Bloomberg BNA

# WORLD DATA PROTECTION REPORT >>>

News and analysis of data protection developments around the world.
For the latest updates, visit www.bna.com

International Information for International Business

VOLUME 16, NUMBER 5 >>> MAY 2016

Reproduced with permission from World Data Protection Report, 16 WDPR 05, 05/26/2016. Copyright © 2016 by The Bureau of National Affairs, Inc. (800-372-1033) http://www.bna.com

In the first of a series on the status of data protection laws in Europe and Eurasia (non-EEA), East, Central, and South Asia and the Pacific, the Western Hemisphere and Africa and the Near East, the author explores developments in Europe and Eurasia, where 17 jurisdictions have comprehensive privacy laws.

## Privacy Laws in Europe and Eurasia (non-EEA)

*By Cynthia Rich*

### Introduction/Region at-a-Glance.

With the recent adoption of the European General Data Protection Directive (GDPR), attention of the business community has been focused on changes to the privacy rules in the 28 members states of the European Union (and 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 17 jurisdictions in Europe and Eurasia that are not part of the EU or 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 examines the commonalities and differences among the privacy laws in the region and discusses current trends and new developments.

*Cynthia Rich is a senior advisor at Morrison & Foerster LLP in Washington. As a member of the firm's international Privacy and Data Security Practice since 2001, Ms. Rich works with clients on legal issues relating to privacy around the world.*

## Common Elements Found in European/Eurasian Laws

***Notice:***

All of the laws in 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); and 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, alternation and destruction. Two-thirds of the countries have specified in greater detail how these obligations are to be met.

***Access and 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 (nine) require organizations to respond to access and/or correction requests within 15 days or fewer (two require as little as five days); more than one-third (seven) 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 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.

## Differences in Approaches.

While the core data protection principles and requirements are embodied in all of these laws, specific requirements, particularly with respect to cross-border transfers, registration, data security, data breach notification and the appointment of a data protection officer (DPO), vary widely from each other and from laws in other regions of the world.

For example, all but two of the countries in the region require registration of processing, and all but one restrict cross-border transfers; however, the reality is that there are 15 different registration and 16 different cross-border rules and procedures. Generally a contract, consent or a contract and consent are required to transfer outside the country. In some cases, the EU Standard Contractual Clauses (SCCs) may be used; in others, the data protection authorities (DPAs) have not specified what must be contained in these contracts or rules. Two-thirds of the DPAs in the region recognize the EEA countries and/or signatories to the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) as providing adequate protection. One-third have not issued lists of countries that they believe provide adequate protection, and thus companies are left to assume that all countries are deemed to be inadequate and must put in place mechanisms (such as consent or contracts) to satisfy the rules.

**There are 15 different registration and 16 different cross-border rules and procedures.**

The differences widen when comparing their respective rules on data breach notification, security and DPO obligations: one-quarter require notification in the event of a data breach; one-third require the appointment of a DPO; and two-thirds have specified in greater detail how their security obligations are to be met.

A careful read of these laws is imperative. These differences pose challenges to organizations, with respect to the adjustments that may be required to global and/or local privacy compliance practices, as well as privacy staffing requirements. Compliance programs that comply with only EEA obligations will run afoul of many of the country obligations of this region.

 COPYRIGHT © 2016 BY THE BUREAU OF NATIONAL AFFAIRS, INC., WASHINGTON, D.C.  ISSN 1473-3579

A country-by-country summary of the obligations in these key areas is provided below. Other noteworthy characteristics are also highlighted and, where applicable, the responsible enforcement authority is identified. In addition, a chart is provided at the end to show at a glance the countries with mandatory cross-border, DPO, data security breach notification and registration obligations.

## Trends.

### *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 DPA (Belarus), the DPA has yet to be established (Armenia) or the DPA was recently established (Azerbaijan and Georgia). For example, in Georgia, the DPA's enforcement powers vis-à-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, violating direct marketing rules by not providing the ability to opt out, and failing to demonstrate that consent had been obtained to disclose personal information.

---

**One of the most significant, recent developments in this region was the entry into force of Russia's data localization requirements in September 2015.**

---

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, in Albania, which has had a privacy law in place since 2008, the DPA 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 of call center companies with the Italy DPA. Fines were issued to call center companies for law violations.

In Serbia, the DPA is advocating for the adoption of a new data protection law: one that will, among others, provide the DPA with authority to issue binding decisions. Last year, the DPA reported that most of the data controllers have failed to comply with Serbia's data protection requirements, citing as an example that less than half of one percent of data controllers have filed the mandatory DPA notifications/registrations.

### *Data Localization:*

One of the most significant, recent developments in this region was the entry into force of Russia's data localization requirements in September 2015. Enacted in July 2014, the Data Localization Law amends three existing laws, including the Federal Law No. 152-FZ On Personal Data, and requires that personal information of Russian citizens be stored in Russia. All operators who are subject to DPA notification requirements under the Federal Law No. 152-FZ On Personal Data must notify the DPA of their personal data processing servers, and operators found by a court to have violated Russian laws on processing personal data will 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. Noncompliance with the data localization requirement can result in administrative penalties, civil penalties and damages and criminal sanctions. Individuals whose personal information is not processed in compliance with the law also have a private right of action for damages and compensation of moral harm.

While the current maximum fines are very low, the Russian Parliament may amend the Russian Code of Administrative Offences to increase the maximum fine to 300,000 rubles ($4,537). The Russian state magistrate courts responsible for deciding administrative fines also may issue an order to rectify noncompliance with the law. Failure to comply with the magistrate court's order may result in criminal liability for company executives.

Since the data localization requirements went into effect, the DPA has been actively auditing large multinationals to determine whether their local businesses meet the Russian data localization requirements. In 2015, the DPA audited 317 companies and found only two local businesses violating the data localization requirements. In mid-January 2016, the DPA announced a detailed plan for 1000 scheduled data localization compliance audits during the course of the year.

### *Right to Be Forgotten:*

Russia has enacted a law on the right to be forgotten and Ukraine is poised to do the same. In addition, a Turkish court has recently recognized for the first time, a very broad right to be forgotten that applies to digital and analog information carriers (e.g., books).

Russia passed its right to be forgotten law in July 2015. The law, which entered into effect on Jan. 1, 2016, requires that a search engine remove links to information that is unreliable or false, outdated or irrelevant, or posted in violation of the law. Search engines have 10 days to either remove the links or provide a reasoned explanation for refusal. Search engines that violate the law on the right to be forgotten are subject to fines of 80,000 to 100,000 rubles ($1,210-$1,512) if they refuse to remove links at an individual's request and fines of 800,000 to 1 million rubles ($12,098-15,123) if they violate a court order to remove links. However, Russian search engines have been hesitant to approve many of the right to be forgotten requests. Since the law took effect in January, 73 percent of requests have been denied by Yandex LLC—Russia's leading search engine.

**Russia has enacted a law on the right to be forgotten and Ukraine is poised to do the same. In addition, a Turkish court has recently recognized for the first time a very broad right to be forgotten.**

In April 2016, legislation was introduced into the Ukrainian Parliament that if approved would amend the country's Civil Code to allow Ukrainian citizens to demand removal and retraction of online information if it discredits "honor, dignity or business reputation of an individual." The legislation would also make the retraction available online.

Lastly, in a recently published judgment, the Turkish Court of Appeals has recognized a very broad right to be forgotten that applies not only to digital but also to analog information carriers (e.g., books). At the time of the Court of Appeals ruling, Turkey had not yet enacted data privacy legislation; however, the court used the EU data protection laws and the European Court of Justices' *Google v. Spain* decision to develop and apply the right to be forgotten. The Turkish Court of Appeals defined the right to be forgotten as a broad right to request erasure and prevention of further dissemination of information pertaining to an individual's past, when such personal information could have negative effects on the individual's future.

#### *New Data Protection Law:*

Turkey became the most recent country in this region to enact data protection legislation in March 2016. The Law on the Protection of Personal Data is intended to bring Turkey, which is seeking to gain admittance into the EU, into compliance with the EU data protection law. Some provisions of the Turkish Law took effect in April while others, such as cross-border transfers, access and correction, registration, and penalties, do not take effect until October 2016.

## Country-by-Country Review of Differences

### ALBANIA

The Protection of Personal Data Law (Albanian Law) which became effective in 2008 and 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 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 (DPA), an independent administrative authority, is 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 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, 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 controllers (with six or more persons engaged in data processing) must authorize in writing one or more persons responsible for the internal data security supervision. One of the people appointed will serve as the contact person, registered with the Commissioner. Small 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 into 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 moveable equipment. The risk assessment and treatment are part of the mandatory Information Security Policy (PSI) of the controller.

 COPYRIGHT © 2016 BY THE BUREAU OF NATIONAL AFFAIRS, INC., WASHINGTON, D.C.  ISSN 1473-3579

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 DPA of 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 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 (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 protection are the EU Member States and countries found by the European Commission or the Andorran 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 Law provides for the establishment of the Authorized State Body for the Protection of Personal Data Processing (Armenian 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, DPA authorization is required to transfer to those countries that are not on the DPA's approved list of countries that provide adequate protection. A transfer permit is required in such cases. The DPA must also approve the organization's contractual clauses governing the transfer.

#### *Data Breach Notification*

The controller must make a public announcement without delay and notify the police and the 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 law also provides for the government to set security standards in 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 or where such processing is provided for or required by law or where the data are publicly available.

#### *Registration*

The DPA has the right to require controllers to notify the DPA 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 declared 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 as public data.

#### *In Brief*

*The Azerbaijani Law requires database registration, restricts cross-border transfers to countries that do not provide adequate 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 is no data breach notification or DPO obligations.*

### Special Characteristics

#### *Data Protection Authority*

The State Register at the Ministry of Communications and Information Technologies (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 be 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 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 Law, cross border transfers are permitted where the transfer is necessary to protect the life or health of the individual. 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 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*

Controllers and processors must implement organizational and technical measures to guarantee the security of personal information during its collection, use and disclosure (including cross-border transfer). They must determine the risks for the security of the personal information and based on such risks 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 bit.

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

 COPYRIGHT © 2016 BY THE BUREAU OF NATIONAL AFFAIRS, INC., WASHINGTON, D.C.  ISSN 1473-3579

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 law imposes 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, to date, OAC's competence is more technical in nature and does not include only data protection-related competence. For example, the OAC is empowered to certify information technology (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, require the consent of the individual.

#### *Data Protection/Security Officer*

A special individual or department for security measures must be appointed.

#### *Data Security*

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 DPA. Organizations must file annual reports on their security measures to the OAC by Dec. 30.

In addition, there are cryptographic regulations that define legal and organizational basics of technical and cryptographic measures of information security. Controllers must comply with these regulations which among others things require that personal information be encrypted in transit.[1]

#### *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.[2]

### *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 (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 DPA may authorize such transfers. Neither the Bosnia and Herzegovina Law nor the DPA provide a specific list of "adequate" countries, so the controller is responsible for assessing whether the country to which personal information are transferred guarantees protections equivalent to those provided for under the Bosnia and Herzegovina Law.

---

[1] 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, available here (in Russian).

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, available here (in Russian)

[2] The 2011 amendments to the Bosnia and Herzegovina Law is available in English here.

#### *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 employees 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 requirement, or vital interests.

#### *Registration*

Controllers must register all processing of personal data with the 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 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 protection. However, there are no data breach notification, DPO, or special security obligations.*

### Special Characteristics

#### *Data Protection Authority*

The Personal Data Protection Inspector (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 protection. The 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, 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*

Controllers must register with the 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 (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 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.

 COPYRIGHT © 2016 BY THE BUREAU OF NATIONAL AFFAIRS, INC., WASHINGTON, D.C.  ISSN 1473-3579

#### *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 controller must keep a record of all processing of personal information, the "Filing System Catalogue," a copy of which must be filed with the 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 cross-border transfers to countries that do not provide adequate 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 (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 be transferred to countries that provide adequate protection, such as EEA countries. For all other transfers, one of the transfer exemptions must apply (e.g., consent, contractual necessity, or vital interests) or prior DPA authorization is required. In order to obtain approval of the Directorate, 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, the adoption and implementation of written security programs, carrying out risk assessments, conducting annual internal and triannual external audits, providing employee security training and encrypting data in transit, data stored on portable devices, and 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 data breach notification and special security obligations. However, there is no DPO obligation.*

### Special Characteristics

#### *Data Protection Authority*

The National Centre for Personal Data Protection (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 protection. If the proposed transfer is to a country that is not considered adequate, one of the transfer exceptions must apply, such as consent, contractual necessity, or vital interests. 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 reevaluate annually 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 cross-border 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 (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 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 protection. Where the transfer is to a country which does not provide adequate protection, one of the specified legal bases, such as consent, vital interests or contractual necessity must apply. In addition, the 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, and legal requirements.

#### *Registration*

Controllers must register all automatic processing of personal information with the DPA unless one of the limited exceptions applies. Certain processing is also subject to 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 (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, DPA authorization is required.

#### *Data Protection Officer*

Where the controller has 10 or more employees performing data protection activities, the controller 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.

 COPYRIGHT © 2016 BY THE BUREAU OF NATIONAL AFFAIRS, INC., WASHINGTON, D.C.  ISSN 1473-3579

#### *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*

Prior to establishing a personal data filing system, the controller must inform the DPA by submitting the notification containing all 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 January 2007, regulates the processing of all personal information of natural persons by 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, (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 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, Israel, Hong Kong, Malaysia, Mexico, Mongolia, Morocco, New Zealand, Peru, Senegal, 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 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 DPA of their server locations. The 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 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 Feb. 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 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 crossborder 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 (DPA) is responsible for enforcement of the San Marino Law. There is no website for the DPA.

#### *Access and Correction*

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

#### *Cross-Border Transfers*

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 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 concern political, union or religious opinions and activities. In such cases, express consent is required.

#### *Registration*

Prior 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 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 relate 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 (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 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, the 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, regulates the processing of personal information of natural persons by individuals and private sector organizations. Some provisions of the Turkish Law took effect in April while others, such as cross-border transfers, access and correction, registration, and penalties, do not enter into force until October 2016. With respect to personal information processed by organizations before the publication of the Turkish Law in April 2016, the organizations must make such information compliant with the Turkish Law within two years or they must delete, destroy or anony-

 COPYRIGHT © 2016 BY THE BUREAU OF NATIONAL AFFAIRS, INC., WASHINGTON, D.C.  ISSN 1473-3579

mize the data. However, the consents lawfully received before the date of publication of the Turkish Law will be deemed to be compliant with this Law if the individuals concerned have not objected to the processing within one year.

#### *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 (DPA), which will be established within six months of the Turkish Law's publication date, 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 protection (the 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 DPA must authorize the transfer. These cross-border transfer rules will take effect Oct. 7, 2016.

#### *Data Breach Notification.*

Organizations must notify individuals and the DPA "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/audits to ensure compliance with the Turkish Law. If the personal information will be processed by third party processor, the data controller will be jointly responsible for taking of 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*

Data controllers will need to register their processing activities before they begin processing. Exceptions may be specified by the DPA. The Turkish Law provides for the establishment of the DPA within six months (October 2016). The registration provisions enter into force at the same time; however, the Turkish Law states that the DPA set the date by which data controllers must be registered.

#### *Sensitive Information*

The Turkish Law defines special categories of personal information (sensitive information) as information related to a person's racial, 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, 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 recently 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 (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 on any entities to give notice in the event of a data security breach; however, the controller must document/log violations of in course of Processing and develop plan of actions in case of 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 DPA about processing of certain categories of sensitive personal information such as health, biometrical and genetic data, geolocation, trade union or political or religious memberships, race ethnic or national origin, criminal records.

## European/Eurasian Privacy Laws

| Countries with Privacy Laws | Registration Requirement | DPO Required | Cross- Border Limitations | Data Breach Notification Requirement [1] |
|---|---|---|---|---|
| Europe/Eurasia (Non-EEA) (17) | 15 | 5 | 16 | 4 |
| Albania | Yes | Yes | Yes | No |
| Andorra | Yes | No | Yes | No |
| Armenia | No | No | Yes | Yes |
| Azerbaijan | Yes | No | Yes | No |
| Belarus | No | No | No | No |
| Bosnia and Herzegovina | Yes | No | Yes | No |
| Georgia | Yes | No | Yes | No |
| Kosovo | Yes | No | Yes | No |
| Macedonia | Yes | Yes | Yes | No |
| Moldova | Yes | No | Yes | Yes |
| Monaco | Yes | No | Yes | No |
| Montenegro | Yes | Yes | Yes | No |
| Russia | Yes | Yes | Yes | Yes |
| San Marino | Yes | No | Yes | No |
| Serbia | Yes | No | Yes | No |
| Turkey | Yes | No | Yes | Yes |
| Ukraine | Yes | Yes | Yes | No |

1 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.

Source: BNA

A BNA Graphic/laws24g1


COPYRIGHT © 2016 BY THE BUREAU OF NATIONAL AFFAIRS, INC., WASHINGTON, D.C.

ISSN 1473-3579