AN OFFERING FROM BDO'S
DATA PRIVACY PRACTICE

PRIVACY INSIGHTS 2020

BDO

FOREWORD

This whitepaper is focussed on global data privacy regulatory insights. However, given the current global COVID-19 pandemic situation it would be injudicious to not mention some of the considerations for data privacy during these unprecedented times. There are two global megatrends to monitor developments of.

The first is the global race to develop contact tracing applications. These are being designed and developed by large corporations, national governments and private companies. Significant work is underway by Data Protection Authorities, lawyers, politicians and privacy advocates to balance citizens privacy rights with the urgent need to manage the pandemic. There is also significant concern that even if privacy rights can be balanced for this specific use, governments and companies may retain too much control over citizens data post the pandemic as a result.

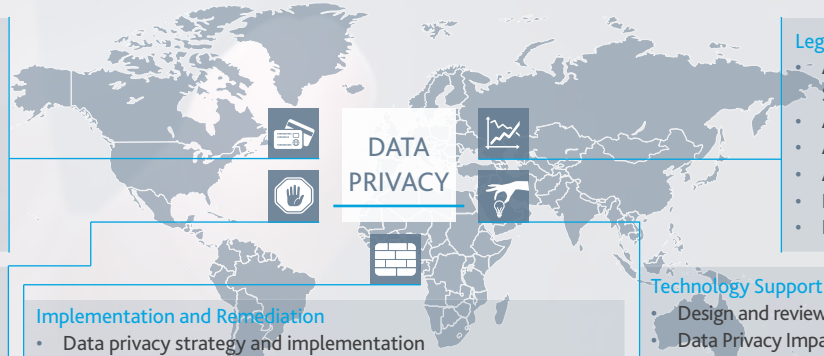
The other megatrend is the mass move globally to working from home. This brings internal and external challenges. Internal considerations include the rapid shift to remote working with increased use of personal devices and dependence on key individuals as well as the need to understand more about the personal health situation of not only employees but those they are co-habiting with. Additionally, timelines for responding to Data Subject Access Requests can be strained. External challenges include the emergence of increased opportunities for fraudsters and criminals to illegally obtain personal data as well as the potential impact of an impaired service from external providers which may result in increased data breaches.

Koen Claessens, *Partner Risk Advisory, BDO Belgium*
Karen A. Schuler, *Governance, Risk & Compliance (GRC), National Leader BDO USA*

INTRODUCTION

BDO's clients operate in multiple jurisdictions around the world. As such, we are pleased to provide a summary of current data privacy obligations along with contact details and commentary, from a sample of jurisdictions where BDO has substantial privacy expertise.

Over the last several years BDO formalized its global privacy program by defining and operationalizing data privacy services that complement data governance, information governance and cybersecurity. Core services that BDO offer includes: assessments, legal support, technology support, implementation and remediation, and managed services. A comprehensive view of our offerings are outlined below.



Managed Services

- Individual Rights Administration
- Privacy by Design Operations
- Maturity Assessments
- PrivacyWatch
- Data Protection Acadamy
- External DPO or internal DPO support
- Representative as a Service

Legal Support

- Ad hoc legal advice (e.g. video surveillance, DSARs, Data Sharing)
- Advice on data subject requests and data breaches
- Advice on interpretation and applicability
- Advice on contractual arrangements with third parties
- Legal representation vis a vis Data Protection Authorities
- International data transfers policies and registers development

Assessment

- Data Privacy readiness assessment
- Data Privacy audit / due diligence
- Annual Privacy Healthcheck
- Data mapping / data flow diagramming
- Records of processing register development
- Data Protection Assurance / Certification

Implementation and Remediation

- Data privacy strategy and implementation
- Privacy project management
- Privacy notices, policies and procedures development
- Technical controls implementation
- Third-party processor remediation
- Data minimization, retention, erasure and classification policies, and process development

Technology Support

- Design and review of planned and existing architecture. 'Data Privacy by design'
- Data Privacy Impact Assessments & implementation of technical measures
- Data subject rights management
- Data privacy management tools: Tool / software selection Plan, design & implementation of tools
- Data masking & Data encryption tool
- Security assessments: Vulnerability scanning, Penetration testing, Ethical hacking & social engineering

GLOBAL INSIGHT

Although there are varying patterns globally, common themes exist across jurisdictions. For example, companies serving European markets are required to comply with the General Data Protection Regulation (GDPR). Those same companies operating in California, United States or in Brazil will be required to comply with their new regulations, which only compounds privacy program obligations. That, in addition to the global pandemic driving regulatory updates and guidance makes it difficult for companies to sustain a business-as-usual state.

In 2017 and 2018 companies rushed to attain compliance in time for GDPR in May 2018. Thousands of readiness assessments were conducted, resources were mobilised, only to wait to see if a regulator would call upon them to evaluate their state of compliance. Following this, in 2019, there were limited GDPR activities across Europe, however companies based in the United States experienced an uptick in activity – in particular, they were called upon to demonstrate compliance. And, if a data breach occurred, then regulators from jurisdictions like the European Union, China, India, Turkey, United States, Hong Kong, Australia, Canada and many others were keen to scrutinise what occurred and demonstrate their new powers. Regulators are also more sophisticated than ever before; often calling in outside experts and lawyers to ensure they are thoroughly investigating such cases.

The dreaded fines which were the oft-cited driver for GDPR compliance in the run up to May 2018 have not made the impact many expected, leading to many (inaccurate) comparisons to Y2K (the millennium bug). It is true that although some hefty fines have been issued, the frequency or magnitude that were predicted in some quarters have not come to fruition. However, penalties were far greater than under existing European data protection regulations. And, the GDPR is driving other jurisdictions to conduct investigations. Therefore, even though GDPR penalties have been in the order of thousands rather than millions and most entities have (so far) remained unscathed, data breaches are being investigated in regions outside of the European Economic Area (EEA). That said, the fine of 50 million EUR issue by the French DP against Google in January 2019 (for lack of transparency, inadequate information and lack of valid consent regarding targeted adverts) certainly caused companies to take notice.

Data breaches are not region-dependent - data knows no boundaries. For example, a company operating in the United States may service consumers in more than 50 jurisdictions. That company experiences a data breach where consumers are impacted in 20 jurisdictions and 15 of them have data protection laws or regulations. The impacted organization will likely receive an enquiry from each of those jurisdictions, which then could lead to five or more investigations. Some jurisdictions ask specific questions about the incident and will surmise that the company operated in good faith to protect the rights of individuals. However, the other five inquiries will typically lead to investigations. Those investigations may result in fines; however, the fees to complete these investigations range from $50,000 to millions.

Regulators have been 'complaint led' and focused on core principles such as fairness, lawfulness and transparency as exemplified in the Cambridge Analytica/ Facebook scandal, where personality tests were used to gain access to data used for targeted adverts, allegedly influencing the outcome of the U.S. election and the UK Brexit referendum. This reflects the fact that in general, scrutiny and publicity has been focused on the social media giants and larger multinational companies. Resting on one's laurels however is not an option. It is worth noting that the big cases take time to bring to fruition and progress through the court system. They may not have hit the headlines yet, but there are cases waiting in the wings. In purely pragmatic terms, the Data Protection Authorities have had a significant workload to examine. Not only that, they also have to manage ongoing issues that pre-dated the GDPR. Both the UK's Information Commissioner's Office (ICO) and the Irish Commissioner have indicated that there are cases in the pipeline for 2020. Now more resources have been allocated and experience gained, it is predicted that regulatory activity will 'step up'- and the highest fines and most significant enforcement notices are yet to come. Data controllers and processors who have become complacent in 2019 may well regret their lack of action.

It has also become apparent that 'GDPR compliance' is by no means a simple or binary matter. Sub-processors are a good example of this. Although one of the compulsory 'GDPR clauses' requires that processors cannot deploy sub-processors without express consent, it is difficult (if not impossible) to implement this in practice. In particular, multinational companies who have 'take it or leave it' online terms could be faced with greater scrutiny in 2020 and 2021. Similarly, subjectivity and lack of clarity can be a problem. The definition of what constitutes an 'adequate' technical or organisational measure to ensure data security is, to some extent at least, a matter of debate.

One obvious global trend is the rise of public awareness related to privacy matters. For example, even though subject access requests have been a right for many years in Europe, with GDPR it is now a matter of public consciousness. The European Commission published in May 2019 that 67% of Europeans had heard of the GDPR and 57% knew that a public authority in their country oversaw it. This awareness has contributed to a rise in complaints and requests, with a resulting increase in enforcement action. Fines (particularly in Europe) are usually derived from complaints from individuals around data subject rights, consumer issues and data breaches.

Cross border data transfer issues have also been a recurrent theme. In the European Data Protection Board's Work Program 2019/2020, denotes that they will more regularly examine "the consistent application of the GDPR, in particular in cross-border data protection cases". The EDPB plans to release guidance on the certification and Codes of Conduct as a tool for transfers, as well as international transfers between public bodies for administrative cooperation purposes. They will also continue to provide opinions from certain Supervisory Authorities on standard contractual clauses for international transfers under Article 46(2) GDPR, standard contractual clauses for processors under Article 28(8) GDPR and ad hoc contractual clauses for international transfers under Article 46(3) GDPR. And, finally the EDPB might provide guidance on the interaction between the Regulation on the free flow of non-personal data in the EU and the GDPR, an opinion on cross-border requests for e-evidence and further work on interoperability. The increase of data being part of every aspect of life is driving organisations to seek 'certifications' or 'guarantees' to provide some level of reassurance. The request for personal information is commonplace, which is driving regulations, but also driving public concern. In the U.S., Senators are calling for a national data privacy law. Moreover, the U.S. Federal Trade Commission (FTC) will require privacy scores for the largest tech companies. Additionally, the FTC recently levied a $5 billion penalty (largest consumer privacy penalty ever) against Facebook for violating its 2012 FTC privacy order and the company will be required to comply with new restrictions. While the mechanisms for such 'official' certifications are being developed, clients are seeking to rely on interim comforts such as service organisation control reports or 'privacy health checks.'

In the EEA over 160,000 data breach notifications have been reported to date

Total Number of GDPR Fines

317

Total Amount of GDPR Fines

€155,398,106

Largest Fine

€50,000,000

Google Inc. on January 21, 2019 - France

Smallest Fine

€90

Hospital on November 18, 2019 - Hungary

Source: Privacy Affairs GDPR Fines Tracker

Note: that these numbers only include actual fines not those announced by regulators as an intention to issue, such as British Airways €204m and Marriott International €110m.

BDO GLOBAL PRIVACY SERVICES FOOTPRINT

BDO partners with its clients to ensure compliance with data privacy legislation and to serve as an independent Data Protection Officer (DPO). Our global organisation and data privacy capabilities and expertise allows our teams to serve global companies in all major jurisdictions.

If not managed well, data privacy projects can easily become wasteful and ineffective. BDO's pragmatic approach ensures a cost-effective and efficient road to compliance. Our legal, operational, IT and privacy expertise provides a multidisciplinary team that works seamlessly across your organization.

Data Protection Resources

An overview of the BDO global privacy services footprint

Multidisciplinary privacy approach supported by over
+600 privacy professionals worldwide

+ 275 Technology specialists

+ 275 Advisory specialists

+ 55 Legal experts

COUNTRY UPDATES

Supporting you on your journey

- We have specialists across the globe who can support you to become compliant, maintain compliance or provide assurance over your level of compliance
- The following pages provide summaries for 26 countries.
- Please feel free to reach out to any of the contacts for support.

AUSTRALIA

Legislation:
Part 3C of the Privacy Act 1988 (Privacy Act)

Adequacy decision with EU:
NO

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

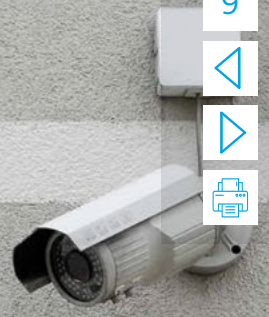
Under the Notifiable Data Breaches (NDB) scheme, any organisation or agency that the Privacy Act covers must notify impacted individuals and the Office of the Australian Information Commissioner (OAIC) when a data breach is likely to result in serious harm. Under section 26WE(2) of the Privacy Act, the test for determining whether a breach is likely to result in serious harm is whether a reasonable person would conclude that the access or disclosure would be likely to result in serious harm to any of the individuals to whom the information relates. Serious harm will be "likely" if it is more probable than not, rather than possible. There are significant financial penalties for non-compliance with this legislation of up to $420,000 for individuals and $2.1 million for organisations. The 2018 BDO/AusCERT Cyber Security Survey found that organisations were significantly more confident and prepared to meet their NDB obligations in 2018 than in 2017 (55.9% completely confident in meeting NDB obligations in 2018, up from 11.2% in 2017). As governments become increasingly agile in responding to the ever-changing nature of cyber security threats, the regulatory landscape also continues to evolve. Naturally, with this increased focus on legislation regarding both cyber security and data privacy, the role of data breach detection, public disclosure and reporting has become significantly more prominent. The 2018 Cyber Security Survey Report also found that 1 in 10 breaches were notified to the OAIC. We expect visibility of data breaches and notification to regulatory authorities and impacted individuals to increase across the 2020 horizon.

BELGIUM

Legislation:
GDPR (Belgian Data Protection Act of 30/07/2018)

Adequacy decision with EU:
N/A

Koen Claessens
koen.claessens@bdo.be
+32 497 51 53 83



In addition to the GDPR being in place since May 2018, Belgium also adopted its own Belgian Data Protection Act on the 30th July 2018, to clarify and further elaborate on certain elements of GDPR. An example of this is the law on surveillance cameras, which has been revised. Significant efforts were made by many organisations to become compliant with GDPR by the 25th of May 2018, however, most still have quite some work to do. Large investments in data privacy were made in healthcare and the financial sector but other sectors still have to catch up. Most service organisations, the so-called 'data processors', are in process of obtaining privacy attestations under pressure from their customers, the so-called 'data controllers'. In general, SOC2 is used as an auditing standard for this attestation.

After May 2018, it took the Belgian Data Protection Authority about 1 year to become fully operational, resulting in a loss of momentum in the industry, as data privacy was temporarily assigned a lower priority. In Belgium, the first fine was imposed on 28 May 2019. With the re-organization and the first fines, it seems that the grace period has officially come to an end and data privacy is moving higher up on the agenda again. In early 2020, a number public and private organisations were hit by cyber security incidents, causing significant business interruptions. As some of these incidents also impacted the personal data and resulted in data breaches, the emphasis on data privacy has increased again.

BULGARIA

Legislation:
GDPR (Personal Data Protection Act (PDPA) (amended and supplemented 26 February 2019))

Adequacy decision with EU:
N/A

Silvana Dzharkova-Aleksandrova
s.dzharkova@murgova.com
+359 2 9898 298

In Bulgaria the amendments and supplements to the local legislation came into force after the GDPR and the national Personal Data Protection Act (PDPA) was revised in 2019. The amendments in the PDPA are with regard to its harmonization with GDPR as some new requirements of GDPR are further elaborated in it. Some other local acts were amended for the same reason. The Bulgarian Commission for personal data protection (the authorized supervising body under GDPR) has conducted several audits to larger companies operating with personal data under its own self-referral or due to signals by data subjects. As a result of these audits, fines have been imposed where violations were found. The sizes of the fines are proportional to the seriousness of the violations found. Based on our professional experience in the data protection field in Bulgaria, our opinion is that there is still much to be done in terms of the implementation of the GDPR by local companies and

most of the international ones operating in the market. Nevertheless, both the companies and data subjects are becoming more aware of data protection issues and the importance of the actual implementation of the new rules. Internal implementation processes are underway but require additional time and resources to be invested.

CANADA

Legislation:
Personal Information Protection and Electronic Documents Act (PIPEDA)

Adequacy decision with EU:
NO

Anisha Gupta
anigupta@bdo.ca

In Canada, most industries have to comply with privacy regulations such as the Personal Information Protection and Electronic Documents Act (PIPEDA) which regulates how organisations may collect, use and disclose the personal information as a part of their business operations. Some provinces have their own privacy regulations similar to PIPEDA. Generally the law governs obligations for data privacy in a similar manner as the GDPR. Fines for non-compliance are actionable up to $100,000 per offence.

There is a constant increase in stakeholder awareness and expectations around privacy, transparency and accountability. Clients, customers and stakeholders expect organisations to safeguard their personal information, protect it from misuse and be transparent and accountable for how it is used.

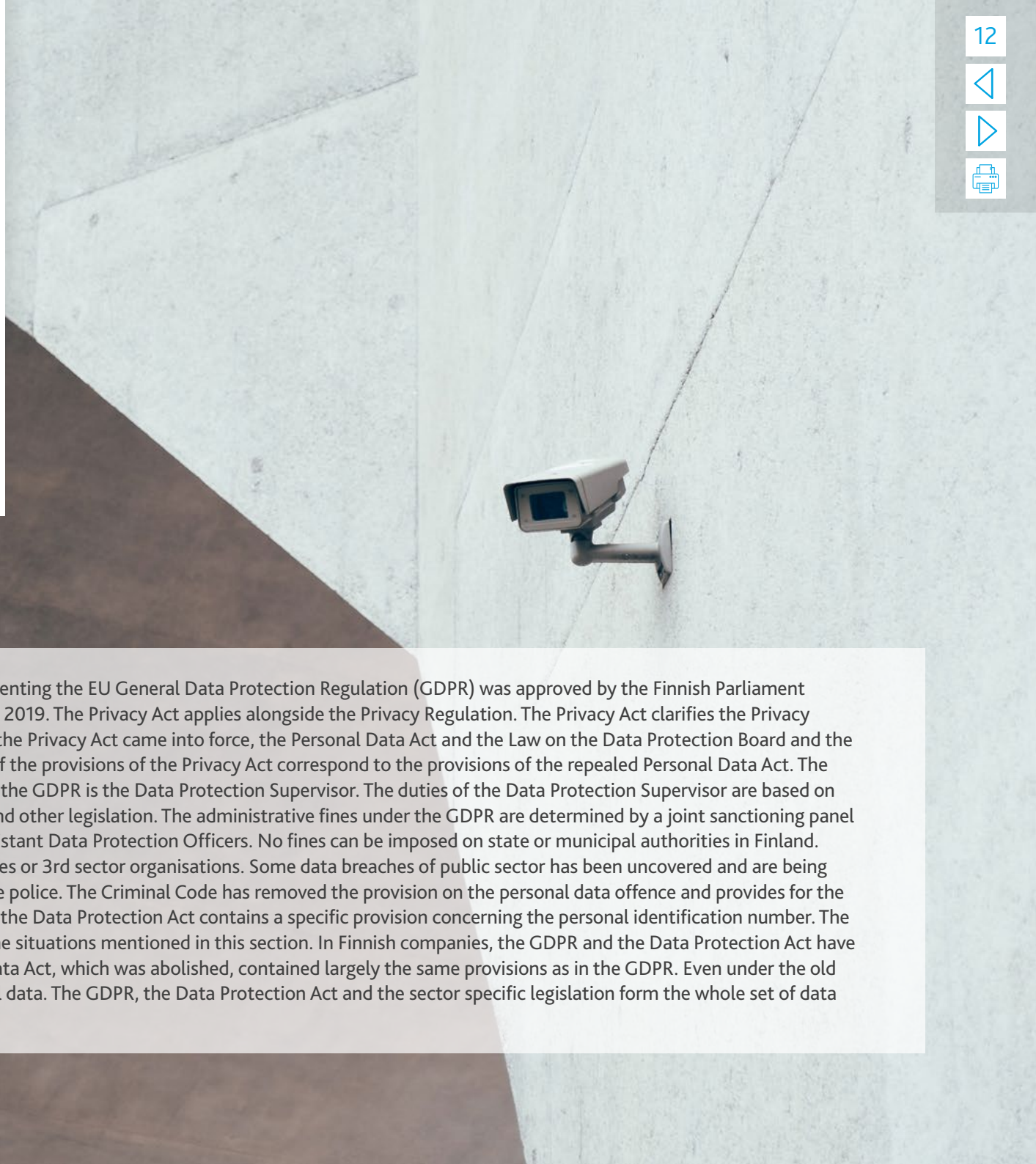
Organisations have started taking into account these expectations while developing and adopting their privacy practices. There are huge risks associated with privacy breaches and violations, including the risk of court action, class action litigation, court-awarded damages and reputational injury. By moving towards alignment with PIPEDA, organisations can maintain the trust and confidence of their customers, clients and other stakeholders, and minimize the risk of reputational damage. By complying voluntarily with PIPEDA, organisations can also avoid accidentally breaching PIPEDA requirements and avoid possible fines and penalties under the legislation. Doing so will help to manage legal and reputational liability and maintain stakeholder confidence in the organisation.

FINLAND

Legislation:
GDPR, Data Protection Act (2019)

Adequacy decision with EU:
N/A

Ossi Määttä
ossi.maatta@bdo.fi
+358 50 351 1453



The new Data Protection Act (Tietosuojalaki) supplementing the EU General Data Protection Regulation (GDPR) was approved by the Finnish Parliament in November 2018 and entered into force on 1 January 2019. The Privacy Act applies alongside the Privacy Regulation. The Privacy Act clarifies the Privacy Regulation and provides some exceptions to it. When the Privacy Act came into force, the Personal Data Act and the Law on the Data Protection Board and the Data Protection Commissioner were repealed. Some of the provisions of the Privacy Act correspond to the provisions of the repealed Personal Data Act. The National Supervisory Authority within the meaning of the GDPR is the Data Protection Supervisor. The duties of the Data Protection Supervisor are based on the provisions of the GDPR, the Data Protection Act and other legislation. The administrative fines under the GDPR are determined by a joint sanctioning panel formed by the Data Protection Supervisor and the Assistant Data Protection Officers. No fines can be imposed on state or municipal authorities in Finland.
No fines have yet been imposed in Finland to companies or 3rd sector organisations. Some data breaches of public sector has been uncovered and are being investigated by the Data Protection Supervisor and the police. The Criminal Code has removed the provision on the personal data offence and provides for the situation to be a data protection offence. Article 29 of the Data Protection Act contains a specific provision concerning the personal identification number. The personal identification number may be processed in the situations mentioned in this section. In Finnish companies, the GDPR and the Data Protection Act have not brought very big changes, because the Personal Data Act, which was abolished, contained largely the same provisions as in the GDPR. Even under the old law, data subjects had the right to verify their personal data. The GDPR, the Data Protection Act and the sector specific legislation form the whole set of data protection laws. The Publicity Act is also still in force.

GERMANY

Legislation:
GDPR (Federal Data Protection Act (2018))

Adequacy decision with EU:
N/A

Julia Dönch
julia.doench@bdo.de
+49 211 1371-326

Together with the GDPR, the revised Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG) came into force on 25th May 2018. The BDSG elaborates on the GDPR, in particular with regard to the figure of Data Protection Officer, as well as employee data protection. In late 2019, a further amendment act of the BDSG came into force, which applies corrections and adaptations to the current BDSG and more than 150 other national laws. While the German data protection authorities acted very cautiously in 2018, they announced stronger controls as of 2019. In the late summer of 2019, the German data protection authorities announced a new sanctioning model that is expected to lead to higher fines in the future. In fact, the fines have increased, even exceeding the million-mark in some cases. However, fines are still imposed in only a few of the reported incidents. The highest fine in Germany to date (mid of 2020) was imposed in October 2019 and amounts to 14.5 Million EUR. Studies show that there is still much to be done in implementing the GDPR in German companies. At the same time, data subjects in Germany are becoming more aware of data protection issues, and the rights of data subjects – especially the right of access – are being exercised more often. An important legal topic concerns the question of whether competitors may issue cease and desist warnings against GDPR infringements. This has still not been answered conclusively. Aside from this, it must be taken into account that court rulings based on the GDPR have only recently begun to accumulate.

GUERNSEY

Legislation:
The Data Protection (Bailiwick of Guernsey) Law 2017

Adequacy decision with EU:
YES

Steve Desmond
steve.desmond@bdo.gg
+44 1481 741629

Guernsey data privacy legislation is in line with EU GDPR and Adequacy has been agreed. Given that the major industry of Guernsey is financial services, the local legislation has some additional exemptions in place, for example in regard to Trusts and how they are treated. The differences between the two Channel Islands laws is not huge and historically a regulator has been shared. However, that is no longer considered practicable and now Guernsey and Jersey have their own regulators.

HUNGARY

Legislation:
GDPR (Act No. CXII of 2011 (Privacy Act))

Adequacy decision with EU:
N/A

Simon Emese
emese.simon@bdolegal.hu
+36 1 2353010

Since the GDPR took effect on 25 May 2018, Hungarian data protection regulations have been greatly modified to bring them in line with the requirements of EU law. The modifications were adopted, with a significant delay, in April 2019. The modifications affected many areas, including employment law, regulations on personal and property protection, commercial law, and rules pertaining to direct marketing. Although the Hungarian data protection authority has launched several thousand disciplinary procedures under the GDPR, it has adopted resolutions in approximately 30 cases; and only some of these involved the imposition of a fine. The highest fine so far amounted to HUF 30 million (approximately 95 million EUR). This was imposed due to the unlawful access control practices of a major music festival, where the data controller processed data without proper legal basis (in violation of the principle of purpose limitation) and without giving appropriate information to the data subjects. The next highest fine was HUF 11 million (approximately 35 million EUR). The rest of the fines have been much lower, ranging from approximately 300 euros to a few thousand euros. Fines have typically been imposed in connection with CCTV monitoring, for not allowing data subjects to exercise their rights (e.g. right to erasure and access) properly, for failing to report personal data breaches, for violating the principle of data minimization, and for failing to inform data subjects adequately. In Hungary, large and well-known companies are generally doing their best to comply with the GDPR, but a number of smaller companies have only started to bring their practices in line with the regulations with a significant delay, or not at all.

HONG KONG

Legislation:
Personal Data (Privacy) Ordinance (PDPO)

Adequacy decision with EU:
NO

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

PDPO was passed in 1995 and took effect from December 1996 (except certain 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'. This recommended that Hong Kong introduce a new privacy law based on the OECD Privacy Guidelines 1980 to ensure an adequate level of data protection to retain its status as an international trading centre and give effect to human rights treaty obligations. The PDPO is applicable to both the private and the public sectors. It is technology neutral and principle based. The Data Protection Principles ("DPPs" or "DPP"), which are 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. However, contravention of certain provisions of PDPO is an offence. Contravention of an enforcement notice issued by the Privacy Commissioner for Personal Data is also an offence which may result in a maximum fine of HK$50,000 and imprisonment for 2 years. Subsequent convictions can result in a maximum fine of HK$100,000 and imprisonment for 2 years.

ITALY

Legislation:
GDPR, Legislative Decree 196/2003 (Privacy Code) and subsequent amendments (Legislative Decree 101/2018)

Adequacy decision with EU:
N/A

Pierluigi Valentino
pierluigi.valentino@bdo.it
+39 335 6216651

At the end of 2018, the Italian Authority (Data Protection Supervisor) acted with caution to give interested parties the opportunity to adapt to the new legislation, announcing more rigorous controls for the year 2019. The profile of the sanctions refers to many aspects of the GDPR. The Italian Authority for the protection of personal data is the body responsible for imposing sanctions, pursuant to art. 15, co. 3 of Legislative Decree 101/2018 (which has finally amended the Privacy Code): the same will have to take care to evaluate the violations on a case by case basis, so that the sanctions are provided for by the GDPR. With regard to criminal sanctions, if on the one hand the GDPR does not directly envisage it, the same admits on the other hand the faculty for the Member States to establish provisions relating to criminal sanctions for violations of the GDPR, as well as violations of national norms adopted by virtue of and within the limits of the Regulation (Recital 148). Also in this case the Decree intervened, modifying the relevant criminal cases already provided for by the Privacy Code and integrating them with further violations. The cases for which penal sanctions will be applicable are therefore, pursuant to the reformed Privacy Code provided for in the articles: 167 (Illicit data processing); 167-bis (Unlawful disclosure and dissemination of personal data subject to large-scale processing); 167-ter (Fraudulent acquisition of personal data subject to large-scale processing); 168 (Falsity in the declarations to the Guarantor and interruption of the execution of the tasks or the exercise of the powers of the Guarantor); 170 (Failure to comply with the provisions of the Authority). The legislator has deemed it appropriate to extend the applicability of criminal sanctions not only to cases in which the fraud of the agent aimed at making a profit for himself or for others (as was foreseen before the reform) is ascertained, but also to the cases in which the agent has acted for the purpose of causing damage to others (specifically in relation to articles 167, 167-bis and 167-ter of the Code). Following the entry into force of the new privacy legislation, interested parties in Italy have become more aware of data protection issues and the rights of data subjects (in particular the right to access and delete data). An important legal argument concerns the issue of violations (and communications to the Guarantor) and the disputes in court. Despite this, issues relating to the GDPR are not yet a major focus of disputes in the Italian courts.

ISRAEL

Legislation:
Protection of Privacy Law 5471-1981 (PPL) and the Privacy Protection Regulation (Data Security) 577-2017

Adequacy decision with EU:
YES

Gilad Yaron
GiladY@bdo.co.il
+972-52-6755514

Israel is among the world's pioneers in Data Protection regulations. The data privacy law was enacted on 1981. Several regulations were enacted therefrom, with the Privacy Regulations (Data Security), enacted on 2017, being the latest and most important one.

The basic principles of the Israeli privacy regulations include transparency, lawfully basis for processing, purpose limitation, Data minimization, Proportionality & Retention.

The individual rights include the right to access data, the right to rectification of errors, the right to deletion, the right to object to processing and more.

The Privacy Regulations (Data Security) apply to both private and public sectors and establish organizational measurements aimed at making data security part of the management framework of all organizations processing personal data.

The regulations classify information repositories to four groups according to the level of risk created by the processing activity in those repositories: high, medium, basic and repositories controlled by individuals that grant access to no more than three authorized individuals.

The duties of the controllers are determined with accordance to the level of risk. The level of risk is defined by the data sensitivity, the number of data subjects and number of authorized access holders.

In specific circumstances, the privacy protection authority (PPA) may instruct a controller/processor to implement additional controls in order to strengthen the security level of its activities, or exempt a controller/processor from applying specific obligations in the regulations. For example, PPA may instruct low level risk repositories to implement provisions that apply on medium risk repositories, and when justified, PPA may exempt medium risk databases from specific provisions.

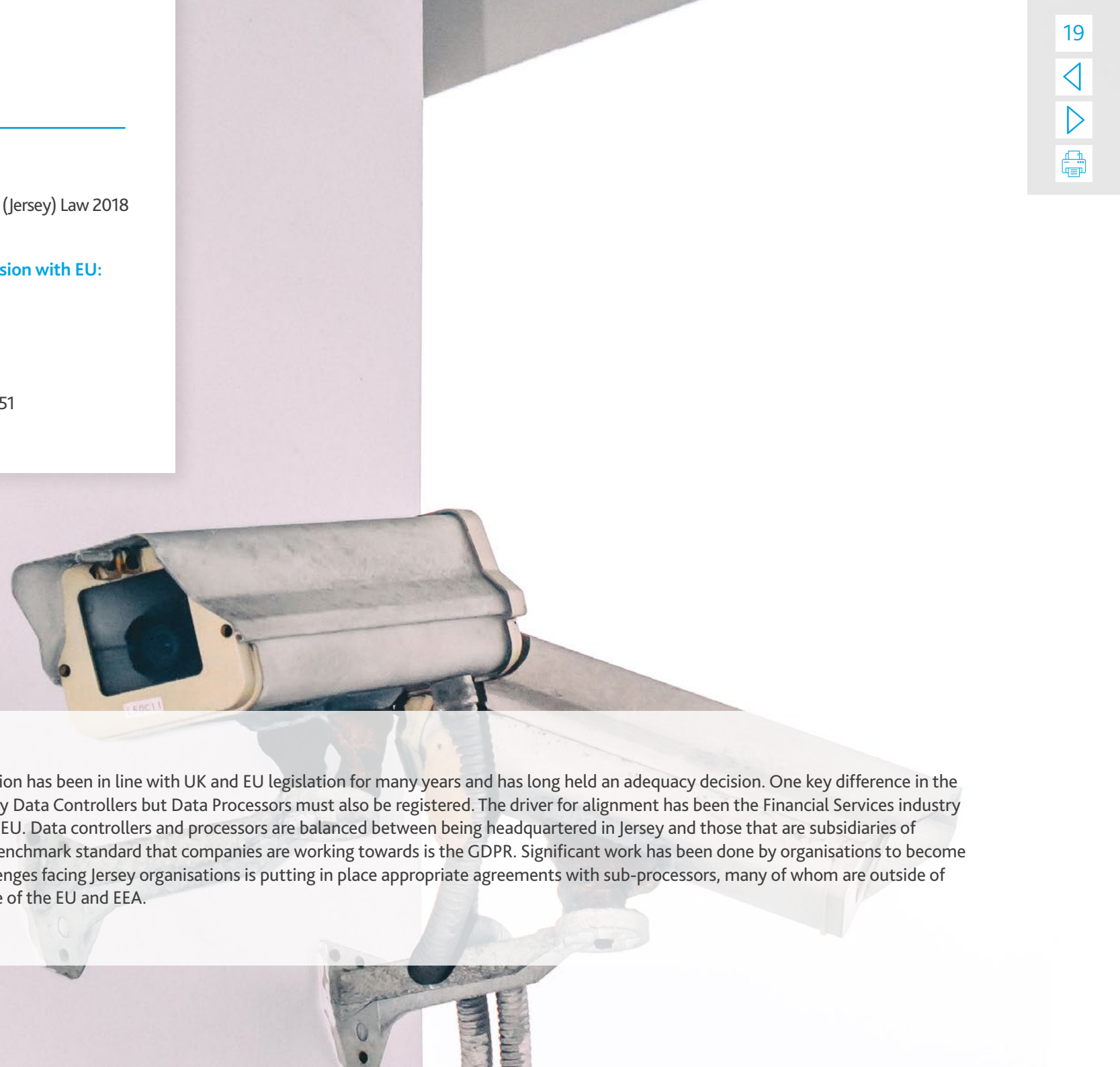
Israel is one of a few countries which qualify with the EU adequacy decision.

JERSEY

Legislation:
Data Protection (Jersey) Law 2018

Adequacy decision with EU:
YES

Damon Greber
dgreber@bdo.je
+44 1534 844451



Jersey's data protection legislation has been in line with UK and EU legislation for many years and has long held an adequacy decision. One key difference in the Jersey legislation is that not only Data Controllers but Data Processors must also be registered. The driver for alignment has been the Financial Services industry which delivers services into the EU. Data controllers and processors are balanced between being headquartered in Jersey and those that are subsidiaries of groups. Regardless of this the benchmark standard that companies are working towards is the GDPR. Significant work has been done by organisations to become compliant, one of the key challenges facing Jersey organisations is putting in place appropriate agreements with sub-processors, many of whom are outside of the jurisdiction and also outside of the EU and EEA.

LATVIA

Legislation:
GDPR (Personal Data Processing Law of 5 July 2018)

Adequacy decision with EU:
N/A

Rolands Zigurs
rolands.zigurs@bdolaw.lv
+371 6722 2237

Although the issue of personal data protection took the spotlight in 2018, Latvia has had a regulatory framework - the Personal Data Protection Law - in place since 2000. When the provisions of the new EU GDPR became applicable in May 2018, the new EU framework for the processing of personal data did not significantly alter the basic principles. However, the framework received a significant update and, among other changes, GDPR introduced larger penalties for data protection violations. On 5th July 2018 the new Latvian Personal Data Processing Law entered into force, thus establishing a legal framework for a system to protect the personal data of natural persons on a national level, as well as providing the Data State Inspectorate the necessary powers to monitor compliance with GDPR.

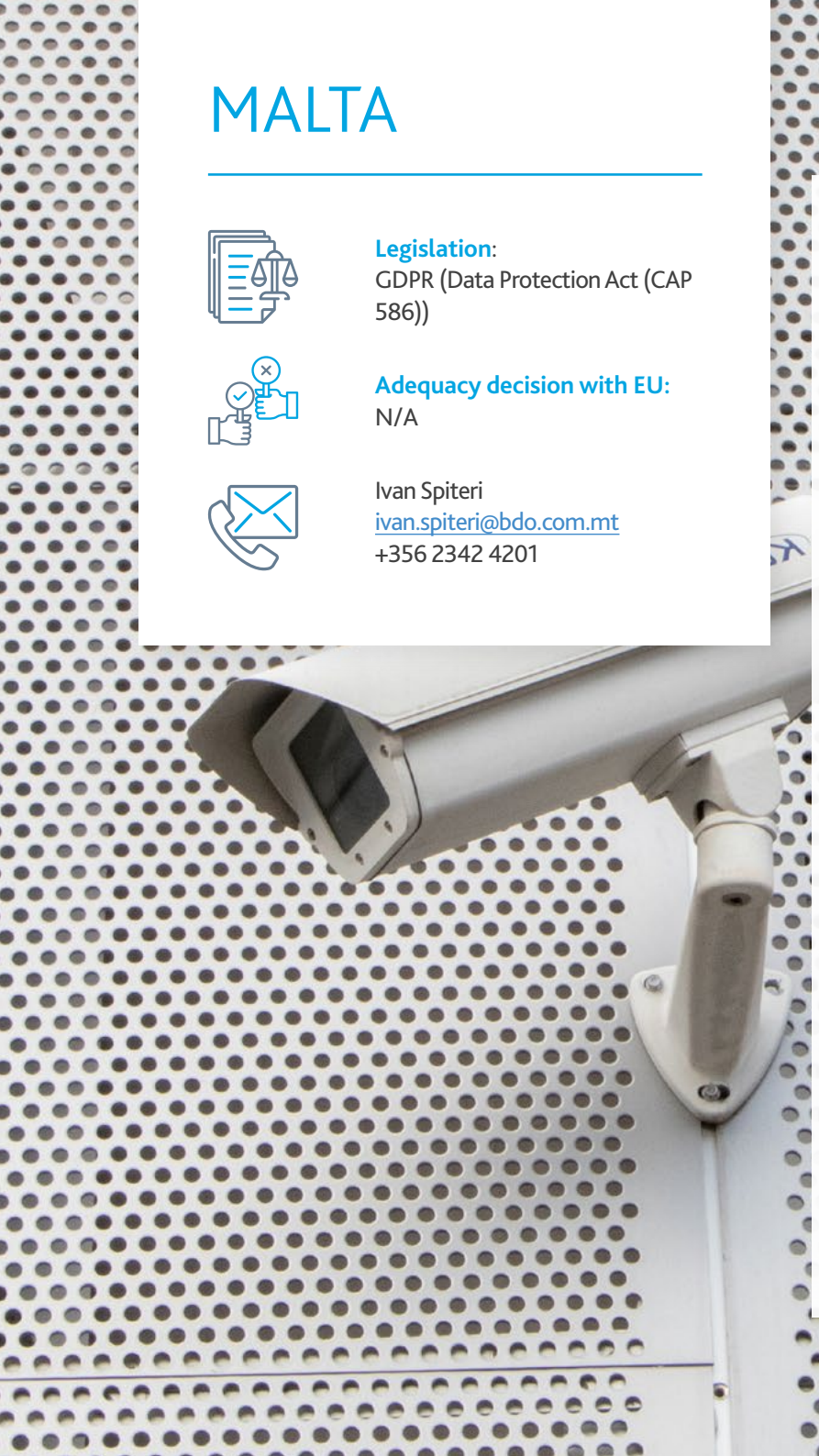
There is still no common understanding of the GDPR rules among entrepreneurs in Latvia. There is also, at times, a misleading notion that GDPR applies only to large companies that employ a large number of employees or have large customer databases. The Data State Inspectorate has stated that the number one challenge for Latvian businesses is to ensure adequate security of personal data in a digital environment. The Latvian Data State Inspectorate normally applies sanctions only in cases where the controller has not responded to the Inspectorate's request to terminate the violation. So far, the Data State Inspectorate has reviewed 140 cases of non-compliance with GDPR, and fines ranging from 200 to 7,000 EUR have been imposed in 40 cases. Most frequently, infringements are related to insufficient information to the data subject (the principle of transparency).

MALTA

Legislation:
GDPR (Data Protection Act (CAP 586))

Adequacy decision with EU:
N/A

Ivan Spiteri
ivan.spiteri@bdo.com.mt
+356 2342 4201



The Data Protection Act, 2018 (Chapter 586 of the Laws of Malta) and subsidiary legislations implemented under it, legislate and further regulate the important obligations of the GDPR. The Act itself embraces a simple approach for GDPR implementation, of which most provisions relate to the role and functions of the Office of the Information and Data Protection Commissioner (IDPC), which is the local regulator for data protection. The following are the subsidiary legislations introduced under the Act as part of GDPR implementation:

- SL 586.01 - Processing of Personal Data (Electronic Communications Sector) Regulations
- SL 586.04 - Processing of Personal Data (Protection of Minors) Regulations
- SL 586.07 - Processing of Personal Data (Education Sector) Regulations
- SL 586.08 - Data Protection (Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties) Regulations
- SL 586.09 - Restriction of the Data Protection (Obligations and Rights) Regulations
- SL 586.10 - Processing of Data concerning Health for Insurance Purposes Regulations
- SL 586.11 - Processing of Child's Personal Data in Relation to the Offer of Information Society Services Regulations
- SL 586.06 - Processing of Personal Data for the Purposes of the General Elections Act and the Local Councils Act Regulations

The IDPC investigated 76 data subject complaints and 148 breach notifications from May 2018 to May 2019. According to the IDPC, in all cases, the severity of the incidents was classified as either low or medium. Since GDPR came into effect, the IDPC has imposed a total of 26,000 EUR in administrative fines. The fines imposed have so far been less harsh compared to other countries in the EU. However, the IDPC has stated that it will be increasingly stringent so as to implement and enforce GDPR and the Data Protection Act, 2018, in their true spirit. Reports show that there is still much to be done in implementing the GDPR in Maltese companies. At the same time, data subjects in Malta are becoming more aware of data protection issues, and their respective rights.

NETHERLANDS

Legislation:
GDPR (Dutch GDPR Implementation Act 'UAVG')

Adequacy decision with EU:
N/A

Menno Weij
menno.weij@bdolegal.nl
+31 610 919 024

Since the 25th May 2018, both the GDPR and the Dutch GDPR Implementation Act ('UAVG') apply in the Netherlands. After evaluation of the GDPR and UAVG, The Netherlands discovered several problem areas. The Dutch Minister for Judicial Protection announced that there is a need for more explicit grounds for processing data in the following situations:

- Processing biometric data for access purposes
- Processing special categories of personal data by accountants
- Processing special categories of personal data by the whistleblowing authorities
- Processing of health-related data by patients' associations, when for internal use

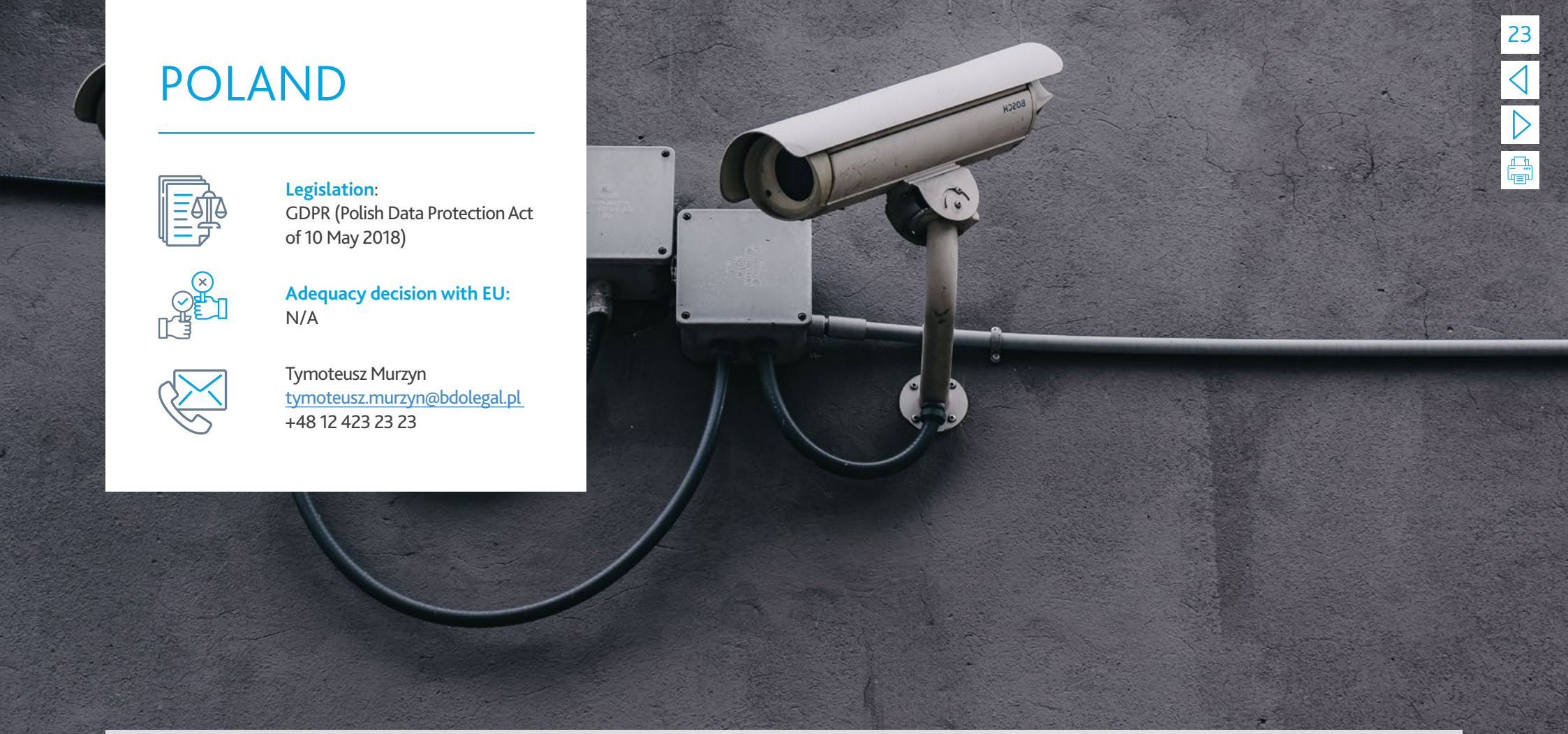
Some other additional changes to the UAVG are also being considered. The house of representatives will discuss these changes during the first quarter of 2020. In July 2019, the first fine under the GDPR in the Netherlands was applied to the Haga hospital in The Hague. The hospital failed in its internal security of electronic patient records, which led to excessive access to electronic patient records by employees. Therefore, the Dutch Data Protection Authority fined the hospital for 460,000 EUR, plus a maximum penalty of 300,000 EUR, in case the hospital does not undertake the necessary security measures. The hospital has appealed this fine. The Dutch Data Protection Authority has also announced an investigation into the use of (tracking) cookies on websites.

POLAND

Legislation:
GDPR (Polish Data Protection Act of 10 May 2018)

Adequacy decision with EU:
N/A

Tymoteusz Murzyn
tymoteusz.murzyn@bdolegal.pl
+48 12 423 23 23



In connection with the start of the application of GDPR provisions, Poland adopted a new data protection act on the 10th May 2018, replacing the old act of 1997. Furthermore, another sizeable act was adopted on the 21st February 2019, amending the existing law in order to fully comply with GDPR. The changes included in this act affected inter alia labour, insurance, telecommunication, banking, consumer protection and administrative provisions. The application of GDPR in Poland certainly proved to be a problem for many. Some organisations still struggle to fully comply with new rules, whilst some became overzealous due to the fear of high fines. The complexity and size of GDPR provisions contributed to the emergence of many "GDPR myths" and paradoxically, to new methods of fraudulent exploitation of personal data. In the first year of application of GDPR provisions, the Polish Data Protection Office has imposed two fines. The first of these was broadly discussed; a company processing data gathered mainly from public registers for the purpose of maintaining its own commercial database failed to meet the information obligations towards affected persons and was fined with 220,000 EUR.

PORTUGAL

Legislation:
GDPR (Portuguese Law 58/2019, 8 August 2019)

Adequacy decision with EU:
N/A

Luís Ricard Crispim
luis.crispim@bdo.pt
+351 937 990 341

The General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) began to apply from 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 key aspects of this Law are the age of natural persons to consent (fixed in 13 years), the rights of deceased persons, the determination of fines amounts (depending on the size of the companies) and the legal obligation 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. In spite of its current legal limitations, in October 2018, the CNPD applied a fine of 400,000 EUR on the Hospital of Barreiro and Montijo ('CHBM'), under the GDPR. Recently, the most significant Portuguese consumer protection association ('DECO'), was fined 107,000 EUR for sending unsolicited e-mails. A stronger CNPD dynamism is expected for 2020, with a new government and a new budget. There is still much to be done in implementing the GDPR in Portuguese companies. There are some grey zones, in particular concerning the processing of health data by insurance companies which should be clarified by the law or supervisory authority. 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.

ROMANIA

Legislation:
GDPR (Romanian Data Protection Law 363/2018)

Adequacy decision with EU:
N/A

Catalina Damaschin
catalina.damaschin@tudor-andrei.ro
+40 744 534 220

Complementary to the GDPR, national data protection laws were also passed in 2018. The respective laws provide measures for the implementation of the Regulation and the processing of personal data in order to carry out the activities involved in prevention, discovery, investigation, criminal prosecution and crime fighting, as well as educational and safety measures, the execution of penalties and maintaining and ensuring public order and safety by the competent authorities. Despite the fact that a Romanian governing body was established long before the introduction of the European data protection regulation, the transition to the GDPR was challenging. A number of public institutions still experienced issues with the provisions of the Regulation in its infancy, in the sense that many of them rejected documents that contained personal information transmitted via e-mail or fax, on the grounds that this might be in contradiction with data protection laws. Consequently, many people felt frustrated by the fact that they had to personally deliver such documents in writing.

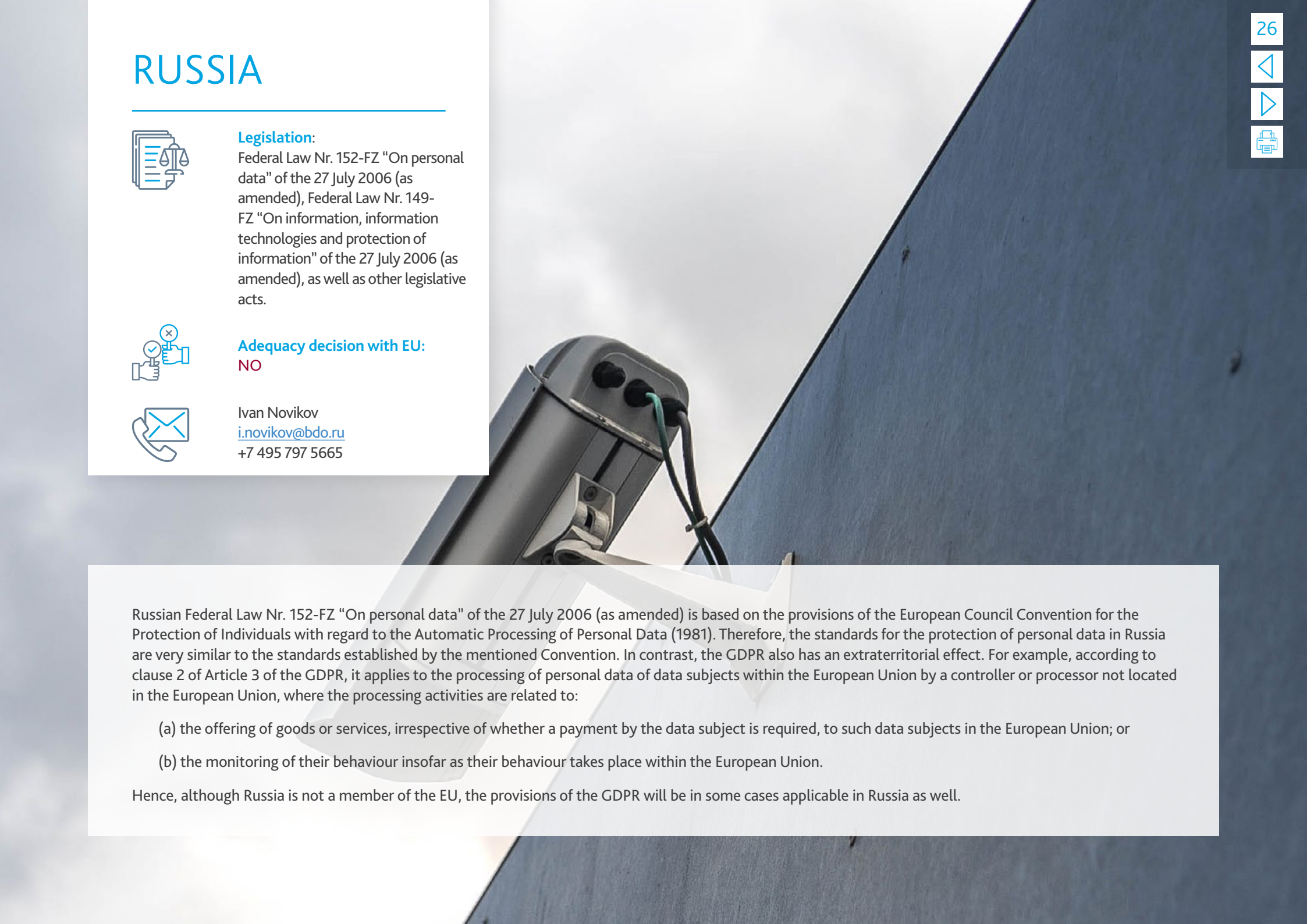
During the first year of implementation of the GDPR, businesses in Romania have increasingly prioritized transparency over their economic activity in order to comply with the Regulation. During this transition period, over 5,000 complaints about breaches of personal data security were reported. From the total number of complaints registered, only 57 resulted in fines and other administrative sanctions (warnings) by the national governing body. The first fine was handed out to a major bank, totaling 130,000 EUR, on the grounds that the bank was including its clients' personal numerical codes in e-mails regarding their bank statements.

RUSSIA

Legislation:
Federal Law Nr. 152-FZ "On personal data" of the 27 July 2006 (as amended), Federal Law Nr. 149-FZ "On information, information technologies and protection of information" of the 27 July 2006 (as amended), as well as other legislative acts.

Adequacy decision with EU:
NO

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



Russian Federal Law Nr. 152-FZ "On personal data" of the 27 July 2006 (as amended) is based on the provisions of the European Council Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (1981). Therefore, the standards for the protection of personal data in Russia are very similar to the standards established by the mentioned Convention. In contrast, the GDPR also has an extraterritorial effect. For example, according to clause 2 of Article 3 of the GDPR, it applies to the processing of personal data of data subjects within the European Union by a controller or processor not located in the European Union, where the processing activities are related to:

(a) the offering of goods or services, irrespective of whether a payment by the data subject is required, to such data subjects in the European Union; or

(b) the monitoring of their behaviour insofar as their behaviour takes place within the European Union.

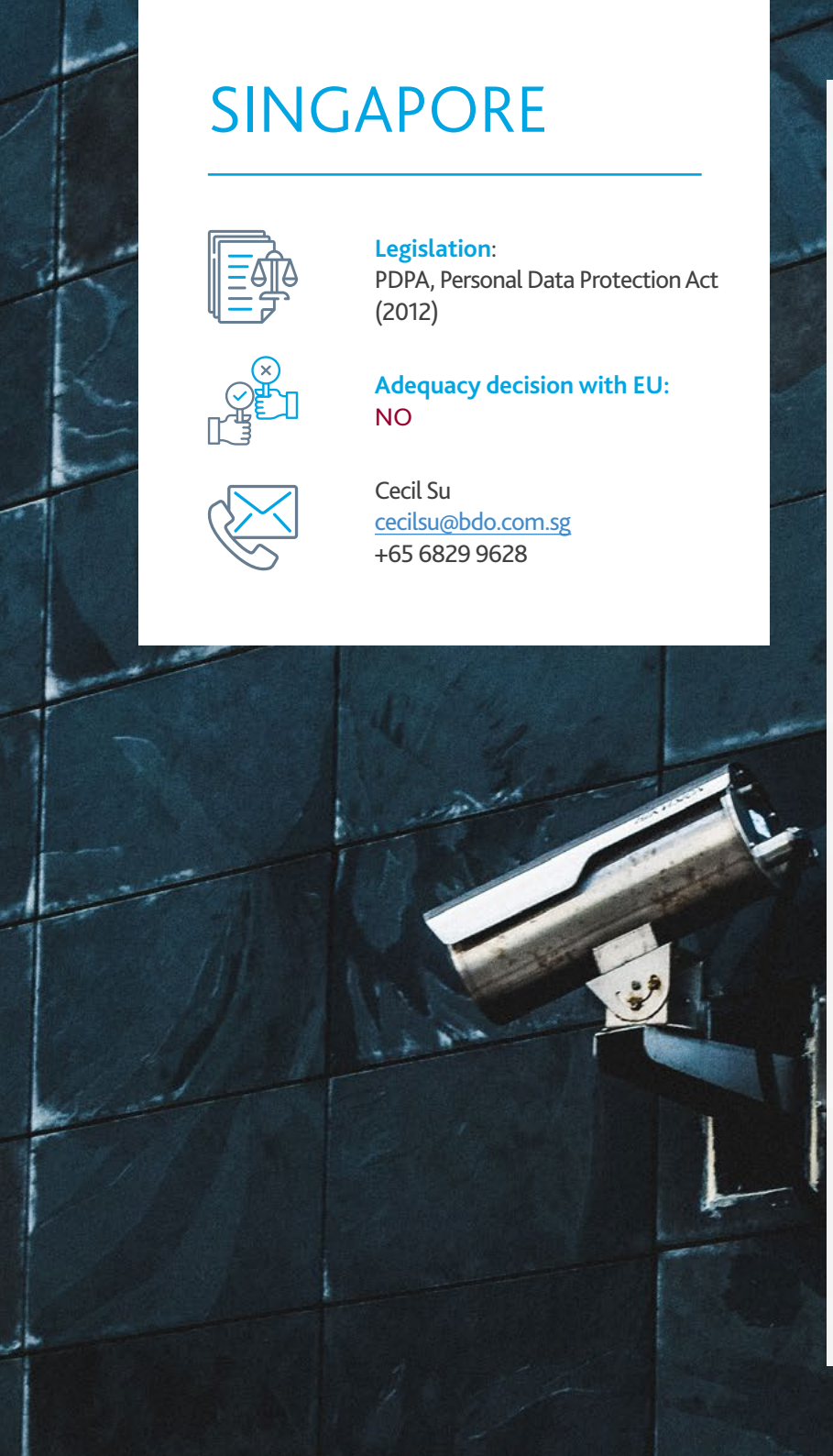
Hence, although Russia is not a member of the EU, the provisions of the GDPR will be in some cases applicable in Russia as well.

SINGAPORE

Legislation:
PDPA, Personal Data Protection Act (2012)

Adequacy decision with EU:
NO

Cecil Su
cecilsu@bdo.com.sg
+65 6829 9628



In response to the evolving digital landscape, significant developments to Singapore's data protection law were proposed or occurred in 2018. As part of the ongoing review of the Personal Data Protection Act 2012 ("PDPA"), the Personal Data Protection Commission ("PDPC") issued a public consultation on 27 April 2018 entitled "Public Consultation for Managing Unsolicited Commercial Messages and the Provision of Guidance to Support Innovation in the Digital Economy" ("Consultation Paper"), under which it was proposed that the Do Not Call ("DNC") provisions and the Spam Control Act be merged into a single legislation governing all unsolicited commercial messages. In addition, the PDPC proposed to introduce an Enhanced Practical Guidance ("EPG") framework for the PDPC to provide organisations guidance with regulatory certainty regarding complex or novel compliance issues. The developments summarised above are a continuation of the PDPC's efforts to pivot from a culture of compliance to accountability in personal data management, whereby organisations are encouraged to adopt a culture of accountability and demonstrate to customers and data subjects that they have proactively identified and addressed risks to personal data. The Data Protection Trustmark certification scheme, which was launched by the Infocomm Media Development Authority and PDPC in January 2019, will be a key element of the pivot to accountability, through which certified organisations can better gain consumers' trust and thereby obtain competitive advantage. The impending mandatory data breach notification regime described in the 2017 Digital Economy Consultation enshrines the accountability of organisations to individuals whose personal data they are processing, through notification of a data breach occurring with respect to those individuals' personal data. On 20 February 2018, Singapore became the sixth Asia-Pacific Economic Cooperation ("APEC") economy to participate in the APEC Cross-Border Privacy Rules ("CBPR") system, and the second APEC economy to participate in the Privacy Recognition for Processors ("PRP") system. The two systems have the same goal – to harmonise data protection standards across jurisdictions in order to facilitate cross-border data flow for organisations. There are currently eight participating economies in the APEC CBPR: Australia, Canada, Japan, Mexico, Singapore, South Korea, Taiwan and the US. In Singapore, the PDPC is also in the midst of nominating an accountability agent, who will implement the two systems for interested data controllers and data processors to be certified as such. In 2018, as was the case in 2016 and 2017, 12 breaches of the Protection Obligation remained the most common among the PDPC's reported decisions. Among the PDPC's 28 reported decisions in 2018, 19 concerned breaches of the Protection Obligation. Notably, the nature of such breaches of the Protection Obligation has somewhat evolved. In the first survey of the PDPC's enforcement activity in 2016, it was remarked that in a number of the enforcement decisions, many organisations appeared to lack an overall awareness of and sensitivity to the data protection obligations under the PDPA, in particular the Protection Obligation. In 2018, there were still some organisations similarly taken to task for failing to develop and implement policies and practices that are necessary for the organisation to meet its obligations under the PDPA.

SLOVENIA

Legislation:
GDPR (Law on Data Protection (ZVOP-1,2004))

Adequacy decision with EU:
N/A

Mateja Vrankar
mateja.vrankar@bdo.si
+386 1 53 00 920

Slovenia has not used the transition period between the adoption of the GDPR and 25 May 2018 to adopt new national Law on Data Protection. At the moment the situation is that the GDPR is in force and applicable in combination with the old Law on Data Protection (ZVOP-1, adopted in 2004). New Law on Data Protection (ZVOP-2) is still in the parliamentary procedure. A draft of the new law is publicly available and known. Business entities and individuals are well aware and sensitive regarding data protection and especially rights of individuals and limitations connected with processing of personal data. Data Protection Officers have been appointed in conformity with GDPR. Many businesses have even appointed DPOs on voluntary basis. Businesses are already preparing for the new national regulation (ZVOP-2), when also the GDPR will be fully applicable in Slovenia. Due to regulation of sanctions in the old Law on Data Protection (ZVOP-1), Data Protection Regulator (Urad Informacijskega Pooblaščenca) is sanctioning violations with very low (even symbolic, compared with GDPR) fines. At the moment, fines defined in the GDPR can't be applicable in Slovenia (as per the interpretation of the regulator). In cases of violations of GDPR which are not covered with ZVOP-1, the regulator is issuing warnings. Inspection activities were only partly intensified. While preparing for the implementation of new data protection regulation, many businesses have also explicitly addressed information and cyber security issues. There have been no judicial cases connected to GDPR to date.

SOUTH AFRICA

Legislation:
Protection of Personal Information Act 4 of 2013

Adequacy decision with EU:
NO

Carl Bosma
cbosma@bdo.co.za
+27214178730

The Protection of Personal Information Act ("POPIA") was assented to on the 19th of November 2013. On 1 July 2020 the majority of the legislation was brought into effect by the President of South Africa. The legislation incorporates a twelve month grace period which means that "Responsible Parties" (known as "data controllers" in the rest of the world) will need to be compliant by 1 July 2021. Only two sections of the Act, namely Sections 110 and 114(4), which deal with the amendment of laws; and the transfer of functions from the South African Human Rights Commission to the Information Regulator regarding the Promotion of Access to Information Act (PAIA) have been delayed until 31 June 2021 POPIA contains similar provisions to the GDPR, and the conditions for the lawful processing of personal data echo the principles set out in the GDPR. One of the main distinctions between most data protection laws and POPIA, is that the protection which POPIA affords extends to juristic persons and not only to natural persons. The South African Information Regulator, being the equivalent of a Data Protection Authority or the UK's Information Commissioner's Office, has taken a proactive approach to investigating data breaches - notwithstanding the fact that data breach reporting was voluntary until the commencement date. Now that the commencement date has been announced, companies domiciled in South Africa or companies who process personal information by making use of automated or non-automated means within South Africa, have a grace period of one year to comply with POPIA. After the grace period, we are likely to see action from the Information Regulator, which has the power to impose fines of up to R10 million or imprisonment for a maximum period of 12 months for a party who commits an offence (although this might be extended as a result of COVID). Being the first Act in South Africa's history to deal specifically with the protection of personal information, it is likely that many companies will need to act quickly in order to comply within the one-year grace period, as many of the requirements are entirely new. We have seen that due to the extra-territorial reach of the GDPR, and the global nature of business, a proportion of companies have already taken steps to comply with GDPR, thereby reducing the burden in terms of ensuring compliance with POPIA.

SPAIN

Legislation:
GDPR, Spanish Data Protection Act (2018)

Adequacy decision with EU:
N/A

Roger Perez
roger.perez@bdo.es
+34 696 723 386

Together with the GDPR, which came into force on 25th May 2018, the new Spanish Data Protection Act (Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales, LOPDGDD) came into force at the end of 2018. The LOPDGDD complements the GDPR's dispositions. In particular, it regulates with more detail the figure of the Data Protection Officer, as well as employee data protection and "new" rights such as the "right to disconnect". While the Spanish data protection authorities acted very cautiously in 2018, in 2019, they sanctioned more frequently and with higher penalties. The highest fine in Spain to date reached almost 250,000 EUR, but the most relevant aspect is that there is a clear increase in the number of fines per month. Studies show that there is still much to be done in implementing the GDPR in Spanish companies. At the same time, data subjects in Spain are becoming more aware of data protection issues, and the rights of data subjects – especially the right to object and the right to erasure are being exercised more often. Moreover, the Spanish data protection authorities are currently working hard on the relationship between the specific regulation on cookies and the GDPR, as has been reflected in some relevant sanctioning resolutions.

SWITZERLAND

Legislation:
Swiss Federal Act on Data Protection of June 1992

Adequacy decision with EU:
YES

Philippe Duenner
philippe.duenner@bdo.ch

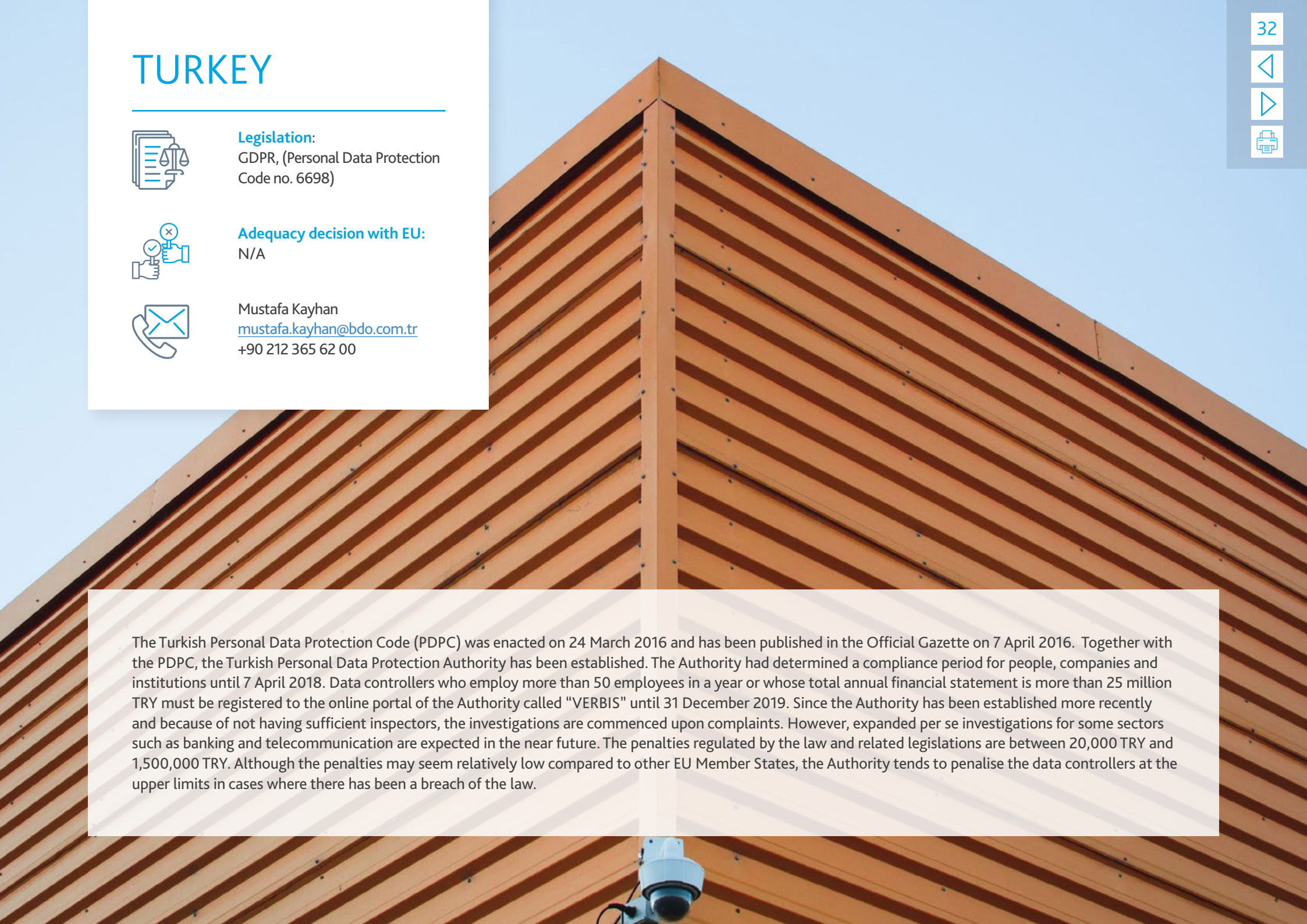
The current Swiss Federal Act on Data Protection (FADP) was enacted in 1992 and reflected the main principles of the former EU data protection directive. Currently, the FADP is under full revision and a new Swiss Federal Data Protection Act (nFSDPA) is expected to be enacted in 2020. The draft bill provides for an alignment to the GDPR, although less detailed and substantial. The main principles of the nFSDPA are similar to the GDPR but have many deviations in the details. Contrary to the sanctions of the GDPR, which are applied to organisations themselves, sanctions under the nFSDPA will be penal sanctions for individuals responsible for data protection within the organisation, therefore, within a Swiss corporation, sanctions will ultimately be applied to board members. Under the current FADP a formal DPO is not compulsory, however, such an appointment may relieve the company from some formal obligations. This will be similar under the nFSDPA.

TURKEY

Legislation:
GDPR, (Personal Data Protection Code no. 6698)

Adequacy decision with EU:
N/A

Mustafa Kayhan
mustafa.kayhan@bdo.com.tr
+90 212 365 62 00



The Turkish Personal Data Protection Code (PDPC) was enacted on 24 March 2016 and has been published in the Official Gazette on 7 April 2016. Together with the PDPC, the Turkish Personal Data Protection Authority has been established. The Authority had determined a compliance period for people, companies and institutions until 7 April 2018. Data controllers who employ more than 50 employees in a year or whose total annual financial statement is more than 25 million TRY must be registered to the online portal of the Authority called "VERBIS" until 31 December 2019. Since the Authority has been established more recently and because of not having sufficient inspectors, the investigations are commenced upon complaints. However, expanded per se investigations for some sectors such as banking and telecommunication are expected in the near future. The penalties regulated by the law and related legislations are between 20,000 TRY and 1,500,000 TRY. Although the penalties may seem relatively low compared to other EU Member States, the Authority tends to penalise the data controllers at the upper limits in cases where there has been a breach of the law.

UNITED KINGDOM

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

Adequacy decision with EU:
N/A

Christopher Beveridge
christopher.beveridge@bdo.co.uk
+44 203 860 6082

Together with the GDPR, the UK DPA 2018 came into force on 25 May 2018 and replaced the much earlier issued UK Data Protection Act 1998. In summary, the update to the UK DPA 2018 mirrors the GDPR, apart from some areas of derogation which allow Member States to make provisions for how they apply the GDPR in their country. An example of a derogation taken up by the UK DPA 2018 relates to the age of a child; such that the DPA 2018 states the age of consent at 13 as opposed to the GDPR which states it at 16. From a UK perspective, the implementation of the GDPR was a long and arduous journey and continues as such for a lot of organisations who have not yet made enough progress. The UK regulator (The Information Commissioner's Office (ICO)) is viewed as being one of the stronger regulators around and this has been seen in recent months through the issuance of some very significant sanctions to organisations that have breached the GDPR regulations post-enforcement. Two noticeable examples include the penalties issued to British Airways (£183 million) and The Marriott Hotel Group (£99 million). Compared to the previous highest sanction issued by the ICO (to Facebook as a result of the Cambridge Analytica scandal) at £500,000, this demonstrates that the UK regulator is not afraid to issue penalties where necessary. There is still significant work going on across the UK in respect of organisations attempting to push themselves into a position that would be classified as reasonable. Lots of organisations have struggled with time, resource and budgets constraints. Interestingly, the ICO softened its stance somewhat leading up to the GDPR enforcement date, recognising this was an issue for many organisations, however it still expected these organisations to have started the journey and to demonstrate they were fully accountable. This is a pattern that has continued. The ICO has really focused on the 'accountability' principle. There were lots of organisations in the UK that thought they had done enough and then downed tools. The ICO expects organisations to demonstrate and evidence that they are continuing to comply with the regulation, usually through a privacy compliance framework. Finally, we have Brexit hovering in the background. This will have an impact on International Data Transfers from a UK perspective along with the potential to be unable to transfer data freely between the UK and EU member states in a 'No Deal' scenario. The UK could also not be deemed an 'adequate' jurisdiction. All this will be decided in the future.

UNITED STATES

Legislation:
Various

Adequacy decision with EU:
NO

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

There is no single law for the United States of America (US) that covers all areas of privacy and data protection of personal information (personal data). At the federal level, there is a patchwork of laws that cover privacy in different areas. For example, marketing/advertising (CAN SPAM), healthcare (HIPAA/HITECH), financial firms (GLBA), and children's privacy (COPPA). Each of the 50 states and four (4) territories in the U.S. has its own unique law regarding data protection and the unauthorized access/loss/theft of personal information of its residents. In the event of a data breach, most of these laws require notification to consumers (data subject) and to the regulatory authority, the state's Attorney General. There is often an expectation that two years of credit protection will be offered to each affected individual. Fines can be imposed as well.

The California Consumer Privacy Act (CCPA), effective on January 1, 2020, is the first law in the US to provide privacy rights to individuals. The CCPA applies to the processing of the personal information of California residents by for-profit businesses that meet one of these thresholds: gross revenue over 25 million USD; personal information of 50,000 California residents, households, or devices; or 50% of annual revenues derived from 'selling' California residents' personal information.

Key features of the CCPA include:

- An expanded definition of personal information, which includes households, and inferences derived to create a profile reflecting an individual's preferences, characteristics, psychological trends, predispositions, behaviour, attitudes, intelligence, abilities, and aptitudes.
- The right to opt-out of the 'sale' of personal information, where 'sale' is broadly defined to include: selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating a California resident's personal information to another business for monetary or other valuable consideration. Businesses must provide a 'Do not sell my personal information' button on their website's home page with a link to an opt-out form.
- The right of private action, where, in the event of a data breach, businesses can be sued for $100 - $750 per consumer, per incident, or actual damages, whichever is greater.
- The right to delete
- The right to know (access) about their personal information that is collected, 'sold', or 'disclosed for a business purpose'. The response must include the categories of sources from which the personal information was collected and the categories of third parties to whom the personal information was sold or disclosed for a business purpose.

Businesses that operate in California and other locations must decide whether to provide California rights to all individuals, or only to California residents, the latter of which would require separate privacy policies, website home pages and provision of rights to know/delete/opt-out of sale for California residents. For context, California is currently the world's fifth largest economy, surpassed only by the gross domestic product (GDP) of the US, China, Japan and Germany. California has approximately 40 million residents.

The General Data Protection Regulation (GDPR) applies to U.S. entities that meet the GDPR Article 3 territoriality threshold for processing the personal data of European Union (EU) residents.

The Privacy Shield (www.privacyshield.gov) can be utilised by US businesses as a mechanism to become an adequate entity for receiving the personal data of EU and Switzerland residents. Enforcement is through the U.S. Department of Commerce.

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.