Bloomberg Law

Privacy and Security Law Report®

Reproduced with permission from Privacy & Security Law Report, 16 PVLR 977, 07/17/2017. Copyright © 2017 by The Bureau of National Affairs, Inc. (800-372-1033) http://www.bna.com

Data Protection

A Look at New Trends in 2017: Privacy Laws in Europe and Eurasia (non-EEA)

In this third article of a four-part series on the status of international data protection laws, the author explores developments in Europe and Eurasia (non-EEA), where 17 jurisdictions have comprehensive privacy laws. Other parts of the series cover East, Central, and South Asia and the Pacific, the Western Hemisphere, Africa and the Near East.



By Cynthia Rich

Introduction/Region at-a-Glance

With the implementation of the European General Data Protection Regulation (GDPR) in May 2018, attention of the business community has been focused on changes to the privacy rules in the 28 Member States of the European Union (as well as Switzerland and the other members of the European Economic Area or EEA). However, these changes are likely to have a ripple effect on existing privacy laws in the seventeen jurisdictions in Europe and Eurasia that are not part of

Cynthia Rich is a senior adviser at the Washington office of Morrison & Foerster LLP. As a member of the firm's international privacy and data security practice since 2001, Rich works with clients on legal issues relating to privacy around the world.

the EU/EEA: Albania, Andorra, Armenia, Azerbaijan, Belarus, Bosnia and Herzegovina, Georgia, Kosovo, Macedonia, Moldova, Monaco, Montenegro, Russia, San Marino, Serbia, Turkey, and Ukraine.

These laws contain the basic elements found under EU Member State laws, but some also have unique elements not found in other laws in the region or within the EEA. Almost half of the laws were enacted in the past five years, so it is unclear if or how soon these countries will amend these relatively new laws to follow the changes under the GDPR.

This article discusses current trends and new developments and examines the commonalities and differences among the privacy laws in the region.

Developments and Trends

Data Localization Over the past year, Russia's communications regulator, Roskomnadzor, the data protection authority (DPA), has been actively enforcing the data localization requirements that went into effect in September 2015. Under the Data Localization Law, personal information of Russian citizens must be stored in Russia and all operators who are subject to DPA notification requirements under the Federal Law No. 152-FZ on Personal Data must notify the DPA of the location of their personal data processing servers. Operators found to be in violation of these rules may have their websites blocked by the DPA and be listed on a public register of companies that have been found to be in violation of the law. In November 2016, the DPA blocked LinkedIn for refusing to locate data servers within Russia and most recently, in April and May 2017, it banned messenger services and communications apps such as Zello, BlackBerry, and Imo. In late May, the Russian government announced that it was drafting a new regulation to increase the DPA's compliance audit powers.

New Data Protection Law Turkey became the most recent country in this region to enact data protection legislation in March 2016. Some provisions of the Turkish Law took effect in April 2016 while others, such as cross-border transfers, access and correction, registration, and penalties, took effect in October 2016. Since that time, a data protection authority has been established and draft regulations on the creation of a database registry and on the deletion, destruction, and anonymization of Personal Data have been issued for public comment. According to the latter regulations, data controllers that are subject to the registration requirements will also be required to develop data retention and disposal policies. The regulations will be finalized and published shortly after the public comments period ends in late June 2016 and suggestions have been processed; it should enter into force immediately upon publication.

Enforcement There are wide variations within this region with respect to enforcement activities, depending on the maturity of the regulatory regime. In some countries, there is no real data protection authority or DPA (Belarus) or the DPA was only established in the past couple of years (Azerbaijan and Georgia). For example, in Georgia, the DPA's enforcement powers vis-a-vis the private sector only began in late 2014 but the DPA has already imposed fines for law violations, such as for failing to obtain consent, disclosing personal information without proper legal grounds, or violating direct marketing rules by not providing the ability to opt out.

Countries such as Kosovo, Macedonia, and Moldova are more focused on building awareness of individuals' privacy rights and private and public sector obligations under the law; although all three conduct routine inspections and issue enforcement actions when violations are found. In Bosnia, the DPA has been largely focused on public sector processing of personal information.

In contrast, the DPA in Albania, which has had a privacy law in place since 2008, conducts regular inspections, issues corrective orders when violations are found and then conducts follow up inspections to confirm the changes have been implemented. It issues administrative fines if the organization fails to implement its orders. In 2015, in response to complaints received, the Albania DPA conducted a joint investigation with the Italy DPA of call center companies. Fines were issued to call center companies with law violations.

In Serbia, the DPA has been advocating for the adoption of a new data protection law to replace the existing law which it characterizes as inadequate and dysfunctional. According to the DPA, there are a number of issues that are not regulated properly, such as video surveillance, processing of biometric data, access rights, cross-border transfers, the Commissioner's powers, and data security. In March 2017, the DPA issued for public consultation a draft law modeled after the GDPR. The model law is expected to be presented to the government in mid-June for its consideration and action.

Common Elements Found in European/Eurasian Laws

Notice All of the laws in the region include some type of notice obligation. That is, every law requires that individuals be told what personal information is collected, why it is collected and with whom it is shared.

Choice/Legal Basis for Collection and Use (Processing) Every privacy law contains some kind of choice element and requires organizations to have a legal basis on which to process personal information. Similar to those found in the EU, these legal bases include the following: the individual has consented to the processing (consent); the processing is necessary to fulfill a contract (contractual necessity); the processing is necessary to pursue a legitimate interest of the controller (legitimate interests), the processing is necessary to protect the vital interests of the individual (vital interests), or the processing is necessary to comply with a legal requirement (legal requirement). However, depending on the jurisdiction, not all of these legal bases are available. For example, one third of the countries in the region do not permit organizations to rely on legitimate interests as a legal basis for their processing. Three of the countries in this group also do not provide for contractual necessity as a legal basis. One country permits processing on the basis of consent only.

Security Furthermore, all of the laws require organizations that collect, use, and disclose personal information to take reasonable precautions to protect that information from loss, misuse, unauthorized access, disclosure, alteration and destruction. Two thirds of the countries have specified in greater detail how these obligations are to be met.

Access & Correction One of the core elements of every privacy law is the right of all individuals to access the information that organizations have collected about them and, where possible and appropriate, correct, update or suppress that information. Interestingly, compared to their EU and Asian counterparts, many countries in this region require organizations to respond to access and correction requests in a much shorter period of time. Slightly more than half of the countries (9) require organizations to respond to access and/or correction requests within 15 days or less (two require as little as five days); more than one third (7) require responses within 30 days and two others do not specify any time periods.

Data Integrity Organizations that collect personal information must also ensure that their records are accurate, complete and kept up-to-date for the purposes for which the information will be used.

Data Retention Generally these laws require organizations to retain the personal information only for the period of time required to achieve the purpose of the processing. Specific retention periods of time are not prescribed in many of the laws in this region, with Russia being the most notable exception. Russia requires that when the purposes have been achieved or if the individual withdraws his or her consent to the processing, the operator must discontinue the processing, destroy the data within 30 days, and notify the individual that his or her data has been destroyed.

OVERVIEW OF DATA PRIVACY LAWS IN NON-EU/EEA COUNTRIES

Countries With Privacy Laws	Year Enacted (Amended)	Registration Requirement	DPO Required ¹	Cross-border Limitations	Data Breach Notification Requirement ²
Europe/Eurasia (Non-EEA) (17)		15	5	16	4
Albania	2008 (2014)	Yes	Yes	Yes	No
Andorra	2004	Yes	No	Yes	No
Armenia	2015	No	No	Yes	Yes
Azerbaijan	2010	Yes	No	Yes	No
Belarus	2008	No	No	No	No
Bosnia and Herzegovina	2006	Yes	No	Yes	No
Georgia	2012 (2014)	Yes	No	Yes	No
Kosovo	2010	Yes	No	Yes	No
Macedonia	2005	Yes	Yes	Yes	No
Moldova	2012	Yes	No	Yes	Yes
Monaco	1993	Yes	No	Yes	No
Montenegro	2012	Yes	Yes	Yes	No
Russia	2007 (2014)	Yes	Yes	Yes	Yes
San Marino	1995	Yes	No	Yes	No
Serbia	2009	Yes	No	Yes	No
Turkey	2016	Yes	No	Yes	Yes
Ukraine	2011 (2015)	Yes	Yes	Yes	No

¹ In some jurisdictions, the appointment of a Data Privacy Officer (DPO) may exempt the organization from its registration obligations.

Source: MORRISON & FOERSTER LLP

Bloomberg BNA

Eurasia Data Privacy

Country-by-Country Review of Differences

ALBANIA

The Protection of Personal Data Law (Albanian Law) which became effective in 2008 and was amended mostly recently in 2014, regulates the processing of all personal information of natural persons by both the public and private sectors.

In Brief The Albanian Law requires database registration, imposes data protection officer (DPO) and special data security obligations, and restricts cross-border transfers to countries that do not provide adequate protection. However, there are no data breach notification requirements.

Special Characteristics

Data Protection Authority The Commissioner for Information Rights and Protection of Personal Data (Albania DPA), an independent administrative authority, is

² This chart identifies only those jurisdictions that have enacted legally binding data breach notification requirements. It does not reflect the local notification practices or the DPA's expectations about whether organizations should provide notice. Consequently, organizations should consider a variety of factors, not just whether the rules are legally binding.

charged with overseeing compliance with the Albanian Law. It carries out online and onsite inspections on its own initiative and in response to complaints and issues fines, most commonly in cases where organizations fail to implement its recommendations or orders. In 2015, in response to complaints received, it conducted a joint investigation of call center companies with the Italy DPA which resulted in administrative fines.

Access and Correction Access and correction requests must be responded to within 30 days.

Cross-Border Transfers There are no restrictions on cross-border transfer of personal information to recipients in countries that provide an adequate level of data protection. Albania has recognized all EU/EEA countries, signatories to the 1981 Council of Europe Convention for "Protection of Individuals with regard to Automatic Processing of Personal Data", and countries recognized by the European Commission as providing adequate protection. To transfer personal information to a country that does not provide an adequate level of protection, Albania DPA authorization is required or an exception under the law must apply. Exceptions include consent, contractual necessity, vital interests, or legal requirement.

Data Protection/Security Officer Large data controllers (with six or more persons engaged in data processing) must authorize in writing one or more persons responsible for internal data security supervision. One of the people appointed will serve as the contact person, registered with the Commissioner. Small data controllers (with less than six persons engaged in data processing) may, but are not required to, authorize in writing, one or more persons responsible for the internal security supervision.

Data Security Different organizational and technical data security measures are provided by law, depending on whether the controller is large or small. For example, small controllers must carry out a risk assessment procedure as a minimum standard measure of data security. Large controllers must apply and maintain an information security management system (SMSI). SMSI is based on the identification, assessment and mitigation of risks threatening personal information security while taking in consideration (i) the information technology and communication system used to process personal information, (ii) all manual forms of processing personal information and (iii) the physical security of premises and the security of the personnel, electronic and movable equipment. The risk assessment and treatment are part of the mandatory Information Security Policy of the Controller. Large controllers must carry out information security audits at least once per year and provide security training to employees. In addition, there are encryption requirements in connection with transfers of sensitive information and equipment used to process information through cloud computing platforms.

Legal Basis for Collection and Use To collect and use personal information, organizations must have a legal basis such as consent, contractual necessity, legal requirement, legitimate interests, or vital interests.

Registration The Albanian Law requires that controllers notify the Albania DPA about all categories of personal information they process for all purposes unless one of the limited exemptions applies. However, even when a notification exemption applies, minimum information on the data processing activities must be provided such as name and address of controller, categories and purposes of processed information and categories of recipients. Depending on the category of information, the controller must either register the processing or obtain an authorization from the Albania DPA prior to processing.

ANDORRA

The Protection of Personal Data Law (Andorran Law), which became effective in 2004, regulates public and private sector processing of all personal information of natural persons, except where the information relates to their business, professional or commercial activities. Andorra is regarded as providing an adequate level of protection for personal information transferred from the EU/EEA.

In Brief The Andorran Law requires database registration and the appointment of a DPO and restricts cross-border transfers to countries that do not provide adequate protection. In addition, the period of time within which organizations must respond to access requests is exceedingly short and there is no provision for processing personal information on the basis of legitimate interests. However, there are no special security and data breach notification requirements.

Special Characteristics

Data Protection Authority The Andorran Agency for Data Protection (Andorra DPA), an independent public authority, is responsible for overseeing compliance with the Andorran Law.

Access and Correction Organizations must respond to access requests within five working days and correction requests within one month.

Cross-Border Transfers Personal data may not be transferred to third countries that do not provide an equivalent level of protection unless consent or another of one of the limited exceptions such as contractual obligations, vital interests or legal requirements applies. Countries that provide an equivalent level of data protection are the EU Member States and countries found by the European Commission or the Andorra DPA to provide equivalent protection.

Legal Basis for Collection and Use To collect and use personal information, organizations must have a legal basis such as consent, contractual necessity, legal requirement, or vital interests.

Registration Controllers must register their databases with the DPA and update their registration records whenever there is a change in the information listed.

ARMENIA

The Law on Personal Data (Armenian Law), which became effective in 2015, regulates the processing of all

personal information of natural persons by both the public and private sectors.

In Brief The Armenian Law requires database registration, restricts cross-border transfers to countries that do not provide adequate protection, and imposes special security and breach notification obligations. In addition, the period of time within which organizations must respond to correction requests is exceedingly short and there are limited legal bases provided for the collection and use of personal information. However, there is no DPO obligation.

Special Characteristics

Data Protection Authority The Armenian Law provides for the establishment of the Authorized State Body for the Protection of Personal Data Processing (Armenia DPA); however, it is not yet established.

Access and Correction The Armenian Law does not specify a time period for responding to access requests. Corrections should be carried out (or refused) within five days after receiving the written request.

Cross-Border Transfers Personal data may be transferred cross border either with the consent of the individual or where the transfer is necessary to carry out processing previously consented to by the individual. In addition, Armenia DPA authorization is required to transfer to those countries that are not on the Armenia DPA's approved list of countries that provide adequate protection. A transfer permit is required in such cases. The Armenia DPA must also approve the organization's contractual clauses governing the transfer.

Data Breach Notification The data controller must make a public announcement without delay and notify the police and the Armenia DPA when a data security breach occurs.

Data Security Encryption measures are required to protect information systems containing personal information from loss, unauthorized access, illegal use and destruction, and illegal copying and disclosure. The Armenian Law also provides for the government to set security standards for information systems, physical records of biometric data and personal data storage technologies other that electronic information systems.

Legal Basis for Collection and Use Personal information may be processed only with the consent of the individual, where such processing is provided for or required by law, or where the data are publicly available.

Registration The Armenia DPA has the right to require data controllers to notify it about the collection or processing of personal information; otherwise such notification is voluntary.

AZERBAIJAN

The Law on Personal Data (Azerbaijani Law), which became effective in 2010, regulates the processing of all personal information of natural persons by both the public and private sectors. The Azerbaijani Law differentiates personal information according to public and confidential categories. Public data are (i) data that are depersonalized or anonymized, (ii) data that are de-

clared public by the individual or (iii) data that are included in an information system created for general use with the consent of the individual. A natural person's name, last name, and patronymic will always be considered to be public data.

In Brief The Azerbaijani Law requires database registration, restricts cross-border transfers to countries that do not provide adequate data protection, and imposes special security obligations. In addition, the period of time within which organizations must respond to access and correction requests is exceedingly short and there are limited legal bases provided for the collection and use of personal information. However, there are no data breach notification or DPO obligations.

Special Characteristics

Data Protection Authority The State Register at the Ministry of Communications and Information Technologies (Azerbaijan DPA) is responsible for registering information systems and ensuring compliance with the Azerbaijani Law.

Access and Correction Organizations must respond to access and correction requests within seven days.

Cross-Border Transfers Cross-border transfers are prohibited where: (i) such transfer creates a threat to the national security of the Azerbaijan Republic, or (ii) the laws of the countries to which the personal information is transferred do not provide the same level of protection as that provided by the Azerbaijani Laws. However, personal information can be transferred across the border to a country regardless of the level of legal protection of personal information where the individual expressly agrees to the transfer. In addition, although not expressly stated in the Azerbaijani Law, crossborder transfers are permitted where the transfer is necessary to protect the life or health of the individual. Azerbaijan DPA authorization is not required; however, information on such transfer and the categories of the personal information transferred must be provided to the DPA at the time of the registration of the information system. The Azerbaijan DPA has stated informally that the cross-border transfer provisions apply to the transfer of databases (i.e. personal information of a significant number of individuals); transfers of personal information limited to one or several individuals across the border would likely trigger the rules for transfers to third parties, not the cross-border transfer rules.

Data Security Data controllers and processors must implement organizational and technical measures to guarantee the security of personal information during its collection, use and disclosure (including crossborder transfer). They must determine the risks to personal information and based on such determination must continually improve the information system in order to neutralize possible risks. There are regulations that prescribe a long list of technical organizational safety requirements. Organizations must encrypt all transmitted records. The length of the encryption key used during the transfer may not be less than 256 bits.

As is evident from the registration card for information systems approved by the Regulations on the Registration and Deregistration of Information Systems, organizations must have control and audit mechanisms for the collection and processing of personal information; however, the frequency of such audits and their substance have not been specified.

Legal Basis for Collection and Use To collect and use personal information, organizations must have a legal basis such as consent, legal requirement, or vital interests.

Registration Information systems containing personal information must be registered with the State Register unless an exemption applies. The State Registry is maintained by the Data Computing Center at the Ministry of Communication and Information Technologies.

BELARUS

The Law on Information, Informatization and Protection of Information (Belarusian Law), which became effective in 2008, regulates the processing of all personal information of natural persons by both the public and private sectors.

In Brief Under the Belarusian Law, consent is the only permissible basis on which to process (and transfer cross-border) personal information. In addition, the lawimposes special security obligations; however, there are no registration, breach notification, or DPO obligations.

Special Characteristics

Data Protection Authority There is no DPA in Belarus akin to the DPAs found in other jurisdictions. The state authority that performs any data protection-related functions is the Operative Analytics Center of the President of the Republic of Belarus (OAC). However, todate, OAC competence is more technical in nature and does not include only data protection-related competence. For example, the OAC is empowered to certify IT systems, hardware and software data protection solutions, and regulate general IT and Internet relations.

Access and Correction The Belarusian Law does not specify a time period for responding to access requests and is silent on correction rights.

Cross-Border Transfers There are no specific limitations on cross-border transfers. By general rule, each transfer, including cross-border transfers, requires the consent of the individual.

Data Protection/Security Officer A special individual or department for security measures must be appointed.

Data Security Data controllers must take effective measures to ensure security of personal information from the moment of receipt until its destruction. Under the Belarusian Law and implementing regulations, this obligation includes various organizational and technical security measures. In particular, controllers must maintain a data protection system certified by the certification centers accredited by the OAC. Organizations must file annual reports on their security measures with the OAC by December 30th of each year.

In addition, there are cryptographic regulations that define legal and organizational basics of technical and cryptographic measures of information security. Data controllers must comply with these regulations which among others things require that personal information be encrypted in transit. Regulation on Technical and Cryptographic Security of Information in the Republic of Belarus, approved by the Edict of the President of the Republic of Belarus N 196 On Certain Measures for Improving Information Security, 2013. Regulation On the Technical Security of Information and Regulation On the Technical and Cryptographic Protection of Information, both approved by the Order of Operative Analytics Center of the President of the Republic of Belarus of 30 August 2013 N 62.

Legal Basis for Collection and Use Consent is required to process personal data. The Belarusian Law does not provide for any other legal bases such as contractual necessity, vital interests or legal requirements.

BOSNIA AND HERZEGOVINA

The Law on the Protection of Personal Data (Bosnia and Herzegovina Law), which became effective in 2006, regulates the processing of all personal information of natural persons by the public and private sectors.

In Brief The Bosnia and Herzegovina Law requires database registration, restricts cross-border transfers to countries that do not provide adequate protection, and imposes special security obligations. However, there are no data breach notification or DPO obligations.

Special Characteristics

Data Protection Authority The Personal Data Protection Agency (Bosnia and Herzegovina DPA), an independent administrative organization, is responsible for enforcement of the Bosnia and Herzegovina Law.

Access and Correction Access requests must be responded to within 30 days; there is no specified time period for responding to correction requests.

Cross-Border Transfers Personal data may not be transferred to another country that does not guarantee adequate safeguards for personal information that are equivalent to those under the Bosnia and Herzegovina Law, unless the prior consent of the individual has been obtained or another exception applies, such as contractual necessity or vital interests. Exceptionally, the Bosnia and Herzegovina DPA may authorize such transfers. Neither the Bosnia and Herzegovina Law nor the Bosnia and Herzegovina DPA provide a specific list of "adequate" countries, so the data controller is responsible for assessing whether the country to which personal data are transferred guarantees protections equivalent to those provided for under the Bosnia and Herzegovina Law.

Data Security In addition to the general security obligations under the Bosnia and Herzegovina Law, regulations issued in 2009 set forth more detailed security requirements. In particular, the regulations require controllers and processors, among other things, to have a written security plan, data protection training for em-

ployees, and additional technical and organizational security measures for sensitive information such as encryption or equivalent "crypto-protection" when the data are in transit.

Legal Basis for Collection and Use To collect and use personal information, organizations must have a legal basis such as consent, contractual necessity, legitimate interests, legal requirements, or vital interests.

Registration Data controllers must register all processing of personal data with the Belarus DPA prior to the establishment of the personal data filing system or any processing, unless one of the very narrow registration exemptions applies.

GEORGIA

The Law on the Protection of Personal Data (Georgian Law), which went into effect in 2012 and was amended in 2014, regulates the processing of all personal information of natural persons by the public and private sectors.

In Brief The Georgian Law requires database registration and restricts cross-border transfers to countries that do not provide adequate data protection. However, there are no data breach notification, DPO, or special security obligations.

Special Characteristics

Data Protection Authority The Personal Data Protection Inspector (Georgia DPA), an independent authority, is responsible for enforcing the Georgian Law.

Access and Correction Organizations must respond to access requests within 10 days and correction requests within 15 days.

Cross-Border Transfers Transfers of personal information outside Georgia are permitted to countries that provide adequate data protection. The Georgia DPA issued a list of approved countries that include: the EEA countries, Australia, Albania, Andorra, Argentina, New Zealand, Bosnia and Herzegovina, Israel, Canada, Croatia, Macedonia, Moldova, Monaco, Montenegro, Serbia, Ukraine, and Uruguay. Where transfers are to jurisdictions that are not recognized as providing adequate protection, Georgia DPA-approved contracts are required.

Legal Basis for Collection and Use To collect and use personal information, organizations must have a legal basis such as consent, contractual necessity, legitimate interests, vital interests, or legal requirements.

Registration Data controllers must register with the Georgia DPA prior to creation of filing systems and inclusion of new categories of data in those filing system.

KOSOVO

The Law on the Protection of Personal Data (Kosovo Law), which went into effect 2010, regulates the processing of all personal information of natural persons by the public and private sectors.

In Brief The Kosovo Law requires database registration, restricts cross-border transfers to countries that do not provide adequate protection, and imposes special security obligations. However, there are no data breach notification or DPO obligations.

Special Characteristics

Data Protection Authority The National Agency for the Protection of Personal Data (Kosovo DPA), an independent agency, is responsible for enforcing the Kosovo Law.

Access and Correction Organizations must respond to access requests within 15 days and provide access within 30 days. They must comply with correction requests within 15 days.

Cross-Border Transfers Personal Data may only be transferred to countries outside Kosovo that ensure an adequate level of data protection, unless one of the legal bases for data transfer applies (e.g., consent, contractual necessity, or vital interests). Adequate countries include the EEA countries and the other jurisdictions recognized by the EU as providing adequate protection. The Kosovo DPA must be notified about all transfers to inadequate countries; authorization is required for such transfers.

Data Security Among other requirements, controllers and processors must have internal documentation that describes the personal information security measures that are in place. Sensitive personal information must be specifically protected and classified in order to prevent unauthorized access and use. Sensitive personal information that is transmitted over telecommunications networks will be considered suitably protected if the information is encrypted to ensure that it is rendered incomprehensible or unrecognizable.

Legal Basis for Collection and Use To collect and use personal information, organizations must have a legal basis such as consent, contractual necessity, legitimate interests, vital interests, or legal requirements.

Registration Registration is required. The data controller must keep a record of all processing of personal information, called the "Filing System Catalogue", a copy of which must be filed with the Kosovo DPA prior to establishment of the filing system.

MACEDONIA

The Law on Personal Data Protection (Macedonian Law), which went into effect in February 2005, regulates the processing of all personal information of natural persons by the public and private sectors.

In Brief The Macedonian Law requires database registration and the appointment of a DPO, restricts crossborder transfers to countries that do not provide adequate data protection, and imposes special security obligations. However, there is no data breach notification obligation.

Special Characteristics

Data Protection Authority The Directorate for Personal Data Protection (Macedonia DPA), an independent state authority, is responsible for enforcing the Macedonian Law.

Access and Correction Organizations must respond to access requests within 15 days and correction requests within 30 days.

Cross-Border Transfers Personal information may only be transferred to countries that provide adequate protection (e.g., EEA countries). For all other transfers, one of the transfer exemptions must apply (e.g., consent, contractual necessity, or vital interests) or prior Macedonia DPA authorization is required. In order to obtain approval of the Macedonia DPA, a written data transfer agreement must be in place between the controller and the recipient, preferably based on the EU Standard Contractual Clauses.

Data Protection Officer The appointment of a DPO is required except where the controller a) has a collection of personal information that only refers to ten employees or less; or b) processes personal information of members of associations founded for political, philosophical, religious or trade-union purposes.

Data Security There are special security rules that, together with the security provisions under the Macedonian Law, require, among other things, adopting and implementing written security programs, carrying out risk assessments, conducting annual internal and triannual external audits, providing employee security training, encrypting data in transit, storing data on portable devices, and retaining back-up copies.

Legal Basis for Collection and Use To collect and use personal information, organizations must have a legal basis such as consent, contractual necessity, legitimate interests, vital interests, and legal requirements.

Registration All data must be registered by controllers for all purposes, unless one of the limited exemptions applies.

MOLDOVA

The Law on Personal Data Protection (Moldovan Law), which took effect in April 2012, regulates the processing of all personal information of natural persons by the public and private sectors.

In Brief The Moldovan Law requires database registration, restricts cross-border transfers to countries that do not provide adequate protection, and imposes databreach notification and special security obligations. However, there is no DPO obligation.

Special Characteristics

Data Protection Authority The National Centre for Personal Data Protection (Moldova DPA), an independent agency, is responsible for enforcing the Moldovan Law.

Access and Correction Access and correction requests must be responded to without delay (no time period is specified).

Cross-Border Transfers Personal data may not be transferred to countries outside Moldova, unless that country ensures an adequate level of data protection. If the proposed transfer is to a country that is not considered adequate, one of the transfer exceptions must ap-

ply, such as consent, contractual necessity, or vital interests. Moldova DPA authorization is also required in such cases.

Data Security The Moldovan Law and implementing regulations prescribe detailed security requirements which include the need to maintain and annually reevaluate the organization's data security policy and implement specific physical and electronic security measures, including encryption. Regular data security audits must be carried out. These audits must include an assessment of the organization, its security measures and use of communication partners and suppliers. The results of the security audit must be documented.

Data Security Breach Notification All controllers must submit to the DPA an annual report on any security incidents involving information systems during that year.

Legal Basis for Collection and Use To collect and use personal information, organizations must have a legal basis such as consent, contractual necessity, legitimate interests, vital interests, and legal requirements.

Registration Controllers and processors must register their processing for all purposes unless one of the limited exemptions applies.

MONACO

The Protection of Personal Data Act (Monaco Law), which took effect in December 1993, regulates the processing of personal data of natural persons by the public and private sectors.

In Brief The Monaco Law requires database registration and the appointment of a DPO and restricts crossborder transfers to countries that do not provide adequate protection. However, there are no data breach notification or special security obligations.

Special Characteristics

Data Protection Authority The Personal Data Protection Supervisory Commission ("Monaco DPA") is responsible for enforcement compliance with the Monaco Law.

Access and Correction Access and correction requests must be responded to within one month.

Cross-Border Transfers Personal information may not be transferred outside Monaco unless the recipient country provides an adequate level of data protection. Parties to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Convention 108") are recognized as providing adequate data protection. Where the transfer is to a country which does not provide adequate data protection, one of the specified legal bases must apply such as consent, vital interests, or contractual necessity. In addition, the Monaco DPA may authorize transfers on the basis of appropriate contractual clauses.

Legal Basis for Collection and Use To collect and use personal information, organizations must have a legal basis such as consent, contractual necessity, legitimate interests, vital interests, or legal requirements.

ISSN 1538-3423

Registration Data controllers must register all automatic processing of personal information with the Monaco DPA unless one of the limited exceptions applies. Certain processing is also subject to Monaco DPA authorization (e.g., biometric data).

MONTENEGRO

The Personal Data Protection Law (Montenegrin Law), which took effect in 2012, regulates the processing of personal data of natural persons by the public and private sectors.

In Brief The Montenegrin Law requires database registration, restricts cross-border transfers to countries that do not provide adequate protection, and imposes DPO and special security obligations. However, there is no data breach notification obligation.

Special Characteristics

Data Protection Authority The Personal Data Protection Agency (Montenegro DPA), an independent regulatory authority, is responsible for enforcing the Montenegrin Law.

Access and Correction Organizations must respond to access and correction requests within 15 days.

Cross-Border Transfers Personal data may be transferred from Montenegro to an EEA country or a country deemed adequate by the EU, or where the transfer is based on EU Standard Contractual Clauses. Alternatively, the transfer may take place where another legal basis applies such as consent, contractual necessity, or vital interests. Otherwise, Montenegro DPA authorization is required.

Data Protection Officer Where the data controller has 10 or more employees performing data protection activities, it must designate a person who will be responsible for the data protection matters immediately after establishing a personal data filing system.

Data Security Detailed security requirements are set forth in the Regulation on the Form and Manner of Maintaining of Personal Data Filing System, covering areas such as the form, the manner of keeping data in personal data filing systems, the content of the records, the types of personal information contained in the filing system, the data retention periods, the manner of collection of personal information, and the transfer of data. For example, the Regulations require that sensitive information be kept separately, according to the type of data and that the legal basis on which the personal information is being processed is noted in the data filing system.

Legal Basis for Collection and Use To collect and use personal information, organizations must have a legal basis such as consent, contractual necessity, legitimate interests, vital interests, or legal requirements.

Registration Prior to establishing a personal data filing system, the data controller must inform the Montenegro DPA by submitting the notification containing all of the prescribed elements. Personal data filing systems required by law do not require registration.

RUSSIA

The Federal Law No. 152-FZ On Personal Data (Russian Law), which took effect in January 2007, regulates the processing of all personal information of natural persons by h the public and private sectors. The Russian Law was recently amended in 2014, imposing controversial data localization requirements.

In Brief The Russian Law requires database registration, restricts cross-border transfers to countries that do not provide adequate protection, and imposes DPO, data breach notification, special security, and data localization obligations. In addition, the period of time within which organizations must respond to correction requests is exceedingly short and there is no provision for processing personal information on the basis of legitimate interests.

Special Characteristics

Data Protection Authority The Federal Service for Supervision in the Field of Communication Information Technology and Mass Communications, commonly known as Roscomnadzor, ("Russian DPA") is responsible for enforcement of the Russian Law.

Access and Correction Organizations must respond to access requests within 30 days and correction and deletion requests within 10 days.

Cross-Border Transfers Personal Data may only be transferred to a country that provides a sufficient level of protection. The countries recognized by the Russia DPA as providing adequate protection include: all of the signatories to the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Armenia, Azerbaijan, Bosnia & Herzegovina, Georgia, Moldova, Montenegro, Macedonia, San Marino, Serbia, Turkey, Ukraine, Uruguay and the EEA Member States), Angola, Argentina, Australia, Benin, Canada, Cape Verde, Chile, Costa Rica, Gabon, Hong Kong, Israel, Kazakhstan, Malaysia, Mali, Mexico, Mongolia, Morocco, New Zealand, Peru, Qatar, Senegal, Singapore, South Africa, South Korea, Switzerland, and Tunisia.

Transfers to countries that do not provide adequate protection are permitted where there is a legal basis such as consent, contractual necessity, or vital interests. Prior Russia DPA approval or authorization is not required; however, if the organization is subject to the registration requirements, it must indicate in its registration the countries to which it transfers the information.

Data Protection Officer The appointment of an internal data protection officer is required.

Data Localization Under the amended law, organizations that collect and process personal information of Russian citizens (in electronic and paper form) must store that information in Russia. Organizations must notify the Russia DPA of their server locations. The Russia DPA will maintain a register of violators and will block any infringing websites. These localization requirements only apply to deliberate activities to collect information from Russians.

Data Breach Notification In the event of a data security breach, organizations must take measures to remedy the breach (or, if that is not possible, to destroy the affected data) within three days and then notify affected individuals about such measures. The Russia DPA must be notified (about rectification of the breach) only if it has issued a request to the organization to remedy the breach. The requirements to notify individuals about a security breach apply to any situation where an organization has processed the wrong data or there was any unauthorized processing of personal information. Such a breach may be detected by the organization itself or as a result of an access or correction request by the individual concerned.

Data Security Organizations must take all reasonable organizational and technical measures to protect personal information, which include adopting internal data protection rules that are mandatory for all employees and conducting risk assessments, audits and oversight of compliance with the Russian Law. In addition, organizations must maintain special IT systems for protecting personal data (software and hardware measures) that comply with the technical requirements of the Russian Federal Security Service (FSB) and the Federal Service for Technical and Export Control (FSTEK), and in particular with the Order of FSTEK No. 21 dated February 18, 2013.

Legal Basis for Collection and Use To collect and use personal information, organizations must have a legal basis such as consent, contractual necessity, legal requirements, or vital interests.

Registration Organizations must notify the Russia DPA of their intent to process personal information, unless an exception applies. For example, registration is not required to process employee data or where personal information was obtained through an agreement between the organization and the individual concerned, and such information is not distributed or transferred to third parties without the consent of the individual; they are used by the organization solely for the purposes of performance of the agreement or for entering into new agreements with the individual in the future;

Organizations must also register the location of databases that contain personal information of Russian citizens.

SAN MARINO

The Law Regulating the Collection of Personal Data (San Marino Law), which went into effect in 1995, regulates the processing of all personal information of natural and legal persons by the public and private sectors.

In Brief The San Marino Law requires DPA authorization to process personal information unless one of the limited legal bases applies. There is no provision for processing personal information on the basis of consent (except in the case of sensitive information) or legitimate interests. DPA authorization is always required for cross-border transfers. However, there are no DPO, data breach notification, or special security obligations.

Special Characteristics

Data Protection Authority The Garante for the Protection of Confidentiality of Personal Data (San Marino DPA) is responsible for enforcement of the San Marino Law. There is no website for the San Marino DPA.

Access and Correction The San Marino Law does not prescribe a time frame to comply with access and correction requests.

Cross-Border Transfers San Marino DPA authorization is required to transfer cross-border personal information of San Marino citizens or companies. The San Marino Law does not set out any specific requirements or conditions that must be met to obtain DPA authorizations for such cross-border transfers.

Legal Basis for Collection and Use To collect and use personal information in a private data bank, prior San Marino DPA authorization is required unless an exception applies such as contractual necessity, legal requirement or the information is publicly available. The San Marino Law does not set out consent obligations for the use of personal information except where such information concerns political, union or religious opinions and activities. In such cases, express consent is required.

Registration Prior San Marino DPA approval is required for the collection, processing and use of personal information by private owners of data banks unless an exception applies such as contractual necessity, legal requirement, the information is publicly available, or the personal information is processed by a political, social or cultural organization and relates to the members of that organization.

SERBIA

The Law on Personal Data Protection (Serbian Law), which went into effect in 2009, protects all personal data of natural persons processed by the public and private sectors.

In Brief The Serbian Law requires database registration and restricts cross-border transfers. In addition, the period of time within which organizations must respond to correction requests is exceedingly short. However, there are DPO, data breach notification, or special security obligations.

Special Characteristics

Data Protection Authority The Commissioner for Information of Public Importance and Personal Data Protection (Serbia DPA) is responsible for enforcing the Serbian Law.

Access and Correction Organizations must respond to access requests within 30 days and correction and deletion requests within 10 days.

Cross-Border Transfers Data can be transferred from Serbia to a country that is a signatory to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Data may be transferred to a state that is not a party to the Convention if such state has a regulation or a data

PVLR

transfer agreement in force which provides a level of data protection equivalent to that envisaged by the Convention. In cases of data transfers that do not provided an equivalent level of protection, Serbia DPA authorization is required.

Legal Basis for Collection and Use To collect and use personal information, organizations must have a legal basis such as consent, contractual necessity, legitimate interests, vital interests, or legal requirements.

Registration Controllers must register their processing with the DPA for all purposes. Very limited exceptions apply.

TURKEY

The Law on the Protection of Personal Data (Turkish Law), which was enacted in March 2016 and entered into full force in October 2016, regulates the processing of personal information of natural persons by individuals and private sector organizations.

In Brief The Turkish Law requires database registration, restricts cross-border transfers to countries that do not provide adequate protection, expansively defines and limits processing of sensitive information, and imposes breach notification and special security obligations. However, there is no DPO obligation.

Special Characteristics

Data Protection Authority The Turkish Data Protection Board (Turkey DPA) is responsible for enforcement of the Turkish Law. Its powers include the ability to impose administrative sanctions for law violations.

Cross-Border Transfers To transfer personal information outside of Turkey, express consent of the individual must be provided unless one of the exceptions applies (e.g., contractual necessity, vital interests, legitimate interests, or legal requirement). In addition, the transfer of personal information may only be to countries that provide adequate data protection (the Turkey DPA will provide a list). If the transfer is to a country that does not provide adequate protection, there must be a contract in place between the parties and the Turkey DPA must authorize the transfer.

Data Breach Notification Organizations must notify individuals and the Turkey "as soon as possible" if personal information is obtained by third parties "in an illegal manner."

Data Security The data controller must take every necessary technical and administrative precaution to prevent unlawful processing of and access to personal information and ensure the safeguarding of that information. In addition, the data controller must carry out the necessary internal inspections and audits to ensure compliance with the Turkish Law. If the personal information will be processed by a third party processor, the data controller will be jointly responsible for the necessary security measures.

Legal Basis for Collection and Use To collect and use personal information, organizations must have a legal basis such as explicit consent, contractual necessity, legitimate interests, vital interests, or legal requirements.

Registration The Turkish Law requires data controllers to register their processing activities before they begin processing. Exceptions may be specified by the Turkey DPA. The registration process is not yet in place; however, the Turkey DPA has issued for public comment draft regulations on the creation of a database registry. Once the public comments period ends in late June 2016, the regulations are expected to be finalized and published shortly after. The regulations should enter into force immediately upon publication.

Sensitive Information The Turkish Law defines special categories of personal information (i.e., sensitive information) as information related to a person's racial and ethnic origins, political opinions, philosophical beliefs, religion, sect or other beliefs, clothing, membership with associations, foundations or trade unions, health or sexual life, criminal convictions, and biometric and genetic data related to security measures. Processing of this information is prohibited except with the explicit consent of the individual. However, such information - with the exception of health and sexual life may be processed without explicit consent where such processing is envisaged under Turkish laws. Health and sexual information may be processed by persons or authorized institutions and organizations that are bound by confidentiality obligations, solely for the purpose of protecting public health, and providing preventive medicine, medical diagnosis, treatment and care, healthcare services and healthcare financial planning and management.

UKRAINE

The Law on the Protection of Personal Data (Ukrainian Law), which went into effect in 2011, regulates the processing of all personal data of natural persons by public and private sectors. The Ukrainian Law was amended in September 2015.

In Brief The Ukrainian Law requires database registration, restricts cross-border transfers to countries that do not provide adequate protection, and imposes DPO and special security obligations. In addition, the period of time within which organizations must respond to correction requests is exceedingly short. However, there is no breach notification obligation.

Special Characteristics

Data Protection Authority The Ukrainian Parliament Commissioner for Human Rights (Ukraine DPA) is responsible for enforcement of the Law.

Access and Correction Organizations must respond to access and correction requests within 10 days.

Cross-Border Transfers Personal data may be transferred to third countries that provide sufficient protection for personal information which include the EEA countries, signatories to the Council of Europe Convention and states on the DPA approved list (which is not yet adopted). Personal information can also be transferred to countries that do not provide adequate protection if a legal basis applies such as consent, contractual necessity, or vital interests. DPA authorization is not required; however, information regarding cross-border

transfers of the personal information must be included in the original registration/negotiation filed with DPA.

Data Protection Officer Organizations must appoint a department or a person responsible for the protection of personal information during the processing of that information.

Data Security Breach Notification There is no obligation for any entity to give notice in the event of a data security breach; however, the data controller must document or log violations in the course of data processing and develop a plan of action in case of any unauthorized access to personal information.

Data Security The Ukrainian Law and implementing regulations require organizations to, among other things, establish an internal security policy and implement specific security measures including employee

training, data disposal measures, and documentation requirements involving access and control procedures.

Legal Basis for Collection and Use To collect and use personal information, organizations must have a legal basis such as consent, contractual necessity, legitimate interests, vital interests, or legal requirements.

Registration Controllers must file a notification with the Ukraine DPA about processing of certain categories of sensitive personal information such as health, biometrical and genetic data, geolocation, trade-union political or religious memberships, race ethnic or national origin, and criminal records.

Links to all of the data privacy laws and data protection authorities discussed in this article are available Morrison & Foerster's online Privacy Library at https://www.mofo.com/privacy-library/.

PVLR