, use and disclose personal information.
- the Privacy Act protects personal information and provides practice frameworks for promoting good privacy practices (e.g., notification, consent, overseas data flows, erasure).
- an individual should have the right to enforce privacy obligations.
- serious invasions of privacy allow for the introduction of torts.
- the impact and effectiveness of the Notifiable Data Breaches Scheme.
- the effectiveness of enforcement powers and mechanisms under the Privacy Act and the interaction with other regulatory frameworks.
- it is desirable or feasible to introduce an independent certification scheme and demonstrate compliance with Australian privacy laws.

From 1 July 2020, the consumer data right ('CDR'), introduced by amendments to the Competition and Consumer Act 2010 (Cth) and the Privacy Act, went live for limited data sharing concerning the four major banks (as the first part of the so-called 'open banking regime'). The rest of the banking data subject to CDR must be shared by those big four banks from **1 November 2020**. The CDR will then be rolled out progressively in the retail energy and telecoms sectors before, we expect, being rolled out across other sectors where there is significant consumer interaction and thus resulting consumer data.

[12] Australian Government, Office of the Australian Information Commissioner, Data breach report highlights ransomware and impersonation fraud as concerns

[13] Australian Government, Office of the Australian Information Commissioner, Privacy Act Review - Issues Paper

AUSTRALIA (CONTINUED)

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

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

Adequacy Agreement with GDPR: No

Faith Page
faith.page@bdo.com.au
+61416207294

Data Protection Authority Focus

The Privacy Commissioner enforces the Privacy Act/Australian Privacy Principles ('APPs'), including receiving and resolving complaints, undertaking own motion investigations, and because of any relevant determination, seeking an enforceable undertaking, publishing determinations/decisions, and issuing guidance in respect of the interpretation and enforcement of the Privacy Act/APPs. The Privacy Commissioner can also seek the imposition of a fine for a severe invasion of privacy or repeated invasions of privacy (i.e., repeated breaches of the APPs).

AUSTRIA

Law: Austrian Data Protection Act / Datenschutzgesetz

Regulator: Österreichische Datenschutzbehörde / Austrian Data Protection Authority

Adequacy Agreement with GDPR: n/a

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

In Austria, both the national DSG and the GDPR apply to privacy issues. The DSG complements the GDPR, tailors its provisions to the national context, and provides the legal basis for the structure and powers of the DSB. The DSB is an active authority and has issued substantial fines, including, for example, a fine of €18 million against the Austrian postal service for violating the GDPR. The DSB and the Austrian Chamber of Commerce ('WKO')[14] regularly issue guidance on privacy issues, including data subject access requests, cookies, direct marketing, and the right to be forgotten. Alongside the GDPR and the DSG, Austria also ratified the Convention for the Protection of Individuals about Automatic Processing of Personal Data ('Convention 108').

Notable Changes

The enforcement agency is taking a stronger position on transparency as evidenced by its recent lawsuits.

Data Protection Authority Focus

Austria recently announced that None of Your Business ('NYOB') reported in August 2021 that the DSB issued a decision following its complaint against the credit rating agency CRIF GmbH[15]. The DSB held that CRIF's credit assessment falls under 'profiling' because personal data was assessed and analysed to predict the data subject's future likelihood of credit default. The activities were deemed as intrusive interference with data subjects' rights. CRIF must inform the inquiring companies that the creditworthiness score of the consumer is calculated only based on address, gender, name, and age. The court also found that CRIF cannot rely on legitimate interests, Article 6(1)(f) under the GDPR because the data subject's interests should not be at a disadvantage in commercial transactions.

[14] Das Serviceangebot der Wirtschaftskammer, WKO

[15] BESCHWERDE GEMASS ARTIKEL, 77(1), 80(1), DSGVO, NOYB

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')

Adequacy Agreement with GDPR: n/a

Alain Vanmeerhaeghe
alain.vanmeerhaeghe@bdo.be
+32497644213

Notable changes

The Belgian Data Protection Authority (DPA) has played an active role in implementing new regulations and measures to fight against COVID-19 while assuring continued protection for citizens' personal data, according to the applicable legislation. The DPA has underlined that public health is of the most significant importance and that its preservation is not incompatible with the right to privacy.

The DPA kept a close watch on the measures taken by the Belgian government and voiced concerns on several occasions. Indeed, 'Tracking' to protect public health touches on two key priorities of the DPA: sensitive (medical) data on the one hand and government processing of data on the other hand.

Data Protection Authority Focus

In 2020 data breaches increased by 21% versus 2019 in Belgium (1,060 breaches vs. 838 breaches), and DPA fines included €835,500, including two significant penalties in 2020[16].

In September 2020, Google received the largest fine to date from the Belgian DPA, €600,000 ($670,000)[17].

A Belgian citizen (the complainant) requested Google Belgium to remove search results linked to his name in their search engine (information related to political party and unfounded harassment complaint). Google decided not to remove any of the pages in question. The DPA ruled that Google was particularly negligent, as it had evidence that the information was outdated and irrelevant. Google Belgium appealed the decision.

This decision is historic because the fine was more than ten times higher than any previous fine imposed by the DPA, and because it ensures that the full and effective protection of citizens is maintained in cases of large international groups, such as Google.

In May 2020, Proximus received a fine of €50,000 ($57,900) for a conflict of interest of its DPO. As Head of Compliance, Risk Management & Internal audit, he played a role in both the advisory role and the decision-making process around data issues. By prohibiting this dual role, the GDPR prevents conflicts of interest.

[16] GDPR Enforcement Tracker

[17] Compliance Week, Google fined $670K for violating GDPR's 'right to be forgotten', 14 July 2020

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) Adequacy Agreement with Adequacy

Agreement with GDPR: No

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

Notable changes

The LGPD passed in 2018 and went into effect in 2020. Enforcement began on August 1, 2021. The comprehensive law covers the activities of data controllers and processors. The law requires companies to:

- Appoint a Data Protection Officer.
- Conduct Data Protection Impact Assessments ('DPIAs').
- Notify individuals of a data breach.
- Evaluate data transfers and the adequacy of third-country company controls.

On August 10, 2021, the President of Brazil appointed the National Council for the Protection of Personal Data and Privacy ('CNPD') of the ANPD board members and surrogates.

The LGPD plays a significant role for the ANPD. The ANPD ensures that personal data is protected under the LGPD (Article 55-J-I) and issues technical opinions and guidance (Article 55-J-XX), education (Article 55-J-VI), enforcement (Article 55-J-IV), complaint handling (Article 55 J-V), international facilitation (Article 55 J-IX), and drafting and updating rules and regulations (Article 55-J-XIII)[18].

Brazilian companies focus on the improvement of their data governance environments, which were previously non-existent for many of them.

[18] Centre for Information Policy (CIPL) and Centro de Direito, Internet e Sociedade of Instituto Brasiliense de Direito Público (CEDIS-IDP), The Role of the Brazilian Data Protection Authority (ANPD) under Brazil's New Data Protection Law (LGPD), April 2020

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

Agreement with GDPR: No

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

Data Protection Authority Focus

The ANPD has not yet issued guidance to companies, but under Articles 9 and 6(IV) of the LGPD data subjects have the right to be informed concerning the processing of their personal data. However, the timing is unclear. Generally, data subjects have a right to access the specific purpose of the processing.

- type and duration of the processing;
- identity and contact information of the data controller;
- data shared by the controller and the purpose for sharing; and,
- data subject's rights, which is outlined in Article 18.

When a company changes the purpose of processing, consent is required under Articles 7 and 11 if the processing is not consistent with the original intent. Data subjects must be informed of these changes and have the right to revoke consent if the individual disagrees with the new purpose (Articles 8(6) and 9(2).

Under Article 18 of the LGPD, the data subject can receive:

- confirmation of the existence of processing;
- access to the data;
- information about public and private entities with which the controller has shared data; and,
- information about the possibility of denying consent and the consequences of such denial.

Data subjects also have a right to correct incomplete, inaccurate, or outdated information (Article 18(III)), and the data controller must notify the data subject of these corrections.

Interestingly, the LGPD does not explicitly require identity verification before fulfilling data subject requests, nor does the LGPD need companies to comply within a specified timeframe.

With the development of the CNPD, we believe that the LGPD will continue to evolve, and enforcement actions will continue to increase.

BULGARIA

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

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

Adequacy Agreement with GDPR: n/a (we are part of the EU)

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

Notable changes

Bulgaria revised its local National Personal Data Protection Act ('PDPA') in 2019, following the inception of the GDPR. The Bulgarian Commission for Personal Data Protection (the authorised supervising body under GDPR) conducted several audits on larger companies processing personal data under its self-referral or due to signals by data subjects. Audits resulted in fines for identified violations, and the size of the penalties is proportional to the seriousness of the offenses.

Data Protection Authority Focus

The focus of the Bulgarian DP Authority, namely the Commission for Personal Data Protection (CPDP), is mainly guidance and decisions under complaints. The CPDP recently stated the legality of personal data processing by the Ministry of Interior during the COVID-19 crisis. In particular, the Statement highlights that the Ministry's collection of declarations from citizens passing through checkpoints around Bulgaria is a temporary measure and concerns a limited number of persons whose data are processed. Personal data protection legislation allows for limiting the scope of rights and freedoms of citizens (Article 23, GDPR, Regulation (EU) 2016/679) and that the Ministry's personal data processing is necessary and proportionate to guarantee public health and crime prevention.

CANADA

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

Regulator(s): 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

Adequacy Agreement with GDPR: Yes

Vivek Gupta
vgupta@bdo.ca
+1 (416) 369-7867

Notable changes

The primary federal Canadian privacy laws are the Personal Information Protection and Electronic Documents Act ('PIPEDA') and the Privacy Act. PIPEDA applies to organisations that conduct commercial activities, while the Privacy Act applies to federal government bodies.

On 17 November 2020, Bill C-11 for the Digital Charter Implementation Act, 2020 ('DCIA') was introduced to the House of Commons. It would reform Canada's federal private sector privacy laws by enacting the Consumer Privacy Protection Act and the Personal Information and Data Protection Tribunal Act. The passing of this law would significantly provide more protection to Canadians' personal information. It would provide Canadians more control and greater transparency into handling their personal data by commercial organisations. The law also provides significant consequences for non-compliance, including steep financial penalties for violations.

Other relevant laws include the Bank Act 1991, Canada's Anti-Spam Legislation 2010, and the Proceeds of Crime (Money Laundering) and Terrorist Financing Act 2000. It is also important to remember that data protection requirements vary between provinces and territories.

Data Protection Authority Focus

Under the CPPA, the Privacy Commissioner would have broad order-making powers, including forcing an organisation to comply with its requirements under the CPPA and the ability to order a company to stop collecting data or using personal information. In addition, the Privacy Commissioner would also be able to recommend that the Personal Information and Data Protection Tribunal impose a fine. The legislation would provide administrative monetary penalties of up to 3% of global revenue or $10 million for non-compliant organisations. It also contains an expanded range of offences for certain severe contraventions of the law, subject to a maximum fine of 5% of global revenue or $25 million[19].

[19] IAPP, Federal privacy reform in Canada: The Consumer Privacy Protection Act

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(s): Office of the Ombudsman

Adequacy Agreement with GDPR: n/a

Richard Carty
rcarty@bdo.ky
+13459281120

Notable changes

The Data Protection Act and the Data Protection Regulations established multiple data subject rights when it went into effect in 2019. Data subjects gained the right to access, rectification, the right to be informed, the right to file a complaint, and the right to seek compensation for violations. In September 2021, the Ombudsman issued additional guidance for data subjects to seek compensation for violations. In this guidance on monetary penalty order ('MPO'), Section 55 grants the Ombudsman the ability to issue an MPO not exceeding $250,000. Section 56 outlines additional guidance on when the Ombudsman can seek the MPO. The direction elaborated on factors contributing to the fines – a breach severity assessment tool and a matrix for monetary penalty calculations.

On 14, July 2021 the Ombudsman released its annual report, which outlined the 87 data breaches reported in 2020 and that the number of data protection complaints doubled during 2020 compared to 2019[20]. In the report, the Ombudsman highlighted the following.

- Data protection complaints doubled from 12 in 2019 to 25 in 2020[21].
- The Ombudsman focused on resolving complaints about government maladministration (seven in 2019 to 18 in 2020). Government maladministration includes but is not limited to delays in action, incorrect action, failure to take action, failure to provide information, inadequate record-keeping, failure to investigate, misleading or inaccurate statements, or broken promises[22].
- The first enforcement order under the DPL required the Registrar to 'immediately collect and process personal data of non-registrable persons because there was no legal basis[23]'.
- Investigators and analysts obtained their certification as mediators and received other credentials to continue to enhance the ability to respond to data protection complaints.

Between 2019 and 2020 there was a reduction in overall inquiries (393 in 2019 and 332 in 2020)[24].

	2019	2020
Freedom of Information Act	45	60
Data Protection	120	192
Whistleblower Protection	6	2
Police Complaints	52	33
Maladministration	109	106

[20] Ombudsman, Cayman Islands, Annual Report, 2021

[21] Ibid.

[22] Oxford Reference, Overview – Maladministration

[23] Ombudsman, Cayman Islands, Annual Report, 2021

[24] Ibid.

CAYMAN ISLANDS (CONTINUED)

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

Regulator(s): Office of the Ombudsman

Adequacy Agreement with GDPR: n/a

Richard Carty
rcarty@bdo.ky
+13459281120

Data Protection Authority Focus

Since the enforcement of the Data Protection Law in the Caymans on 18 September 2019, the Ombudsman office has been more focused on public comments and guidance. Due to the complexity of the business structures in the Cayman market and the cultural norms in the Caribbean, the Ombudsman saw greater value in supporting the business environment in their endeavours and achievements to comply with the DPL instead of issuing fines or judgement when a failure or non-compliance was identified.

CHINA

Law: Personal Information Protection Law, Data Security Law

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

Adequacy Agreement with GDPR: 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 20 August 2021, China passed the PIPL – its first comprehensive data protection legislation. China begins enforcement on 1 November 2021. The law established personal information processing rules, data subject rights, and obligations for personal information processors. Additionally, on 10 June 2021 the National People's Congress of the People's Republic of China ('NPC') approved the Data Security Law, which entered enforcement on 1 September 2021. Other laws the take personal data protection into account include the Cybersecurity Law of 2016 and the Standard GB/T 35273-2020 on Information Security Technology – Personal Information Security Specification.

Operators that collect, analyse, store, transmit, query, utilize, delete, and provide personal information or important information overseas during the design, production, sales, operation and maintenance, and management of automobiles within the territory of the People's Republic of China.

Organisations must comply with relevant laws and regulations and the requirements of the regulation. Using local data storage to separate the China local data from other countries is recommended. Proper separation of duties should be implemented over the system and data access as a matter of standard appropriate risk management approaches.

China has recently, over the past year, liberalised the use global crypto technologies by companies operating within their borders. And new regulations require or recommend the encryption of certain personal information for commercial purposes, with specific focus on Blockchain and quantum encryption methods.

Some ambiguities exist in this new regulation, as well:

- Older, more restrictive regulations have not been phased out yet.
- Commercial encryption that involves 'national security or the societal public interest' requires an import permit.
- 'Critical Information Infrastructure' (CII) vendors require security reviews of encryption, but without specific goal points.

Companies are still required to produce data for the government upon request, irrespective of whether the data is encrypted or not.

In summary, while China is attempting to security PI and other sensitive data from cybercriminals, individuals and companies should understand that these security and cryptography techniques are not to be designed to thwart access by their government.

CHINA (CONTINUED)

Law: Personal Information Protection Law, Data Security Law

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

Adequacy Agreement with GDPR: 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

China does not have one specific law dealing with the protection of employee data, but they have two overarching laws: Labour Contract Law of the People's Republic of China and Information Technology – Personal Information Security Specification (GB/T 35273-2017).

Generally, these laws require companies to:

- Applies to prospective employees collected by the employer and is limited to data directly connected to the Labour contract (e.g., age, gender, work experience, educational background)
- Applies to other pre-employment data, when necessary (e.g., health, criminal background)
- Employers must expressly state the purpose, means, and scope of the collection and use of personal data
- Consent must be obtained from the candidate or employee
- If the data is stored on a local network, then the company is considered a network operator
- Employers should notify applicants if background checks are conducted
- Retain personal data for the shortest time frame necessary to realise the purpose of the personal data
- Under the PRC Labour Contract Law, employer shall keep copies of rescinded or terminated Labour contracts for at least two (2) years for inspection purposes

Employer should carry out deletion or anonymisation after the required necessary retention period expires

- For personal information handlers (e.g., the employer) who need to provide personal information (of the employees') outside of (mainland) China for business or other purposes, the PIPL provides three mechanisms for export (i.e., cross-border data transfer):

  1. Conducting a security assessment organized China's cybersecurity authority.
  2. A standard contract as determined by China's cybersecurity authority (like a GDPR standard contractual clause).
  3. Obtaining a Personal Information Protection Certification from a qualified agent.
  4. Personal Information handler must provide the data subject with notification of expert and obtain their consent.

CHINA (CONTINUED)

Law: Personal Information Protection Law, Data Security Law

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

Adequacy Agreement with GDPR: 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

Data Protection Authority Focus

The focus of the CAC is to provide data protection to its citizens and requires companies to comply with its obligations.

- On 16 September 2021 the revised Law on Protection of Minors went into effect. The law requires the protection of privacy and personal information for minors. Information handlers that process data through the Internet must follow principles of lawfulness, justification, and necessity. This applies to the processing of information for minors under the age of 14.
- On 15 September 2021 the Provincial Communications Administration of Quinghai announced that it organised a special campaign to rectify camera network security in the information and communications industry across the province. They goal is to combat violations of laws and regulations such as the use of camera security violations that infringe on citizens' personal privacy.
- On 10 September 2021 the National Information Security Standardisation Technical Committee of China ('TC260') solicited participants for five national standards – Privacy Protection Information Technology Security Evaluation Guideline, Big Data Service Security Capability Requirements, and the authentication requirements for mechanisms using a cryptographic check function and technology based on cryptographic tokens.

Fines for violators of the PPL are up to 50 million Yuan (about $7.7 million) or 5% of annual revenue. The law goes into effect on 1 November 2021 and BDO believes that this will be the focus of the CAC.

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(s): Colombian Data Protection Authority ('SIC')

Adequacy Agreement with GDPR: No

Paula Giraldo Gutierrez
pgiraldo@bdo.com.co
+573173311331

Notable changes

On 16 July 2021, the Ibero-American Data Protection Network ('RIPD') announced that SIC updated the implementation guide for international transfers of personal data. The guide contains specialised recommendations for cross-border data transfer about the rights of data subjects' information sent to third countries. The goal is to improve its content and consider the Implementing Decision (EU) 2021/914 regarding standard contractual clauses ('SCCs') for the transfer of personal data to third countries.

The updates recommend companies to:

- Incorporate privacy, ethics, and security by design and default into their practices.
- Carry out Privacy Impact Assessments before transferring data to a third country.
- Ensure compliance to comply with accountability obligations.
- Articulate the accountability mechanisms in a contract are specific to each transfer.
- Establish accountability measures when transferring data.
- Replicate proactive measures for the processing of data for international transfers of personal information.

The RIPD implemented SIC Facilita, an alternative dispute resolution mechanism between data controllers and data subjects. The SIC Facilita is a virtual tool where the SIC acts as a facilitator to allow data subjects and controllers to agree on claims. The SIC highlights the following benefits of the SIC Facilita.

- Resolve data privacy complaints quickly.
- Reduce costs, resources, and human capital associated with resolving data privacy complaints.
- Reduce risks for organisations to resolve judicial or administrative conflicts over data subject rights.
- Increase levels of satisfaction and trust between the data subject and the company.

Data Protection Authority Focus

The SIC ensures the protection of the consumers' rights and is responsible for 'inspecting, monitoring, and controlling market agents so that the rights and interests of consumer are not violated when the commercial exchange has been made[25]'.

The focus of SIC is to investigate complaints and violations of Colombia's data subjects' data privacy, and data protection rights and ensure the protection of consumers' rights. The primary focus of the SIC is on the protection of consumers from health and safety hazards, access to personal information, education, freedom to build consumer organisations, and the protection for children's data[26].

[25] Superintendencia de Industria y Comercio, International Community, Consumer Protection

[26] Ibid.

CZECH REPUBLIC

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

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

Adequacy Agreement with GDPR: n/a

Stanislav Klika
stanislav.klika@bdo.cz
604226734

Notable changes

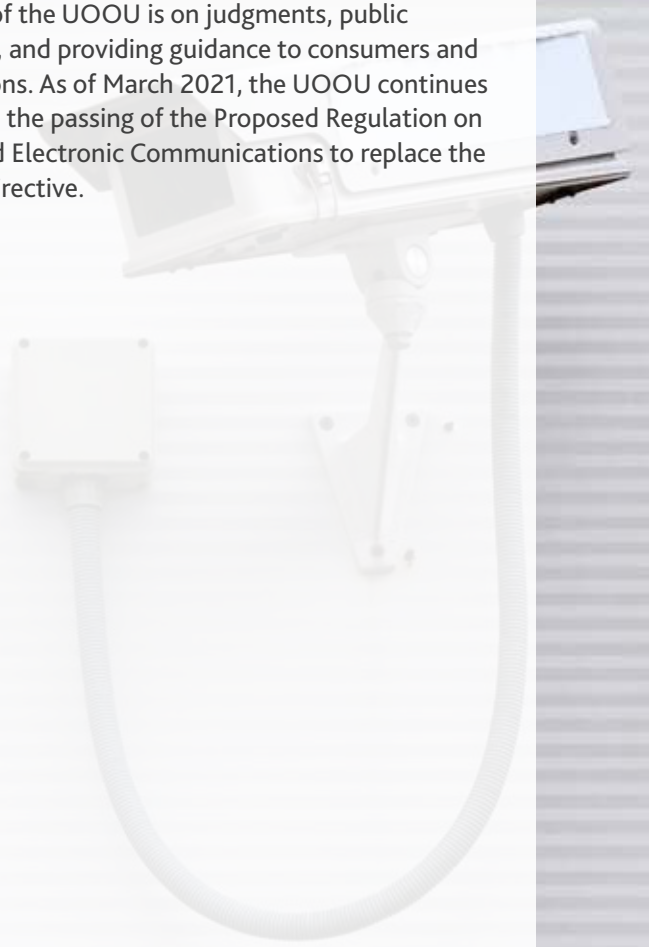
The Act No. 110/2019 Coll. on Personal Data Processing ('the Act') is the primary privacy regulation in the Czech Republic that transposes the GDPR. The UOOU performs audits, publishes Standard Contractual Clauses (SCCs), investigates data breach complaints, and imposes fines. Act No. 127/2005 Coll. of 22 February 2005 on Electronic Communications and on Amendment to Certain Related Acts implements the ePrivacy Directive. The derogation from the GDPR is that the Czech law maintains the 'opt-in' consent obligation versus the GDPR 'opt-out' requirement.

On 15 September 2021 the Chamber of Deputies overruled the Senate and approved the transposition amendment to the Act No. 127/2005 on electronic communications and on Amendment of Certain Related Acts.

On 20 September OneTrust DataGuidance confirmed that the draft of the whistleblowing implementing act in the Czech Republic and the Chamber of Deputies will not proceed to a second round of discussions[27]. It is possible that this act could pass later but will not pass prior to the elections in October 2021.

Data Protection Authority Focus

The focus of the UOOU is on judgments, public comments, and providing guidance to consumers and organisations. As of March 2021, the UOOU continues to focus on the passing of the Proposed Regulation on Privacy and Electronic Communications to replace the ePrivacy Directive.



[27] OneTrust DataGuidance, Czech Republic: Legislative process on whistleblowing transposition law discontinued, September 2021

DENMARK

Law: The Danish Act on Supplementary Provisions, GDPR

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

Adequacy Agreement with GDPR: n/a

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

Notable changes

Datatilsynet is the Danish regulator that is active in publishing GDPR guidance. The Datatilsynet works with other supervisory authorities, the Centre for Cybersecurity, and the Danish Business Authority, for cybersecurity, cookies, and telecommunications security.

Denmark was the first EU country to publish Standard Contractual Clauses ('SCCs') for contracts between data controllers and data processors in accordance with Article 28 of the GDPR.

Data Protection Authority Focus

The Datatilsynet focuses on monitoring data processors and sub-processors and ensuring that companies have a legal basis for data processing and storage.

On 22 September 2021, Datatilsynet announced that the Tax Authority's notification of a data security breach violated Article 24(1) of the GDPR for failing to notify the data subjects of the data breach promptly. The 2020 data breach that exposed 1.26 million Danish citizen ID numbers and resulted from a software error that lasted for five years resulted in the notification of data subjects 40 days after learning of the breach.

On 21 September 2021, Datatilsynet announced that Falck Danmark A/S' ('Falck') processing of personal data about COVID-19 testing of primary school students followed the GDPR. Falck's processing and privacy policy transparency complied with Articles 12(1) and 13 of the GDPR.

On 16 September 2021, Datatilsynet announced that it recommended a DKK 75,000 fine for Favrskov Municipality's security failure. The police failed to implement sufficient technical security measures to safeguard data subject's personal data confidentiality. The breach resulted from a stolen laptop, which contained a program with the personal data of approximately 100 people with reduced physical or mental capacity. More importantly, the computer was not encrypted, and the program containing the information was not equipped with proper safeguards, which violated Article 32 of the GDPR.

FINLAND

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

Regulator(s): Office of the Data Protection Ombudsman

Adequacy Agreement with GDPR: 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 due to data leaks published for the public interest.

There have been a few significant data leaks in Finland. In particular, the Vastaamo Psychotherapy hack of psychotherapy records resulted in the exposure of at least 2,000 patients and their therapist records landing on the 'dark web.' Patients reported receiving emails with a demand for €200 in bitcoin to prevent the contents of their discussions with therapists from being made public[28]. Another report indicates that the ransomware attackers requested 40 bitcoins worth about €450,000 from the company and between €200 and €500 from patients[29].

The event woke up both private individuals and companies to think about their data protection and security level.

Privacy data auditing is even more involved in auditing assignments. Interest is also only for data protection-specific auditing tasks.

Public administration organisations that are clients of internal audits are subject to regular data protection audits.

Data Protection Authority Focus

The data protection authorities have made decisions based on the notifications made by private individuals. One prominent industry, which has been the subject of decisions, is the real estate industry. Example decisions include the location data, where an inhabitant has used electronic key, legal to register or not. Due to the incorrect installation of the around ten taxi CCTV camera software, the system recorded the image and the speech. The DPA has taken it as a precedent, and a fine of 70,000 euros was imposed for the error. The DPA's decision is in the legal process, and the DPA has also paid attention to data protection impact assessment.

[28] The Guardian, 'Shocking' hack of psychotherapy records in Finland affects thousands, 26 October 2020

[29] Euroactiv, Huge data breach in Finland shocks citizens and politicians alike, 26 October 2020

FRANCE

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

Regulator(s): French Data Protection Authority ('CNIL')

Adequacy Agreement with GDPR: n/a

Bruno Saucourt
bruno.saucourt@bdo.fr
+33686282959

Notable changes

In France, amendments and supplements to local legislation came into force after revising the national law known as «Loi Informatique et Liberté» in June 2018. The decree published on May 30, 2019, is the last step in bringing federal law into compliance with the General Data Protection Regulation (GDPR) and the Police-Justice Directive, applicable to files in the criminal sphere. The national legal framework for data protection is stabilised.

The Act and its Implementing Decree, which had undergone a significant overhaul, now allow both individuals and data processing organisations to understand their rights and obligations more clearly about personal data protection.

Data Protection Authority Focus

The supervisory authority in France, the CNIL, has an important educational role by signing agreements with administrations and organisations to promote personal data protection.

Penalties imposed because of controls shall be proportionate. In early 2021 the CNIL fined an undisclosed data controller €150,000 and the data processor €75,000 for the failure to implement adequate security measures[30]. The lack of security lead to a credential-stuffing attack[31] resulting in the leak of last name, first name, email address, date of birth, loyalty card balances, and orders for approximately 40,000 individuals.

The supervisory authority provided guidance concerning:

- COVID-19 tracking applications
- Human resource treatments and data retention
- Cookies
- Chatbots
- Video surveillance
- List of treatments for which a Privacy Impact Assessments ('PIA') is required
- List of treatments exempt of PIA

In June 2021 CNIL released PIA tool. More information is available on the CNIL website. Two versions exist, a portable version and an open source web version.

[30] JDSUPRA®, France's CNIL Fines Data Processor and Data Controller over Credential-Stuffing Attack, 4 February 2021

[31] Credential-stuffing is an attack method where hackers use compromised credentials to breach a system.

GEORGIA

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

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

Adequacy Agreement with GDPR: No

Anzor Mekhrishvili
amekhrishvili@bdo.ge
+995598212007

Notable changes

Georgia adopted the Data Protection Act in 2011, which governs data protection and processing activities. The Law of Georgia on State Inspector Services (N3273-RS, 21.07.2018) and the Resolution of the Government of Georgia on the Approval of Regulations on the Activities of the Personal Data Protection Inspector and the Rule of Exercising the Power by him/her (n 180, 19.07.2013) provide the regulatory framework for Georgian data protection. 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[32]'. 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[33].

Data Protection Authority Focus

The focus of PDP is to provide guidance to Georgian companies around:

- Data processing
- Violations of data processing principles
- The development and use of artificial intelligence
- Failure to comply with data protection requirements
- The use of data for direct marketing
- Violations related to video surveillance
- Processing special categories of data

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 non-compliance.

[32] Georgia Technology Authority, General Data Protection Regulation (GDPR) Guidance

[33] Georgia State Inspector's Service, 2 Years Since the Enforcement GDPR and Its Impact on Georgia. 25 May 2020

GERMANY

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

Regulator(s): 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')

Adequacy Agreement with GDPR: n/a

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

Notable changes

Together with the GDPR, the revised Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG) came into force on 25 May 2018. The BDSG elaborates on the GDPR, particularly regarding the figure of Data Protection Officer, as well as employee data protection. In mid-2019, the BfDI announced an amendment to the BDSG, which applied corrections and adaptations to the current BDSG and more than 150 other national laws. While the German data protection authorities acted cautiously in 2018, they announced more robust controls for 2019. Nevertheless, the fines have been low compared to other countries in the EU. In the late summer of 2019, the German data protection authorities announced a new sanctioning model that could lead to higher fines in the future.

Data Protection Authority Focus

Until recently the highest penalty in Germany was almost 200,000 EUR (2019). However, on 24 September 2021, the Hamburg Commissioner for Data Protection and Freed of Information ('HmbBfDI') announced that it had fined Vattenfall Europe Sales GmbH €901,388.84 (about $1 million) for violating the data protection transparency obligations under Articles 12 and 13 of the GDPR. HmbBfDI noted that nearly 500,000 customers were not appropriately informed about the internal data comparison relating to contract inquiries for special contracts that were associated with special bonus payments.

Schrems II Decision of ECJ of the last year has still a significant shakeup for the transatlantic data transfer. In its judgment of 16 July 2020, the ECJ found the privacy shield agreement between the EU and the United States to violate European data protection law. At the time of the decision, the privacy shield agreement was the basis for a vast part of transatlantic data transfer and used by virtually all major providers such as Google, Facebook, and Microsoft. As a result of the Court´s decision, EU companies can no longer legally transfer data to the US-based Privacy Shield framework. Companies that do not comply with this ruling and continue to transfer data based on an invalidated mechanism (e.g., Privacy Shield) risk a penalty of €20 million or 4% of global turnover.

The Court of Justice of the European Union (CJEU) left the only basis for US transfers to conclude standard contract clauses set up by the European Commission. The EJC now requires additional technical and organisational safeguards on top of the standard contractual clauses. At present, the local Data Protection Authorities have begun to investigate whether local businesses have implemented these new requirements. The fines issued by German DPAs mainly concern data breaches and the criteria to delete personal data in time.

GUERNSEY

The Data Protection (Bailiwick of Guernsey) Law, 2017

Adequacy agreement with the GDPR: Yes

Steve Desmond
Steve.desmond@bdo.gg
+447781124243

Notable changes

Whilst there has been little change to legislation over the last 12 months, as a result of BREXIT, there was an intermediate law recognising the UK as an equivalent jurisdiction prior to the EU extending this recognition in 2021.

During 2020, the States of Guernsey, (the islands government) approved a self-funding model for the Office of the Data Protection Authority (ODPA) effective from the 1st January 2021. This means that the ODPA costs are met by annual fees paid by the regulated community, including the States of Guernsey who are a Data Controller in their own right. This widened the net for qualifying data controllers including clarification for those entities that were not domiciled on the island but by way of processing qualified as being "established in the Bailiwick" as well as introducing the concept of a "Levy Collection Agent" for administered companies.

Data Protection Authority Focus

The ODPA has been active during the Covid pandemic in providing guidance to firms in how to process information such as Special Category Data, vaccination status for example and working from home policies and procedures. Education and training are also key factors.

In terms of enforcement, there have been several in the last 12 months, some specific ones; A law firm who sent files to the correct email address where these attachments contained highly confidential and sensitive personal details relating to the complainant. The complaint was upheld on the basis the email address was also available to unconnected third parties who unwittingly accessed the files unaware of the confidential nature of the contents. A government body and a large retail commercial store reprimanded for failure to disclose information within the statutory timeframe following a request. An enforcement order on the Guernsey Police, who shared information on a vulnerable individual with two professional teams without consent. Whilst this was arguably in the best interest of the individual concerned, it was upheld the Police were unable to provide the basis of how the processing was compliant with the law. Clearly mitigating factors in this case, but emphasises procedures need to be in place to deal with these difficult issues.

HONG KONG

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

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

Adequacy Agreement with GDPR: No

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

Notable Changes

The Personal Data (Privacy) Ordinance ('PDPO') was passed in 1995 and took effect from December 1996 (except for specific provisions). It is one of Asia's longest-standing comprehensive data protection laws. It has its origins in the August 1994 Law Reform Commission Report entitled Reform of the Law Relating to the Protection of Personal Data[34]. The reform recommended that Hong Kong introduce a new privacy law based on the OECD Privacy Guidelines 1980 to ensure adequate data protection to retain its status as an international trading centre and affect human rights treaty obligations.

In September 2021, the PCPD published frequently asked questions ('FAQs') and answers regarding the European Commission's Standard Contractual Clauses ('SCCs') for the transfer of data from the EU to non-EU regions. The FAQs focused on the implementation framework of the new SCCs and third-country party obligations. The PCPD stated, 'The New SCCs will be relevant to a local entity in Hong Kong if the obligations under the GDPR apply to it as an exporting party on an extra-territorial basis'[35].

Data Protection Authority Focus

The PDPO applies to both the private and the public sectors, and it is technology-neutral and principle-based. The Data Protection Principles ('DPPs' or 'DPP'), contained in Schedule 1 to the PDPO, outline how data users should collect, handle and use personal data, complemented by other provisions imposing further compliance requirements.

Principles of PDPO include DPP1 Purpose and Manner of Collection; DPP2 Accuracy and Duration of Retention; DPP3 Use of Data; DPP4 Data Security; DPP5 Openness and Transparency; DPP 6 Access and Correction. Contravention of a DPP is not an offence, and however, contravention of specific provisions of PDPO is an offence.

In September 2021, the Kowloon City Magistrates' Court convicted an estate agent for violating the PDPO (Cap. 486). The estate agent called a data subject months after he opted out and requested that no further direct marketing calls be made to them. The estate agent received a fine of HK$15,000 (approximately €1,631 or $1,927). While this is a relatively small penalty, individuals need to understand that they are responsible for protecting data subjects' privacy.

Contravention of an enforcement notice issued by the Privacy Commissioner for Personal Data is also an offence that may result in a maximum fine of **HK$50,000** and imprisonment for two years.

Subsequent convictions can result in a maximum penalty of **HK$100,000** and imprisonment for two years.

[34] Logon Software & Services, Hong Kong's Personal Data (Privacy) Ordinance PDPO

[35] The Office of the Privacy Commissioner for Personal Data, Understanding the European Commission's New Standard Contractual Clauses for Transfer of Personal Data from EU to Non-EU Regions, September 2021

INDIA

Law: (Pending) Personal Data Protection Bill, 2019

Regulator(s): The Data Protection Authority of India (Central Government)

Adequacy Agreement with GDPR: No

Saumil G Shah
saumilgshah@bdo.in
+919900079563

Notable changes

In 2017 the India Supreme Court declared privacy a fundamental right because of the Puttaswamy case[36]. In 2018, the Government released a draft Personal Data Protection Bill, which is derived from the GDPR. A revised bill was proposed in 2019 and was introduced to the lower house of the Indian Parliament. India originally planned to pass that bill in 2020, but delays have been encountered.

India is awaiting the approval of the Personal Data Protection Bill (PDPB) in parliament. Once approved and enacted, the privacy laws in India will take a dramatic change, like those of GDPR or CCPA or equivalent privacy laws. Data protection awareness is increasing drastically in India, especially after digital transformation and the digital payment ecosystem.

India is also home to Aadhaar, the world's most extensive biometric ID system. Indian citizens use Aadhaar cards to access various services, such as opening bank accounts, obtaining mobile SIM cards, and government welfare schemes. The voluntary use of Aadhaar was upheld in 2019 when a law was passed allowing for the voluntary use of Aadhaar.

Data Protection Authority Focus

The PDPB underwent public, and industry comments and is awaiting parliament review and enactment. Due to the COVID-19 pandemic, delays occurred.

[36] In the Supreme Court of India, Civil Original Jurisdiction, Writ Petition (Civil) No. 494 of 2012, Justice K.S. Puttaswamy (Retd.) and another (Petitioner) versus Union of India and Others (Respondents)

IRELAND

Law: Data Protection Act 2018, GDPR

Regulator(s): Data Protection Commission ('DPC')

Adequacy Agreement with GDPR: n/a

David McCormick
DMcCormick@bdo.ie or DPO@BDO.ie
00353 1 4700000

Notable changes

There have been no significant changes to legislation. However, new guidance in the use of cookies and tracking technologies was published. The Data Protection Commission 'DPC' conducted an extensive public awareness campaign signalling its intention to begin follow-up enforcement action during Q4 of 2020. Enforcement Notices were served on seven organisations for non-compliance in December 2020.

The Irish Data Protection Commission (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 based in Ireland but operating across the European Union.

IRELAND (CONTINUED)

Law: Data Protection Act 2018, GDPR

Regulator(s): Data Protection Commission ('DPC')

Adequacy Agreement with GDPR: n/a

David McCormick
DMcCormick@bdo.ie or DPO@BDO.ie
00353 1 4700000

Data Protection Authority Focus

In 2020 the DPC issued its first fine in a cross-border case and was the first supervisory authority in the European Union to use the GDPR dispute resolution process. In December 2020, the DPC issued a decision to Twitter regarding the notification and documentation of a personal data breach (Articles 33(1) and 33(5) GDPR). This decision provided a critical analysis of the data breach notification and documentation requirements imposed on organisations by Article 33 GDPR, which requires the notification of personal data breaches within 72 hours. The DPC found that Twitter delayed its reporting and failed to document the personal data breach adequately. Twitter had argued that the delay in notification was due to an internal delay in the breach notification to its own Global Data Protection Officer. The DPC disagreed, pointing out that a failure of internal processes does not justify a delay in reporting.

As part of the GDPR dispute resolution process (Article 65), the draft decision submitted to other EU supervisory authorities was the first draft decision in a 'big tech' case. It was the firm all EU Supervisory Authorities were consulted. The European Data Protection Board ('EDPB') adopted the DPC's decision and issued a final decision to Twitter in December 2020. The decision imposed an administrative fine on Twitter.

The DPC has also provided a draft decision to its EU counterparts 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. A final decision is expected near the end of 2021.

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

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(s): Italian Data Protection Authority ('Garante')

Adequacy Agreement with GDPR: n/a

Stefano Minini (partner)
stefano.minini@bdo.it
Luigi Sasso (Legal Manager)
luigi.sasso@bdo.it

Stefano Minini
+393346829871
Luigi Sasso
+393392222014

Notable changes

At the end of 2018, Italy amended the Personal Data Protection Code to adapt to the GDPR.

As far as the business environment in Italy is concerned: 2021 is mainly focused on fine-tuning privacy compliance frameworks at the corporate level and deploying them to sister companies abroad.

In September 2021, the Garante adopted body cameras by two law enforcement agencies (i.e., state police, national military police). Use limits were imposed, especially concerning facial recognition and the implementation of security measures. The State Police and National Military Police conducted Data Protection Impact Assessments ('DPIAs'). They agreed to limit the recording time, disallow unique facial recognition identification, and limit activation to document situations of concrete and 'real' danger for the public or criminal offences.

Following other prominent Data Protection Authorities (e.g., France CNIL, Spain AEPD, Denmark Datatilsynet) and the European Data Protection Board ('EDPB') in July 2021, the Garante launched an informational page on cookies use to protect users' personal data when browsing online. The Garante identified a six-month deadline for Italian companies to comply with the new guidance[37].

[37] GPDP, Garante per la Protezione Dei Dati Personali, Linee guida cookie e altri strumenti di tracciamento - 10 giugno 2021 [9677876], 10 July 2021

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(s): Italian Data Protection Authority ('Garante')

Adequacy Agreement with GDPR: n/a

Stefano Minini (partner)
stefano.minini@bdo.it
Luigi Sasso (Legal Manager)
luigi.sasso@bdo.it

Stefano Minini
+393346829871
Luigi Sasso
+393392222014

Data Protection Authority Focus

The Garante focuses on technology, telecommunications, multi-utility, and sanitary industries in terms of control activities. Significant sanctions of more than **€20 million** have been applied mainly for undue telemarketing activities in the past months.

In September 2021, Garante fined the Region of Lombardy **€200,000** for publishing personal data of more than 100,000 students on the institution's website[38]. The students requested state scholarships and economic subsidies to purchase of textbooks, technological equipment, and teaching tools. The Garante found that the data published lacked a legal basis and violated Article 6 of the GDPR and Article 5(1)(a) and (c) for publishing data revealing economic hardship.

In September 2021, the Garante fined the Municipality of Rome **€800,000** for several privacy violations about to parking metres located in Rome[39]. The municipality contracted a service to Atac Spa to manage the parking lots and implement technology to offer new services and introduce new payment methods. The Garante found that the municipality (the data controller) and Atac Spa (data processor) violated Articles 5(1)(a), 12, 13, and 28.

In September 2021, the Garante announced that it asked the Irish DPC to investigate Facebook regarding the recent announcement of smart glasses before marketing the glasses to the Italian market. The Garante requested inquiries include legal basis, data protection, anonymisation, and voice assistant connected to the glasses. The Irish DPC and the Garante published a joint statement calling for Facebook Ireland to confirm their newly released product, Facebook View, properly informs individuals when recorded[40].

[38] GDPRhub, Garante per la protezione dei dati personali (Italy) - 9697724

[39] P365 Blog, BY THE ITALIAN DATA PROTECTION AUTHORITY: Roma Capitale, parking are not protected by drivers. The Italian DPA sanctions the Municipality and Atac, 09 October 2021

[40] IAPP.org, Irish and Italian DPAs on Facebook smart glasses privacy issues, 23 September 2021

JERSEY

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

Regulator(s): Jersey Office of the Information Commissioner (JOIC)

Adequacy Agreement with GDPR: yes

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

Notable changes

There have been no significant changes to legislation in the last 12 months. There has been a change in the Information Commissioner who leads the Jersey Office of the Information Commissioner ('JOIC').

Within businesses, there has been a maturing of data protection with many programmes moving into business as usual and privacy governance tools being invested in to remove the use of excel and other manual registers.

Generally, the Data Protection (Jersey) Law is based on six principles of good information handling. The JOIC issued guidance on various data protection issues.

- Data Protection by Design and Default
- Data Protection Impact Assessments
- Data subjects' rights

The JOIC signed a memorandum of understanding with the Guernsey Office of the Data Protection Authority ('ODPA') to enhance the exchange of information and cooperation between the JOIC and the ODPA.

Data Protection Authority Focus

JOIC increased the amount of guidance it is issuing and has naturally focused on protecting health data by businesses during the COVID-19 pandemic.

In June 2021 the JOIC announced that they plan to continue 'data protection audits to raise awareness of the benefits to business of good data protection and improve respect for personal information[41]'.

An announcement was made in April 2021 that Jersey firms may disclose personal data to the United States SEC in appropriate circumstances.

Additionally, the Jersey Office of the Information Commissioner (JOIC) is continuing its programme of data protection audits to raise awareness of the benefits to business of good data protection, improve respect for personal information and ensure organisations across Jersey are compliant with the Data Protection (Jersey) Law 2018.The programme, which began in November 2020, formed part of the JOIC's Regulatory Action and Enforcement Policy. The programme aims to:

- Assist companies in discovering the strengths and weaknesses in their data protection management programmes.
- Identify security gaps to decrease the risk of personal data breaches and act like a dose of preventative data protection healthcare.

[41] JOIC, JOIC Data Protection Audit Programme enters Phase Two, 01 June 2021

LATVIA

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

Regulator(s): Data State Inspectorate ('DVI')

Adequacy Agreement with GDPR: n/a

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

Notable changes

The last 12 months have unfortunately passed in the shadow of the COVID-19 pandemic. The coronavirus remains the focus of personal data protection issues, especially in labour law, education, and medicine.

Most employees work remotely, which means that their homes have become a 'workplace,' which poses a more significant risk of the breach of their privacy. Most employees work remotely, which means that their homes have become a 'workplace,' which poses a more significant risk of the breach of their privacy. The Data State Inspectorate questioned organisations around the legality of employers requiring employees to keep the computer video on during work hours. Health-related data processing was another point of contention in Latvia as employers requested COVID-19 testing results, vaccination status, and the employee's view towards receiving the vaccination.

Similar issues have been highlighted in the field of education, as students also learn remotely. In providing the assessment, The Data State Inspectorate ('DVI') considers the interaction between the teacher and student and the students themselves as a critical element in the educational process.

The Data State Inspectorate actively performs the advisory function by providing remote consultations and publishing explanations on the appropriate application of binding regulatory enactments during the pandemic.

Data Protection Authority Focus

Latvia is currently working to increase privacy in the digital environment while promoting the balance between personal data protection rights and the introduction of innovative technologies in the business, including the use of artificial intelligence.

OECD recommendations and the capacity of the DVI are taken into consideration as the DVI improves consumer protection.

The Data State Inspectorate has also applied for membership in the Global Privacy Network to facilitate cooperation with European Union countries and third countries.

MALTA

Law: The Data Protection Act (Act XX 2018) ('the Act'), GDPR

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

Adequacy Agreement with GDPR: n/a

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

Notable changes

The Government of Malta appointed Mr. Ian Deguara as the new Information and Data Protection Commissioner for five years, which went into effect on 21 December 2020. Mr. Ian Deguara was one of the first employees to join the Office of the Information and Data Protection Commissioner in December 2002 after completing his studies at the University of Malta, where he obtained a degree in computing and management.

In February 2020, Malta's Information and Data Protection Commissioner (IDPC) Office embarked on an awareness campaign designed to increase public awareness on the data protection rights deriving from the General Data Protection Regulation. The IDPC's objective is to instil a culture where citizens of different age groups understand the importance of safeguarding their personal data and being well-informed of exercising their rights under the GDPR. Various media channels published a series of publicity materials.

Data Protection Authority Focus

Year-to-date in 2021, the IDPC issued five complaints, two data breach notification violations and three data protection complaints[42]. The recurring theme surrounds the infringement of GDPR Articles 5, 6, and 32.

In 2020, the IDPC issued **€64,500** in Administrative fines, as well as 24 reprimands[43].

Like other Data Protection Authorities, in August 2021, the IDPC published guidance on cookie consent requirements.

In May 2021, the Malta Financial Services ('MFSA') and the Malta Police Force signed a Memorandum of Understanding to enhance collaborative efforts to fight financial crimes.

[42] IDPC, Decisions issued by the Information and Data Protection Commissioner, 2021

[43] Ibid.

MAURITIUS

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

Regulator(s): Data Protection Office ('the Office')

Adequacy Agreement with GDPR: No

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

Notable changes

Mauritius amended its data protection laws to align with the GDPR and international standards. The Mauritius Data Protection Act (MDPA) came into effect in 2017 to fit Mauritius' evolving digital environment. The new act makes a commendable effort to reassure data subjects of the reasons for collecting and processing their personal data. For example, the MDPA defines 'consent' more explicitly, unlike the former act, aiming to give individuals more autonomy over decision-making powers regarding their personal information.

In 2016, Mauritius became a signatory to the Convention for Protection of Individuals with regard to Automatic Processing of Personal Data ('Convention 108').

The Data Protection (Fees) Regulations 2020, concerning the new fees for registration of controllers and processors, came into force on 01 August 2020. The fees caused an essential change in the privacy culture across organisations in Mauritius. Per the regulations, data controllers and processors had a moratory period of 3 months to register with the Data Protection Office. The registration process pushed local organisations to focus on privacy program development and identify special categories of personal data, the purpose of processing, categories of data subjects, data transfers, risk management, and security.

In addition, Mauritius has recently signed and ratified the Protocol amending Convention for the Protection of Individuals concerning the automatic processing of personal data.

Data Protection Authority Focus

The complaints' mechanism is yet another novelty of the MDPA. The power to investigate a complaint in contravention of the act is conferred upon the Data Protection Commissioner. In the past year, the Commissioner has been researching complaints concerning unlawful access to personal data, the use of CCTV cameras, alleged data breaches, among others.

The MDPA brings criminal sanctions, including fines and possible imprisonment for unlawful processing of personal data. The MDPA says that any person who commits an offence could be liable to fines not exceeding 200,000 rupees and imprisonment up to five years. To date, the Commissioner has not imposed fines.

In June 2021, the Canadian Securities Administrators ('CSA') signed a FinTech cooperation agreement with the Financial Services Commissioner, Mauritius ('FSC'). The purpose of the agreement is to framework for cooperation and referrals between the jurisdictions to accommodate the evolving financial services industry.

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')

Adequacy Agreement with GDPR: No

Greg Reid
greid@bdo.com
+1 617 456-2582

Joelys Gonzalez-Mendez
jgonzalezmendez@bdo.com
+1 404 979-7108

Notable changes

In the last 12 months, no changes have been made legislatively in Mexico. Mexico's data protection regulators are focusing primarily on e-commerce and telework, considering the COVID-19 pandemic. Recently, Congress passed several bills intending to improve the legal framework for social media platforms. However, there are currently no bills designed to modify the data privacy framework.

Data Protection Authority Focus

The National Institute of Transparency for Access to Information and Personal Data Protection (Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales) (INAI) and in some ways the Ministry of Economy (Secretaría de Economía) are both considered Mexico's data protection authorities.

The INA's primary purpose is the protection of personal data and individual's right to privacy. In light of this, INAI has the authority to conduct investigations, review, sanction data protection controllers, and authorize, oversee and revoke certifying entities. The INAI has focused on national enforcement and has not exercised its powers on businesses located in other jurisdictions.

The Ministry of Economy is also an authority responsible for informing and educating on the obligations regarding protecting personal data internationally. Part of this includes issuing guidelines on security measures, identity theft, data breaches, and how to draft a privacy notice, which usually becomes part of Mexico's legal framework.

Success Story

BDO works closely to align the practices of Mexican subsidiaries and affiliates with their US, Canadian and European counterparts. One example where BDO assisted a client was helping them to design a data transfer protocol from Europe to Mexico. We supported the client institute adequate data protection measures, data protection agreements, and standard contractual clauses.

[44] https://www.duanemorris.com/site/static/Mexico_Federal_Protection_Law_Personal_Data.pdf

THE NETHERLANDS

GDPR and Dutch Implementation Law ("UAVG")

Adequacy Agreement with GDPR: n/a (we are part of the EU)

Law: Act Implementing the GDPR, GDPR

Regulator: Dutch Data Protection Authority ('AP')

Adequacy Agreement with GDPR: n/a

Menno Weij
menno.weij@bdo.nl
+31 (0)6 10 91 90 24

Notable changes

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

Dutch data subjects are increasingly aware of their rights under the GDPR. The Dutch data protection authority received approximately 25,590 complaints in 2020[45]. Many of the complaints focused on COVID-19-related privacy issues, and the AP has still yet to address nearly 9,800 of last year's complaints[46].

The AP plans to grow, so we expect to see more fines and more rapid responses to complaints in the future.

We furthermore expect to see new developments regarding (regulation of) online platforms, connected care, artificial intelligence ('AI'), and similar subjects.

Data Protection Authority Focus

The Dutch data protection authority (Autoriteit Persoonsgegevens, AP) has expressed its concerns about the continuous change of society due to digitisation and technological innovation, leading to more data that are also more diverse, specific, and personal. In this digital society, personal data protection is essential. The AP is afraid of an increase in 'digital injustice', for example, illegal data trading, inadequate security, discrimination, and undermining of the democratic legal order.

The AP has selected three focus areas:

- Data brokering (supervision on sale of data, internet of things, profiling, behavioural advertising),
- Digital government (data security, smart cities, partnerships, elections, and microtargeting), and
- AI and algorithms.

The AP will focus on designing a system for the supervision of AI and algorithms in which personal data are used and will focus, among other things, on transparency and the proper explanation of automated decision-making.

Privacy by design will become increasingly essential and perform DPIA's and meet other GDPR requirements that may not yet have had proper attention so far.

[45] IAPP, Dutch DPA summarizes 2020 work, 12 March 2021

[46] Ibid.

NIGERIA

Law: Nigerian Data Protection Regulation (NDPR)

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

Adequacy Agreement with GDPR: No

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

Tutu Oshineye
toshineye@bdo.com
+1 301 354-0723

The legal name of Nigeria's local data privacy legislation is The Nigerian Data Protection Regulation (NDPR). The NDPR is the current data protection regulation in Nigeria. It provides for the rights of data subjects, the obligations of controllers, data administrators (processors), international data transfer, data security, amongst others. The NDPR applies to natural persons residing in Nigeria or residing outside Nigeria who are Nigerian citizens.

The Nigerian Information Technology Development Agency ('NITDA') issued the NDPR.

Notable Changes

Nigeria is fast becoming a digital economy, and many Data Controllers are engaging the services of Data Protection Compliance Organisations (DPCO) to help their organisations comply with the requirements of the NDPR. Article 1(3)(j) of the NDPR states that:

'A Data Protection Compliance Organisation (DPCO) is any entity duly licensed by NITDA for training, auditing, consulting, and rendering services aimed at ensuring compliance with this Regulation or any foreign Data Protection law or regulation having effects in Nigeria.[47]'

Additionally, pending data protection lawsuits include:

- Incorporated Trustees of Laws and Rights Awareness Initiative v. Zoom Video Communications Inc.
- Digital Rights Lawyers Initiative v. National Youth Service Corps (NYSC)

These lawsuits demonstrate a growing awareness by the public of the need to protect their data. By law, Nigerian data controllers in Nigeria must comply with the NDPR by safeguarding the privacy of data subjects.

Focus of the Data Protection Authority

Recently, on 17 August 2021, NITDA exercised its enforcement powers when it sanctioned Soko Lending Company Limited (Soko Loans) for privacy invasion. Soko Loans engaged in 'unauthorised disclosures, failure to protect customers' personal data and defamation of character as well as carrying out the necessary due diligence as enshrined in the NDPR.[48]'

NITDA imposed a fine of Ten Million Naira (**N10,000,000.00**) on Soko Loans.

Success Story

BDO works closely with Nigerian law firms to develop privacy and compliance solutions to ensure that organisations and companies across Nigeria to comply with the NDPR.

[47] NITDA, Nigerian Data Protection Regulation 2019

[48] NITDA, NITDA Sanctions SokoLoan For Privacy Invasion, August 17, 2021

PANAMA

Law: Law No. 81 on Personal Data Protection 2019

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

Adequacy Agreement with GDPR: No

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

Notable changes

Law No. 81 on Personal Data Protection 2019 entered into force on 29 March 2021. In July 2021, the Executive Decree passed, which governs Panama's personal data protection principles, rights, obligations, and procedures. The Law provides consent procedures, responsibilities for cross-border data processing originating in Panama, and a Personal Data Protection Council.

The National Constitution of the Republic of Panama ('the Constitution') is another law regulating personal data protection. The Constitution outlines the right to the privacy of personal communications and documents, the right to access information contained in databases held by public bodies or by private persons providing public services, and the right to correct, rectify, and delete personal data.

Data Protection Authority Focus

In November 2020, the National Authority of Transparency and Access to Information ('ANTAI') joined the Ibero-American Data Protection Network ('RIPD'). Panama is one of the first countries in Central America to have a personal data protection law.

Since the passing of the Executive Decree, Panama focuses on topics such as:

- Legal conditions for data processing
- Consent
- Regulator obligations
- Data breach notifications
- International data transfers

POLAND

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

Regulator: Polish Data Protection Authority ('UODO')

Adequacy Agreement with GDPR: n/a

Tymoteusz Murzyn
tymoteusz.murzyn@bdolegal.pl

Notable changes

Over the last 12 months, there have not been any significant changes to legislation or local data protection authority behaviour. The new Polish Act on Personal Data Protection, adopted in May 2018, replaced the 1977 Act. The 2018 Act (adopted February 2019) contains more extensive and complex data protection regulations binding at the EU level. Also, in February 2019, the act of December 2018 implementing 'Police' Directive no. 2016/680 came into force.

Data Protection Authority Focus

Polish President of the Personal Data Protection Office regularly notifies on its activity via its official website.

The UODO continues to fine private organisations and public institutions for GDPR and local data protection regulation violations. Recent fines include privacy violations associated with health data management (e.g., body temperature measurement, vaccination data gathering). Interpretation of law presented by the Polish data protection authority regarding such socially sound issues sometimes appeared to be quite controversial and was often widely commented by experts.

In August 2021, the UODO fined District Court in Zgierz PLN 10,000 (approximately €2,180 or $2,530) for failing to implement approach safeguards (i.e., technical, organisational). Four hundred impacted data subjects, and the decision highlights a violation of Articles 5(1)(f), 24(1), 25(1), 32(1)(b), 32(1)(d), and 32(2).

In August 2021, the UODO announced that the Provincial Administrative Court in Warsaw dismissed the appeal brought by the Warsaw University of Life Sciences ('SGGW') against the UODO's decision to fine the SGGW for its failure to implement sufficient technical and organisational measures.

In July 2021, the UODO fined the Lex Nostra Foundation for the Promotion of Medication and Legal Education PLN 13,644 (approximately €3,000 or $3,481) for failing to notify the UODO and data subjects without undue delay about a data breach that occurred in 2020. The lack of notification was a violation of GDPR Article 34(2).

In June 2021, the UODO fined Funeda Spółka Sp. z o.o. PLN 22,000 (approximately €4,843 or $5,620) for lack of cooperation with the Supervisory Authority. The infraction was a direct violation of GDPR Articles 31, 58(1)(a), and 58(1)(c).

PORTUGAL

Law: 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')

Adequacy Agreement with GDPR: n/a

Luís Crispim
luis.crispim@bdo.pt
+351937990341

Notable changes

The General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) began to apply on 25 May 2018. However, Portugal failed to implement in a timely fashion the Data Protection Law Enforcement Directive (Directive (EU) 2016/680) (LED). The European Commission urged Portugal to implement the LED by the end of March 2019. Finally, the Portuguese legislation to ensure the application of the GDPR in the National legal context was published and came into force on 8 August 2019.

The critical aspects of this Law are the:

- age of natural persons to consent (fixed in 13 years),
- rights of deceased persons,
- determination of fine amounts (depending on the size of the companies), and
- legal obligation of confidentiality of confidentiality for all people that deal with personal data concerning health.

The Portuguese data protection authorities still are not performing fieldwork. They are acting only in case of complaints. Despite its current legal limitations, in October 2018, the Portuguese Data Protection Authority (CNPD) applied a fine of 400,000 EUR on the Hospital of Barreiro and Montijo (CHBM) under the GDPR[49]. Recently, the most significant Portuguese consumer protection association (DECO) was fined 107,000 EUR for sending unsolicited e-mails. The new government and budget are expected to drive more significant CNPD dynamics.

There is still much to be done in implementing the GDPR in Portuguese companies. There are some grey areas concerning the processing of health data by insurance companies which the Law or supervisory authority should clarify. At the same time, data subjects in Portugal are becoming more aware of data protection issues, and the rights of data subjects – especially the right of access – are being exercised more often. However, GDPR matters have not yet been brought in great numbers before the Portuguese courts. Due to the state of emergency caused by the spread of COVID-19, on 16 March 2020 the

Portuguese Data Protection Authority (the 'CNPD') issued Resolution 2020/170 which interrupted, with immediate effect, the deadlines to respond to its draft decisions in the context of administrative proceedings.

[49] IAPP, First GDPR fine in Portugal issued against hospital for three violations, 03 June 2019

PORTUGAL (CONTINUED)

Law: 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')

Adequacy Agreement with GDPR: n/a

Luís Crispim
luis.crispim@bdo.pt
+351937990341

Data Protection Authority Focus

In the context of the widespread practice of remote working owing to the lockdown and isolation measures imposed to address the pandemic caused by COVID-19, the CNPD (Portuguese Data protection Authority) issued, on April 17, 'Guidelines on monitoring remote working[50]'.

Several complaints from citizens diagnosed with COVID-19 had their personal information disclosed by local authorities on their websites. The CNPD issued:

(i.) Guidelines on disclosure of information relating to the COVID-19 diagnosis, and

(ii.) Guidelines on the collection of workers' health data, including the worker's body temperature.

[50] Uria Menendez Proenca de Carvalho, Guide to key legal matters relating to the COVID-19 outbreachv, 03 June 2020

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')

Adequacy Agreement with GDPR: n/a

Raluca Andrei
raluca.andrei@tudor-andrei.ro
(00) 40755633856

Notable changes

No significant legal changes regarding privacy occurred in the past 12 months.

There has been an increasing number of complaints and notifications raised with the ANSPDCP (in the first four months of 2021, 1733 complaints and data breach incidents have been notified with the data protection authority, out of which 288 investigations have been opened), proof that the data subjects become more aware of their rights and freedoms while the legal entities try to mitigate the dangers to the rights and freedoms of the data subjects following the law.

According to the GDPR Enforcement Tracker[51], fines and penalties by year include:

Year	Count of Fines	Penalties (EUR/USD)
2021 (through August)	15	€184,650
2020	26	€33,900
2019	21	€484,500
2018	0	0

Data Protection Authority Focus

The data protection authority's focus in terms of investigations relates to financial banks, telecommunication companies. However, the ANSPDCP has also sanctioned the entry into force of the GDPR, House Tenants' & Flat Owners' Associations, public authorities, and healthcare clinics.

The most recent fines applied by the data protection authority (in May - June 2021) concerned the fact that:

- The controllers did not provide the authority with the requested information for the performance of the investigation (two fines, EUR 2,000 each).
- A telecommunication company has wrongfully circulated the invoices of some clients to the e-mail addresses of third parties, which led to unlawful processing of personal data (name, surname, telephone number, client code, address) (one fine, EUR 1,000).
- The House Tenants' & Flat Owners' Association disclosed on a digital board payment due with the full name and surname of the members in the association; also, the plaintiff claimed that the association disclosed a defamatory note with his name and surname (one fine, EUR 500).
- A telecommunication company has sent marketing communications to a client who has previously revoked his consent for marketing processing activities (lack of legal basis) (one fine, EUR 2,000).

[51] GDPR Enforcement Tracker, 2021

RUSSIA

Law: Basic legislative act is the Federal Law No 152-FZ 'On personal data' of 27 July 2006 (as amended)

Regulator: The Federal Service for Supervision of Communications, Information Technology, and Mass Media ('Roskomnadzor')

Adequacy Agreement with GDPR: no

Ivan Novikov
i.novikov@bdo.ru
+7 495 797 5665 ext. 4286

Notable changes

Data protection in Russia is governed by several laws:

- Law on Personal Data (2006), which follows a similar approach to the GDPR
- Federal Law of 27 July 2006 No. 149-FZ on Information, Information Technologies, and Protection of Information ('the Law on Information')
- Federal Law of 21 July 2014 No. 242-FZ ('Data Localisation Law')

There are also potential laws around genetic data, financial assets, and digital profiles.

The most significant changes were introduced by Amendment Law No. 519-FZ of 30 December 2020. The amendments introduce a special status of personal data, namely, personal data, distribution of which is allowed by the subject of personal data.

The amendments mean that an unlimited number of persons may have access to this data if the subject of personal data provided consent for processing the personal data allowing its public distribution. The consent for processing the personal data allowed for public distribution shall be documented separately from other consents for processing. The operator must provide the subject of personal data with an opportunity to determine in the consent a list of personal data belonging to each category of personal data. The issue of personal data has the right to claim cessation of transfer of their personal data, which was previously allowed for public distribution. Claims can be raised against any person processing such personal data in violation of the law.

Data Protection Authority Focus

Basic focus of the regulator is explanation of some provisions of personal data legislation, field audits of Russian companies in the sphere of personal data and imposing of fines for significant violations of law.

In September 2021, the State Parliament ('Duma') that Bill No. 1256973 ratified legal assistance between the Member States of the Commonwealth of Independent States ('CIS'), which was signed in December 2020.

In September 2021, the office of the Moscow Region of the Federal Antimonopoly Service ('Moscow FAS') announced that Clinique Cosmetics, LLC (Estée Lauder Companies, Inc. subsidiary) breached Part 1 Article 18 of Federal Law No. 38-FZ of 13 March 2006. Clinique Cosmetics distributed advertising messages to an individual without their explicit consent, did not respond to requests to stop advertising mailing, and was fined RUB 500,000 (approx. € 5,898 or $6,839).

SINGAPORE

Law: Personal Data Privacy Commission (PDPC)

Regulator: Personal Data Protection Commission ('PDPC')

Adequacy Agreement with GDPR: no

Gerald Tang/ Cecil Su

geraldtang@bdo.com.sg /
cecilsu@bdo.com.sg
+65 68289118

Notable changes

On November 2, 2020, Singapore's legislature finally approved amendments to the Personal Data Protection Act (PDPA). The proposed changes include:

1. NEW mandatory data breach notification requirement

(i.) Organisations are now required to notify the PDPC within three calendar days after the data breach is assessed to be notifiable, of violations that result in or are likely to result in significant harm to the affected individuals or are of a substantial scale (more than 500 affected individuals).

(ii.) An organisation is required to assess once it has 'credible grounds to believe that a data breach has occurred.' It is therefore necessary to document steps taken once the company is aware of the breach to justify the time taken to do this assessment.

(iii.) Organisations are also required to notify the affected individuals as soon as practicable.

2. Expanded scope of 'deemed consent'

(i.) Consent to the processing of personal data will now be deemed to have been obtained based on contractual necessity: where the data processing is reasonably necessary to perform a contract; or

(ii.) notification and opt-out: where reasonable steps have been taken to notify individuals of the purpose of the data processing and they are given a reasonable period to opt out. To rely on this ground, organisations are required to first conduct a risk and impact assessment to determine that processing is unlikely to have an adverse effect on the individuals.

Data Protection Authority Focus

Organisations are required to notify both PDPC and the affected individuals as soon as practicable 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.

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')

Adequacy Agreement with GDPR: n/a

Marek Priesol
priesol@bdoslovakia.com

Notable changes

In the past 12 months, there have been minor changes at the national level, except in one case - the addition of legal conditions for the processing of personal data on the health status of patients in the national register, for which the corresponding legislative basis for processing was not, until recently, adopted.

In this regard, the Slovak Office for Personal Data Protection dealt in October 2020 with the legislative conditions for the processing of personal data regarding health status based on secondary legislation (Decree of the Regional Public Health Office) related to the COVID-19 – especially processing of the information on the negative result of COVID-19 test/Certificate from nationwide testing. The Office found a violation of the principles of personal data processing, as it stated in its opinion that decrees adopted since the Slovak Act on Protection and Promotion of Public Health could not be considered an adequate legal basis for personal data processing.

There was also quite a serious incident in connection with the processing of personal data relating to health. In September 2020, the Slovak security IT company Nethemba drew attention to a critical vulnerability in the Moje eZdravie ('My eHealth') application, which is operated by the National Center for Health Information ('NCZI')[52]. NCZI obtained personal information about more than 130,000 patients that tested for COVID -19 in Slovakia. According to that IT company, the error made it possible to obtain information about more than 390,000 patients in the database. NCZI later informed the ÚOOÚ that the application lacked appropriate security protections required for public administration information systems. The case is pending currently.

[52] Ekdeeps, Sensitive data have been compromised for months on the Internet – Home – News, 17 September 2020

SLOVAKIA (CONTINUED)

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')

Adequacy Agreement with GDPR: n/a

Marek Priesol
priesol@bdoslovakia.com

Data Protection Authority Focus

The Slovak Office for Personal Data Protection is focused on the guidance and informing the public in the news, especially in EU legislation, and the controlling activities.

According to official data from the Office, in 2020, the Office registered 65 new inspections on the processing of personal data[53]. The ÚOOÚ inspected ten potential data processing violations while fifty-five inspections (at various procedural stages) carried over to 2021.

The subject of 39 inspections completed in the observed period was in 10 cases processing activities of state bodies and organisations, in 4 cases processing activities of local self-government bodies (cities and municipalities), in 20 cases processing activities of other legal entities (including two banks, one insurance company and one health care provider) and processing activities of a sports association. In 2020, checks on the processing of personal data were also performed on four natural persons.

The most frequent subject of the personal data protection proceeding was reviewing the legal regulations required when processing personal data via camera systems. And the most frequent violation was a violation of the legal basis of processing, respectively contrary to the principle of integrity and confidentiality, which was linked to the failure to take appropriate security measures by processors.

[53] Office for Personal Data Protection of the Slovak Republic

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')

Adequacy Agreement with GDPR: no

Carl Bosma
cbosma@bdo.co.za

Notable changes

The data privacy legislation in South Africa is called the Protection of Personal Information Act ('POPIA'). Although POPIA has been in existence since 2013, it only became effective from 1 July 2020 and will be enforced from 1 July 2021. Additional regulations support POPIA and provide detail regarding the Act's implementation and compliance.

Over the past year, we have noted a marked interest in POPIA as companies scramble to become compliant before the deadline at the start of July. However, this has been tempered to a certain degree as companies have focused their efforts on the global pandemic. Likely, a significant proportion of companies will not be compliant, and the legislation carries penalties of up to **ZAR 10 million** (€ 567,761 or $658,516) or imprisonment for a maximum period of 10 years[54]. Or course, the actual harm to a company of non-compliance is potential reputational damage.

Similarities between the POPIA and the GDPR include:

- develop, implement, and monitor a compliance framework
- undertake a personal information impact assessment to ensure that adequate measures and standards exist to comply with the conditions POPIA
- develop internal measures, together with adequate systems to process requests for information or access to it
- conduct internal awareness sessions regarding the provisions of the Act

Differences between POPIA and GDPR are that the protection POPIA affords to juristic persons and not only to natural persons. A company's CEO is the Information Officer by default (a compulsory position).

Data Protection Authority Focus

The South African legislation follows a punitive approach as outlined above. Although the financial impact is reasonably small compared with international jurisdictions, the possibility of imprisonment is generally considered severe, and the fines will be applied to each breach.

[54] IAPP, After 7-year wait, South Africa's Data Protection Act enters into force, 01 July 2020

SPAIN

Law: Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), GDPR

Regulator: Spanish Data Protection Authority ('AEPD')

Adequacy Agreement with GDPR: n/a

David Molina and
Roger Perez
david.molina@bdo.es and
roger.perez@do.es
+34 676 587 589 and
+34 696 723 386

The AEPD is one of the most active data protection authorities in Europe in terms of issuing enforcement actions and responding to data subjects' complaints and requests. Since 2018, the AEPD filed approximately 295 complaints[55].

According to the GDPR Enforcement Tracker[56], fines and penalties by year include:

Year	Count of Fines	Penalties (EUR/USD)
2021 (through August)	124	€23,461,800
2020	133	€8,152,710
2019	38	€1,318,100
2018	0	0

Notable changes

There have been no relevant legislative changes in privacy in the last year, but our Spanish Data Protection Authority has increased the number of sanctions and the economic number of sanctions for companies of all sizes.

Data Protection Authority Focus

Companies of all sizes have been fined for breaches of the RGPD that are very different from each other (from data breaches not notified to e-mails without hidden copy through the content of the privacy policy or the transfer of data between companies or legitimate interest).

[55] GDPR Enforcement Tracker, 2021

[56] Ibid.

SWITZERLAND

Schweizer Datenschutzgesetz - Swiss Data Protection Act

Law: Federal Act on Data Protection 1992 ('FADP')

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

Adequacy Agreement with GDPR: yes

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

Notable changes

The Swiss Parliament has enacted a total revision of the Swiss Data Protection Act (DPA) in the fall of 2020. The revised DPA bases on principles equivalent to the GDPR, however, is not just a copy of the GDPR. The rules in the revised DPA deviate slightly from the GDPR in the details. Generally speaking, the Swiss DPA is somewhat less detailed and thus, gives some more room for interpretation. Similar to the GDPR, the revised DPA will also have an extraterritorial effect. There are data incident notification duties and data subject access rights. The revised DPA grants several exceptions relating to the information duties upon collection of the data. Data transfers to countries with an equivalent level of data protection are privileged. The revised DPA is expected to enter into force most likely from 1 July 2022. There will be no grace period.

Data Protection Authority Focus

Contrary to the administrative fines against the company in the GDPR, the revised Swiss data protection act provides for penal sanctions against responsible persons in the organisation. In a Swiss limited liability company for instance, that means that the board of directors is liable in first instance. They are responsible for ensuring data protection compliance within the organisation and should regularly seek to report on the maturity of the organisation in the respect, for gaps and potential improvements.

UNITED ARAB EMIRATES (UAE)

Law: No Federal Law

Regulator: No Federal Regulator

Adequacy Agreement with GDPR: no

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

Notable changes

Currently the UAE does not have a country wide privacy legislation, however, there are discussions of such a law. Multiple sectoral data protection and security laws exist, including Federal Law by Decree No. 3 of 2003 Regarding the Organisation of the Telecommunication Sector, Federal Law by Decree No. 5 of 2012 on Combating Cybercrimes (13 August 2012), Federal Law No. 18 of 1993: Commercial Transactions Law, and the UAE Federal Law No. 2 of 2019.

A few jurisdictions have specific laws apply such as DIFC Data Protection Law[57] and the ADGM Data Protection Law[58]. Along with this there are privacy laws in general and some specific standards for healthcare sector[59].

Data Protection Authority Focus

In the last 12 months, we have seen more than two Data Protection laws updated significantly in UAE (i.e., DIFC Data Protection Law and ADGM Data Protection Regulation). We have also seen updates to standards for the healthcare sector too such as the Department of Health (DOH) Abu Dhabi's - Abu Dhabi Healthcare Information and Cyber Security Standards (ADHICS). These legislations cover not only the data protection angle but also the data privacy aspects too. In the next couple of years, we believe we may expect UAE to have its country-wide data privacy and protection legislation.

Regarding the jurisdiction-specific data privacy and protection laws implemented, they 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 is why the ADGM became the first in the gulf country to join the Global Privacy Assembly's International Enforcement Cooperation Working Group ('IECWG').

We have also seen much effort put in by the authorities to educate the organisations and public about the legislation in force and how to comply with the same. Further, specific guidance materials have also been made available to the organisations and people who can implement the controls specific to the legislation. This guidance material also incorporates some self-service questionnaires, which can clarify the usual confusions such as FAQs.

The jurisdictions have a proper organisational structure to cater to the current requirements. 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.

[57] Dubai International Financial Centre, DIFC Data Protection

[58] Abu Dhabi Global Market, ADGM Enacts its New Data Protection Regulations, 2021

[59] BDO UAE, A Snapshot of DIFC Data Protection Law (DPL) 2020, Data Privacy in UAE, July 2020

UNITED KINGDOM

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

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

Adequacy Agreement with GDPR: yes

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

Notable changes

The UK exited the European Union and they adopted two adequacy decisions for the UK:

- Commission Implementing Decision of 28 June 2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council
- 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

COVID-19 and the processing of health-related data is another key focus for the UK. The ICO issued guidance as to what companies can do with health-related information. Additional guidance around working from home followed shortly after that.

Data Protection Authority Focus

Despite the developments of Brexit and COVID-19, the UK's ICO was busy in 2020, and this continued into 2021. The ICO had several comments calls, including direct marketing and the Age Appropriateness Code (collection of minor's information). They also guided data subject access requests and criminal offence data. Separately, the UK Governmental Department for Culture, Media & Sports ('DCMS') launched a consultation on a National Data Strategy. In September 2021 the DCMS launched its Cyber Security Breaches Survey 2022, which details the costs and impacts of cyber breaches and attacks on UK businesses[60].

The UK also reacted to guidance pushed out from the European Union, notably regarding consent, data protection by design & default, and health data processing, especially for reasons attributed to COVID-19.

In September 2021 the UK Government the DCMS presented to Parliament the National Artificial Intelligence ('AI') strategy. The strategy lays out a long-term plan for the UK AI ecosystem, support requirements, and the governance structure.

In 2020, investigations and sanctions continued to rise. The most notable cases include British Airways (fine, **£20.0 M**[61] or $27 M) and Marriott Group (fine, **£18.4 M**[62] or $24 M). More recently, Ticketmaster was fined **£1.25 M** ($1.7 M), and an EasyJet data breach investigation is underway. EasyJet is managing litigation and class action suits that resulted from the compromise of approximately 9.4 million customers and 2,208 credit card details accessed[63].

[60] CBI/ABI, Cyber Security Breaches Survey 2022 Frequently Asked Questions

[61] ICO, ICO Fines British Airways £20m for data breach affecting more than 400,000 customers, 16 October 2020

[62] ICO, ICO fines Marriott International Inc £18.4million for failing to keep customers' personal data secure, 30 October 2020

[63] IDC, easyJet Data Breach – Rebuilding Trust Now a Priority, 22 May 2020

UNITED STATES

Law:

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

Adequacy Agreement with GDPR: Privacy-Shield Renegotiation[64]

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

Greg Reid
greid@bdo.com
+1 617-456-2582

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

Notable changes

Federal Privacy and Data Protection Laws

There is no comprehensive privacy or data protection law for the United States of America. As of August 2021, 30 privacy bills had been introduced to the House of Representatives ('House') and in the Senate. While many of them are identical to one another, there are 24 unique privacy bills. Two proposed federal legislations exist for the US - Setting an American Framework to Ensure Data Access, Transparency, and Accountability (SAFE DATA) Act (S.249) proposed by Senator Roger Wicker (R-Miss.). The Consumer Data Privacy and Security Act of 2021 (S.1494) presented by Senator Jerry Moran (R-Kan.) has similar expectations.

- The right to access
- The right to correction of personal data
- The right to deletion
- The right to portability
- The ability to opt-out of processing and opt-in for sensitive processing
- Notice and transparency requirements
- The requirement for companies to hire a privacy officer
- Processors and service providers must meet and follow specific requirements

There is a myriad of sectoral laws and industry-specific frameworks at the federal level, including CAN-SPAM, HIPAA, HITECH, GLBA, and COPPA.

State Privacy and Data Protection Laws

Three states passed privacy laws: California, Virginia, and Colorado. California passed the California Consumer Privacy Act and then later passed the California Privacy Rights Act of 2020; Virginia passed the Consumer Data Protection Act; Colorado passed the Consumer Data Protection Law.

California

Law: California Consumer Privacy Act of 2018 (last amended in 2019) ('CCPA')

Regulator: The California Attorney General ('AG')

The California Consumer Privacy Act ('CCPA') took effect January 1, 2020. The CCPA places limitations on collecting and selling consumer personal information and grants rights to consumers concerning their personal data.

[64] Privacy Shield Framework, FAQs – EU-US Privacy Shield Program Update, 31 March 2021

UNITED STATES (CONTINUED)

Law:

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

Adequacy Agreement with GDPR: Privacy-Shield Renegotiation

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

Greg Reid
greid@bdo.com
+1 617-456-2582

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

The CCPA applies to the processing of personal information of California residents by for-profit businesses that do business in the State of California, collect personal information, and meet any of the following:

1. Annual gross revenue in excess of $25 million.
2. Buys, receives, sells, or shares for commercial purposes, the personal information of at least 50,000 Californians.
3. Derives 50% or more of its annual revenues from selling consumers' personal information.

In November 2020, California voted to enact the California Privacy Rights Act (CPRA), significantly expanding the CCPA when CPRA takes effect on January 1, 2023. The CPRA maintains the core framework of the CCPA while introducing substantive changes inspired by the EU General Data Protection Regulation (GDPR).

Virginia

Law: Consumer Data Protection Act ('CDPA')

Regulator: The Virginia Attorney General ('AG')

Virginia passed the Consumer Data Protection Act (CDPA), effective January 1, 2023. The CDPA applies to all persons or companies conducting business in Virginia, or those which target their products and services to Virginia residents, and that either:

(i) control or process the personal data of at least 100,000 Virginia residents; or

(ii) control or process the personal data of at least 25,000 Virginia residents and derive more than 50% of gross revenue from the sale of personal data.

The CDPA will not apply to Virginia state agencies, non-profits, institutions of higher education, and entities governed by HIPAA or GLBA.

Colorado

Law: Senate Bill 21-190 for the Colorado Privacy Act ('CPA')

Regulator: The Colorado Attorney General ('AG')

Colorado became the third state in the United States to pass a privacy law. The Colorado Privacy Act ('CPA') provides consumers the rights to opt-out of processing, access personal data, correct personal data, delete personal data, and obtain a copy of their personal data. Like the GDPR, CPA requires controllers and processors to limit the purposes they process data, minimize data, and conduct impact assessments. Colorado's Attorney General maintains the Colorado Consumer Data Protection Laws FAQ for businesses and government agencies.

UNITED STATES (CONTINUED)

Law:

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

Adequacy Agreement with GDPR: Privacy-Shield Renegotiation

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

Greg Reid
greid@bdo.com
+1 617-456-2582

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

Following the invalidation of Privacy Shield by the Court of Justice of the European Union in July 2020, organisations transferring personal information from the EU now rely on other adequate means of transfer, such as Standard Contractual Clauses or Binding Corporate Rules. Further, organisations must verify on a case-by-case basis whether US law ensures adequate data protection. Some organisations also consider consent or other derogations under Article 49 of the GDPR to address adequacy.

Data Protection Authority Focus

Although there is no comprehensive law in the US, the State Attorney Generals and the FTC investigate and file suit against companies that encounter a data breach, mislead consumers, expose unnecessary risk to patients, or mispresent its data privacy and protection standards.

In 2020, more than 29 million healthcare records were breached, resulting in a 25% increase year-over-year in healthcare data breaches. There were 642 healthcare data breaches of 500 or more records in 2020, and one breach involved more than 10 million records, while 63 breaches experienced exposure of more than 100,000 records[65].

In 2019 it was reported that Google and YouTube were fined $170 million for alleged violations of children's privacy law[66]. Google will pay $134 million and YouTube $34 million to New York[67]. The companies collected personal information in the form of persistent identifiers that are used to track users across the Internet, from viewers of children's related television channels, without first notifying the parents and getting their consent.

Under Section 5 of the FTC Act of 1914, the Federal Trade Commission ('FTC') takes law enforcement action against companies that violate consumers' privacy rights[68]. The FTC files suit against companies misleading or failing to protect sensitive consumer information that may have caused a substantial consumer injury. Additionally, the FTC sues for unfair and deceptive trade practices and enforces other federal laws relating to consumers' privacy and security. The most notable cases that the FTC brought in 2020 and 2021 are Facebook, Kohl's Department Store, Zoom Video, and Vivint Smart Home.

Despite the absence of federal privacy law, the US states and the federal government continue to expand their enforcement efforts for companies violating consumers' privacy and data protection.

[65] HIPAA Journal, 2020 Healthcare Data Breach Report: 25% Increase in Breaches in 2020, 19 January 2021

[66] Federal Trade Commission, Google and YouTube Will Pay Record $170 Million for Alleged Violations of Children's Privacy Law, 04 September 2019

[67] Ibid.

[68] Federal Trade Commission, Protecting America's Consumers, Privacy and Security Enforcement

This publication has been prepared by BDO member firms who contributed to it, but it has been written in general terms and based on the most recent information available at the time of its development. This publication should be seen as containing broad statements only and might be subject to further updates. This publication should not be used or relied upon to cover specific situations and you should not act, or refrain from acting, upon the information contained in this publication. No entity of the BDO network, its partners, employees and agents accept or assume any liability or duty of care for any loss arising from any action taken or not taken by anyone in reliance on the information in this publication or for any decision based on it.

'BDO', 'we', 'us', and 'our' refer to one or more of BDO International Limited, its network of independent member firms ('the BDO network'), their related entities, and any BDO member firms. Service provision within the BDO network is coordinated by Brussels Worldwide Services BV, a limited liability company incorporated in Belgium. Each of BDO International Limited (the governing entity of the BDO network), Brussels Worldwide Services BV and the member firms is a separate legal entity and has no liability for another such entity's acts or omissions. Nothing in the arrangements or rules of the BDO network shall constitute or imply an agency relationship or a partnership between BDO International Limited, Brussels Worldwide Services BV and/or the member firms of the BDO network. Neither BDO International Limited nor any other central entities of the BDO network provide services to clients. BDO is the brand name for the BDO network and for each of the BDO member firms.

© Brussels Worldwide Services BV, August 2021

Europe

Koen Claessens
Koen.claessens@bdo.be

North America

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.