alrud.com

DATA PROTECTION COMPLIANCE in the CIS and neighboring countries:

Top 10 Frequently Asked Questions





ALRUD

Dear Readers!

We would like to present you with our new brochure "Data protection compliance in the CIS and neighboring countries: Top 10 Frequently Asked Questions".

Over the past few years, ALRUD has gained a global reputation as a focal point of contact for international law firms and clients with interests in Russia, other members of the CIS (Commonwealth of Independent States) and neighboring countries. We have established strong business relationships with the leading national law firms and high-profile experts in Armenia, Azerbaijan, Belarus, Georgia, Kazakhstan, Kirgizstan, Moldova, Tajikistan, Turkmenistan, Ukraine, Uzbekistan. Trusted ALRUD lawyers have a deep understanding of the local business environment and regulatory framework in these countries. Thus, we are able to provide you with practical and efficient advice on all aspects of law in the CIS and neighboring countries.

During recent years, we have been accumulating our experience of advising clients on data protection issues, that companies face when doing their business in Russia. Many of our clients do their business in other CIS countries as well and usually face quite similar issues there. However, the level of regulation and, more importantly, enforcement, in different jurisdictions of the post-Soviet Union territory, varies significantly. We decided to create an easy-to-read brochure shedding the light on the most frequently asked questions, in the area of data protection.

To do so, ALRUD and leading law firms in the region – Revera (Belarus), BLC Law Office (Georgia), Aequitas Law Firm (Kazakhstan) and Vasil Kisil & Partners (Ukraine), have prepared their responses to the same questions, covering the most sensitive issues in terms of data protection regulation, so you can easily see the differences and similarities. Specifically, we have started from the notion of personal data, and applicability of local data protection laws, and continued with the specific requirements relating to data localization, direct marketing practices, use of cookies, data disclosures to the third parties and other issues.

We hope that this brochure will be a helpful guide in your day-to-day business. Please do not hesitate to reach out to us, if you have any feedback, or any further questions triggered by this material, and we will be delighted to contact you.

With thanks to the following firms partnering with ALRUD Law Firm:

REVERA BLC Law Office AEQUITAS LAW FIRM VASIL KISIL

ALRUD

REVERA

Belarus

REVERA

What information is defined as personal data?

The information laws define personal data as: an individual's main and additional personal data to be included in the Population Register, as per the Belarusian laws, as well as other data allowing the individual's identification.

Main personal data includes: identification number, full name, sex, date of birth, place of birth, digital photo, citizenship, residence information, information on death or declaration as a dead, declaration of absence, incapacity, limited capacity. Additional personal data is defined as: data on parents, guardians, custodians, family status, spouse, children, higher education, academic degree, academic rank, occupation, tax liabilities, disability and pension.

Although the law lays down an exhaustive list of main and additional personal data, there is no legal, nor practical, guidance on attribution of information to the other data allowing identifying an individual.

In June 2019, the Belarussian Parliament, in the first reading, adopted a novel draft law on personal data protection. The draft law defines personal data as: any information relating to an identified individual, or individual that can be identified, on the basis of such information. If adopted, the new law will extend the scope of information that may be qualified as personal data – it will cover the information relating to directly, and indirectly, identifiable individuals.

Do data protection laws in Belarus apply to foreign companies?

Belarusian information laws apply solely to Belarusian companies and branches/representatives offices of non-Belarusian companies registered there. Unlike in Russia, there is no practice demonstrating that Belarusian laws are construed as applicable to foreign companies without a presence in Belarus, even if their online services target a Belarusian audience.

Are there any local data storage/localization requirements in Belarus?

Entities established/located in the Republic of Belarus and offering services, or goods, in the Belarusian market, via the Internet, shall use information networks, systems and resources of the national segment, located in the territory of the Republic of Belarus and registered in accordance with the local laws.

How is the use of cookies and other tracking technologies regulated from the data protection perspective?

There are no special regulations, nor guidelines, on using cookies in the Republic of Belarus. However, in practice, companies usually request an individual's consent to use cookies and implement the relevant provisions in their privacy notices.

Are there any local privacy policy requirements in Belarus? How can global policies (*e.g.,* GDPR-based) be implemented locally?

There are no specific requirements for a local privacy policy in Belarus. However, the draft law on personal data protection obliges each data controller to develop local policy on data processing and to ensure that employees, directly involved in the processing, are familiar with the policy, as well as to provide unlimited access to the policy (including via the Internet). Practically speaking, it is possible to implement global policies in Belarusian companies. However, they shall be reviewed as per the local requirements and translated to Russian in advance.

Are there any requirements for data disclosures/transfers to the third parties?

As per the information laws, both internal and cross-border transfers of personal data, are allowed only after obtaining an individual's written consent.

The draft law on personal data protection sets out special grounds for cross-border data transfer. These include the individual's consent, entering into and performance of the agreement, transferring publicly-available data, permission of the responsible governmental authority, etc.

Are there any specific requirements relating to personal data processing performed for direct marketing purposes?

The advertising laws lay down the requirements for the advertising communications, via the telephone, or with the use of electronic means of communication. In particular, such communications are allowed only on the basis of the subscriber's consent, and an advertiser shall terminate advertising communications upon the subscriber's respective request.

Are there any other data protection/privacy requirements companies in Belarus to comply with?

Under information laws, companies shall take the following measures for the protection of personal data:

- **Legal measures:** enter into the agreements with users, setting out the terms of the data usage, as well as liability for violating them;
- **Organizational measures:** ensure special rules of access into the territory (premises) where access to data (mediums) can be obtained, as well as restriction of access to the data, according to the nature of the data being processed;
- **Technical measures:** use means of technical and cryptographic protection of information, as well as implement measures aimed at carrying out control over the information security.

The draft law on personal data protection sets out additional measures such as: appointment of an officer responsible for data protection issues (data protection officer), conducting of employees' training programmes, determining the procedure of access to personal data, notifying the authorities of data breaches, etc.

REVERA

What data protection/privacy rights do individuals enjoy in Belarus?

The current legislation contains only general guarantees for the protection of the individuals' rights, such as providing consent to data processing, securing access to personal data, the right to personal data protection.

According to the draft law on personal data protection: individuals will also have the right to receive information about their rights in connection with the processing of personal data, to withdraw consent, to have access to their personal data, to demand termination of the collection and further processing of data, to demand deletion of their data, etc.

What are the sanctions for non-compliance with data protection laws?

Belarusian law sets out administrative and criminal liability for violation of personal data processing requirements.

Namely, unauthorized disclosure of personal data, by a person having access to such data, in connection with a professional activity, may entail an administrative fine of up to 4 to 20 base units (approximately 45 to 225 USD) In addition, an administrative fine of up to 200 base units (approximately 2 250 USD) can be imposed for the failure to use certified data security tools.

As for the criminal liability, the respective sanctions may be imposed for the unlawful (i.e., performed without individual's consent) collection, or dissemination, of information about private life, which entails harm to the rights, freedoms and legitimate interests of an individual. In addition, unauthorized access to computer information is also penalized under the Belarusian law – this may be relevant if such computer information contains personal data.

On a separate note, the draft law on personal data protection explicitly mentions individuals' private right of action, namely that they may claim compensation for reputational damage, suffered due to violation of their privacy rights.

BLC
Law Office

Georgia

What information is defined as personal data?

Georgian legislation defines personal data as any information relating to an identified, or identifiable, individual. Identifiable individual means that: he, or she, can be identified directly, or indirectly, in particular with the use of an identification number, or any physical, physiological, psychological, economic, cultural, or social, features specific to that individual. There is no test set out by law, nor by practice, to conclusively decide what can be considered personal data. In certain cases, technical information, such as IP Address, may be also considered personal data.

Georgian law also provides for the special categories of personal data such as: data relating to an individual's racial or ethnic origin, political views, religious or philosophical beliefs, membership in professional organizations, state of health, sexual life, criminal history, administrative detention, putting a person under restraint, plea bargains, abatement, recognition as a victim of crime or as a person affected, also biometric and genetic data that allow to identify a natural person by the above features. Data protection standards vary according to the type of data being processed – special categories of personal data enjoy greater protection.

Do data protection laws in Georgia apply to foreign companies?

Georgian data protection laws apply to the processing of personal data within the territory of Georgia, as well as, to diplomatic representations and consular offices of Georgia abroad. Likewise, they are applicable to data processors, who are not registered in the territory of Georgia, but employ technical means located in Georgia for data processing, except when such technical means are used solely for data transfer.

Are there any local data storage/localization requirements in Georgia?

Georgian laws do not set out any straightforward localization/local data-storage requirements. However, there are cross-border data transfer requirements (see Q.6 below) to ensure safe transfer of the data, outside Georgia.

How is the use of cookies and other tracking technologies regulated from the data protection perspective?

Georgian laws do not lay down any specific rules with regard to the use of cookies and tracking technologies – where their use implies processing of information relating to individuals, general data protection requirements apply. For instance, data processing is allowed, when it is necessary for a data controller to perform its statutory duties, or protect its legitimate interests, or is otherwise required to render the services to the data subject.

Are there any local privacy policy requirements in Georgia? How can global policies (*e.g.,* GDPR-based) be implemented locally?

Every data controller is obliged to ensure the security of personal data and accountability of its data processing activities. This shall be done by of keeping a catalogue for each data processing system and further register such catalogues with the data protection authority ("**DPA**"). The catalogues shall contain recordings of personal data processing activities performed, including legal grounds for data processing, retention terms, general description of data security procedures, etc. Any data subject has the right to: request rectification, update, blocking, erasure or destruction of incomplete, inaccurate, out-of-date or illegally-obtained data. European data protection laws are more rigorous than Georgian ones, so global policies are normally implemented locally, which does not entail violation of local data protection laws. Data protection policy needs to be adopted by the respective management body of the company. It needs to be generally authorized under the company charter to do so. It is also important to ensure that the employees are familiar with, and consent in writing to, the adopted policy.

Are there any requirements to data disclosures/transfers to the third parties?

Personal data may not be transferred, nor otherwise disclosed, to any third parties in the absence of the individual's consent, or other appropriate legal grounds. There are legal requirements additional to appropriate legal grounds and applicable in case of cross-border data transfers. In particular, prior to transferring personal data outside Georgia, the data controller shall satisfy itself that a recipient state, or international organization, provide appropriate data protection guarantees – the list of such states and international organization is defined by the DPA. Where data is transferred to any countries, other than included into this list, the data controller shall enter into a data processing agreement with the recipient party and request the DPA's authorization to transfer the data.

Are there any specific requirements relating to personal data processing performed for direct marketing purposes?

According to Georgian laws, an individual's name (names), address, telephone number, e-mail address, and fax number may be processed for direct marketing purposes, irrespective of the purpose, for which such data was initially collected. Furthermore, any data may be processed for direct marketing purposes on the basis of an individual's written consent. In the meantime, individuals are entitled to opt-out from personal data processing for direct marketing purposes at any time - the company shall take the required steps within ten (10) business days.

Are there any other data protection/privacy requirements companies in Georgia to comply with?

Other than general data protection requirements, and the obligation to notify the data processing before set up of a filing system and entry of a new category of data therein, there are no additional requirements imposed on companies in Georgia. However, this may change in the future: in May 2019, a new package of legislative amendments on the protection of personal data was introduced to the Georgian Parliament. The new bill introduces much stricter requirements on data processing, including an obligation for companies working in certain fields (public agencies, banks, insurance companies, etc.) to appoint a data protection officer.

What data protection/privacy rights do individuals enjoy in Georgia?

According to Georgian laws, individuals may request the information about the type of personal data being processed, purpose of and legal grounds for data processing, the ways in which the data were collected, third parties to whom his/her personal data were disclosed, legal grounds and purpose of such disclosure. Individuals are also entitled to: request a correction, update, addition, blocking, deletion, destruction of data, and to withdraw a consent. The law sets out a general procedure for exercising the data protection rights, as well as imposing certain exceptions in this regard (e.g., national defense and public security). In case individuals are not satisfied with the controller's data processing practices, they may lodge their respective compliant with the DPA, or a court.

What are the sanctions for non-compliance with data protection laws?

Failure to comply with Georgian data protection laws may entail a warning and administrative fines of up to GEL 10,000 (approx. USD 3,200), which vary according to the type of violation. Such sanctions are imposed by the DPA. Moreover, unlawful use of personal data resulting in considerable damage to individuals concerned may entail criminal sanctions for the company's executives. The DPA is authorized to mandate suspension of unlawful data processing, or resort to other remedies reasonable in the circumstances, to ensure the compliance with the data processing regulations.

AEQUITAS
LAW FIRM

Kazakhstan

What information is defined as personal data?

Personal data means: information relating to the data subject identified, or to be identified, on the basis of such information, recorded on an electronic, paper and/or any other tangible medium. Personal data includes: full name, address of residence, information on citizenship, date of birth, information on education, marital status, biometric data, individual identification number, etc. The source, or the subject, of personal data may be an individual only.

The law defines two types of personal data – public and restricted data. Public personal data is the data considered as such, by virtue of the Kazakh legislation (such as the name of an individual entrepreneur, name, place and date of birth, within the state statistical accounting, etc.) or by virtue of the individual's consent to use such data in a publicly-available manner.

The personal data protection laws do not contain an exhaustive list of restricted personal data, but provide for an obligation of a person collecting personal data, for its needs, to elaborate and approve the "List of Personal Data Required and Sufficient for Achievement of the Objectives Pursued by an Owner and/or Operator".

Do data protection laws in Kazakhstan apply to foreign companies?

The requirement to localize personal data applies only to persons carrying out their activities in Kazakhstan. The data protection laws apply to foreign companies doing business in Kazakhstan through their dependent agents (for example, distributors), even without the establishment of a local legal entity, representative office, or a branch.

Are there any local data storage/localization requirements in Kazakhstan?

The Law establishes a direct obligation of the personal data database owner, or operator, to store personal data in a database located in Kazakhstan. The owner of a database containing personal data is a person who collects data, uses the database in its business activities and has the right to dispose of such database itself, at its own discretion. The database operators are persons who use databases in their activities, with the owner's consent, or render data storage, or processing services to the owner. Kazakhstan citizens' personal data shall be stored mainly in Kazakhstan. It may be transferred to other states, only subject to compliance with requirements on personal data database localization and necessity, to ensure appropriate personal data protection.

How is the use of cookies and other tracking technologies regulated from the data protection perspective?

Processing of personal data, with the use of tracking technologies, is governed by the general rules of the Kazakh laws: there are no specific regulations in this regard. Cookies relate to electronic information resources containing restricted personal data, so local information laws govern their protection. Owners and possessors of information systems must take measures to protect cookies, from the moment of access to cookies containing personal data, until their destruction or anonymization.

AEQUITAS
LAW FIRM

Are there any local privacy policy requirements in Kazakhstan? How can global policies (*e.g.,* GDPR-based) be implemented locally?

Owners and/or operators and third parties that have access to restricted personal data must ensure its confidentiality, by preventing distribution of such personal data, without consent of the data subject (or its legal representative), or any other legal ground. In this sense, implementation of the local privacy policy serves as a basic measure for the protection of personal data.

The Kazakh legislation does not provide for a legal mechanism of implementing global policies in the area of personal data, such as the GDPR; however, Kazakhstan pursues the general principles of ensuring personal data protection. From the practical perspective, it is possible to implement global policy locally, provided that it is reviewed, as per the Kazakhstan legal requirements, and translated into Russian, or Kazakh language.

Are there any requirements relating to data disclosures/transfers to the third parties?

Transfer, or disclosure, of personal data to a third party, is only allowed with the consent of an individual or his/her legal representative.

The Kazakh laws provide for a number of cases where personal data may be transferred without the individual's consent (in the course of activities of law-enforcement authorities and courts, enforcement proceedings, or state statistical activities, etc.).

Are there any specific requirements relating to personal data processing performed for direct marketing purposes?

Personal data processing for direct marketing purposes is not directly regulated by the Kazakhstan legislation; however, based on the general rules, it is only allowed in case of complying with requirements relating to protection of rights and liberties of man and citizen, when collecting and processing personal data (there must be an individual's consent, the purpose limitation principle shall be met, etc.).

Are there any other data protection/privacy requirements companies in Kazakhstan to comply with?

In order to regulate the scope of "personal data" being processed each legal entity must draft, and approve, the list of personal data required and sufficient for attaining the pursued objectives.

What data protection/privacy rights do individuals enjoy in Kazakhstan?

The individuals enjoy the rights to:

- know that an owner and/or operator, or a third party, has his/her personal data and receive information on the fact, purpose, sources and methods of collecting and processing personal data, obtain a list of personal data, term of personal data processing, including the term of storage;
- request that an owner and/or operator changes, or supplements, the data subject's personal data, if there is a basis to do so, verified by relevant documents;
- request an owner and/or operator, or a third party, to block and to destroy the data subject's personal data that was collected and processed, in violation of the Kazakh legislation;
- withdraw a consent to personal data collection and processing;
- give a consent to an owner and/or operator to distribution of the data subject's personal data in public sources, or refuse to do so;
- seek for the protection of own rights and legitimate interests, including to claim compensation of reputational and material damages suffered; etc.

What are the sanctions for non-compliance with data protection laws?

The Kazakh laws do not set out specific sanctions for the failure to comply with the localization requirement. However, it may constitute a general offence associated with unlawful processing of personal data and failure to comply with the security requirement. This entails administrative fines up to 1,000 Monthly Calculation Indices ("**MCI**") and, in some cases, seizure of the tools used for unlawful data processing. MCI is an index used in Kazakhstan for calculation of various social payments as well as penal sanctions, etc. Now its unit is valued at KZT 2,778 (approx. USD 7), so the maximum administrative fine now is about USD 7,000.

There is also a criminal liability for data protection offences (e.g., where failure to comply with the requirements entails substantial damages). Applicable penalties include criminal fines, imprisonment, limitation of liberty, corrective labor or community service, and disqualification.

Ukraine

VASIL KISIL

What information is defined as personal data?

Personal data is defined as: information, or set of information, about an identified data subject, or a data subject who can be certainly identified. The data subject's full name, individual tax number and address of residence, taken in conjunction, or separately, are usually defined as personal data. The phone number is not considered as personal data, unless it is taken in conjunction with other data that allows to one to define the data subject with utmost certainty. There is no relevant guidance, nor court practice, on the technical data (IP address, cookies, etc.) so far.

Some types of personal data are more sensitive than others: racial and ethnic origin, political and religious beliefs, membership in trade unions, political parties, and religious organizations, health, sexual life, biometric and genetic data, criminal or administrative convictions, location and route tracking. Sensitive data is accorded with higher standards of protection. This data may be processed subject to the data subject's explicit consent, or on limited grounds provided by law. The data controller must notify the data protection authority ("**DPA**") each time sensitive data is collected, amended or erased.

Do data protection laws in Ukraine apply to foreign companies?

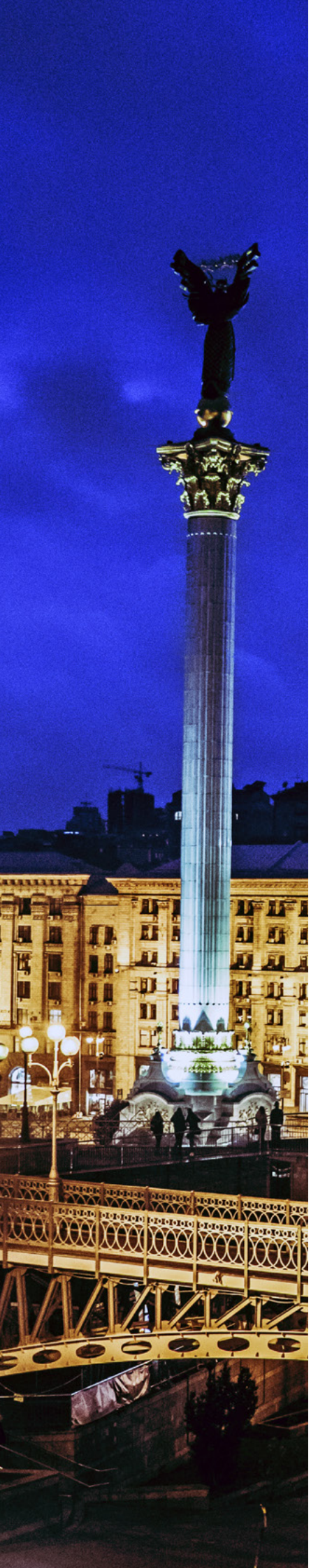
In Ukraine, personal data processing is governed by the Law of Ukraine "On Personal Data Protection" dated 1st June 2010, No. 2297-VI, as well as the regulations and guidance issued by the DPA. The law is silent on the territorial scope of its application. There is no test, nor applicability criteria, that would define whether the processing of personal data is regulated by the laws of Ukraine, at the moment of data collection. However, in any case, data protection laws apply on a territorial basis, i.e., to Ukrainian legal entities and local branches/representative offices.

Are there any local data storage/localization requirements in Ukraine?

There are no data localization requirements in Ukraine applicable to the companies doing business in Ukraine. However, there is a requirement, which is de facto construed as a local data storage requirement. Namely, state authorities and local self-government bodies acting as data controllers (data owners) may assign personal data processing only to state- or municipally-owned Ukrainian enterprises.

How is the use of cookies and other tracking technologies regulated from the data protection perspective?

There is no relevant guidance, nor enforcement practice, on the use of cookies. Use of tracking technologies, enabling a controller to locate an individual, may be considered as processing of sensitive data, since its processing may entail significant risks to the individual's rights and freedoms. The data controller, processing such sensitive data, must implement a privacy policy, appoint a data protection officer, and inform the DPA of every case of such processing.



VASIL KISIL

Are there any local privacy policy requirements in Ukraine? How can global policies (*e.g.,* GDPR-based) be implemented locally?

There is no general obligation to implement a personal data processing policy – formally speaking, a requirement, to ensure lawful and secure processing of personal data, may be fulfilled in the absence of the data protection policy. However, data controllers processing sensitive personal data must implement a personal data processing policy, on the basis of the standard one adopted by the DPA. Foreign companies having Ukrainian subsidiaries normally incorporate provisions of their global policies into the standard policy and thereby implement such policies in Ukraine. The scope of such policy normally covers the processing activities of the Ukrainian office (employee data, emails, archive storage, etc.), while data processing activities on the company web-site hosted abroad remain governed by the global privacy policy.

Are there any requirements relating to data disclosures/transfers to the third parties?

The data controller may assign processing of personal data to the data processor. In this case, they must enter into a data processing agreement, which may be either a separate document, or a part of another contract. There are no requirements to the form and content of such agreement. In practice, companies use the standard contractual clauses for controller-to-processor transfers, as approved by the EU Commission. The controller-to-controller assignments are not recognised by the Ukrainian law, though if such transfers occur, the respective standard contractual clauses are also used. There are no special, nor simplified, rules for intra-group data transfers.

Are there any specific requirements relating to personal data processing performed for direct marketing purposes?

The Ukrainian law does not lay down any specific requirements governing privacy of electronic communications (e-privacy), so the direct marketing (including digital marketing) and processing of personal data for the related purposes are mostly regulated by general data protection requirements. As regards applicable grounds, each individual's consent and the data controller's legitimate interests (subject to balance of interests) are the applicable ones. In the absence of e-privacy regulation there are no requirements of opt-in, nor opt-out (unsubscribing), for direct marketing: therefore, there is no common practice and companies in Ukraine follow different approaches.

Are there any other data protection/privacy requirements companies in Ukraine to comply with?

There are two significant data protection requirements companies in Ukraine shall comply with. Firstly, the data controllers shall inform the DPA of the appointed data protection officer (including full name, job position, telephone number, and e-mail address). Secondly, the data controllers who processes sensitive personal data must inform the DPA in writing/electronically of every processing event with sensitive personal data. The second obligation is quite extensive and it is rarely complied with.

What data protection/privacy rights do individuals enjoy in Ukraine?

Individuals are entitled to request: information about processing of their personal data and access to their personal data, to object to processing of personal data, to request correction or erasure of personal data, to protection of personal data from any unlawful processing and disclosure, to withdraw a consent, or claim reservation regarding personal data processing. based on such consent, to know the mechanism of automatic processing. If individuals are not satisfied with the controller's data processing practices, they can lodge their complaints with the data protection authority, National Police, and court.

What are the sanctions for non-compliance with data protection laws?

The Ukrainian law sets out administrative and criminal liability for the companies' officials who fail to comply with data protection laws. The administrative liability includes administrative fines of up to UAH 34,000 (approx. USD1,250), which are imposed by the DPA as result of the state data protection audits. The criminal fines of up to UAH 17,000 (approx. USD 625), or imprisonment of up to 5 years may be imposed only by a court, which implies prior investigation of a case by the National Police. At the same time, there have been no criminal convictions for violations of data protection laws, so far. There are no specific liability rules or enforcement practice against foreign companies.

ALRUD

Russia

What information is defined as personal data?

Personal data is defined as: any information relating to directly, or indirectly, identified, or identifiable, individual (data subject). In practice, the notion of personal data is construed broadly so that, together with information traditionally attributed to personal data (such as name, contact details, etc.), it may also include certain technical (e.g., information processed with use of cookies) and other data.

Additionally, Russian laws distinguish special categories of personal data (i.e., relating to race, national origin, political views, religious and philosophical commitments, intimate life, health and criminal convictions) and biometric personal data (i.e., relating to an individual's physiological and biological characteristics, enabling and used for the individual's identification). Processing of such data is subject to specific legal rules, in terms of applicable legal grounds and security.

Do data protection laws in Russia apply to foreign companies?

Basically, Russian data protection laws apply on a territorial basis - i.e., to Russian legal entities and branches/representative offices of non-Russian legal entities. However, they may apply to companies without such Russian presence, but processing personal data on websites/apps targeting a Russian audience. Although the targeting test is not formalized under Russian laws, it is widely applied by local authorities and courts, as a matter of practice. It implies examination of such diverse signs as domain zone registration, existence of the Russian version of a website/app, possibility to arrange products' delivery to Russia, etc. – the list is not exhaustive, so any signs are analyzed on a case-by-case basis.

Are there any local data storage/localization requirements in Russia?

Since September 1st 2015, data controllers have had to ensure that certain operations on Russian citizens' personal data are performed in a Russian database, once such data is collected. There is a number of legal exceptions, which are quite narrow and, therefore, applied very rarely. In the meantime, in practice, the localization requirement may be construed in a way enabling companies not to localize the data under certain circumstances, for example, where company acts purely as a data processor – in practice, the possibility to apply such exceptions shall be defined on a case-by-case basis.

How is the use of cookies and other tracking technologies regulated from the data protection perspective?

Russian laws do not set out any specific rules on use of cookies and similar tracking technologies – in such cases, general rules apply. Their use shall be transparently described in a dedicated section of a Privacy Policy, or a specific Cookie Notice. As for legal grounds, it is necessary to request an individual's opt-in consent for such use. However, it is feasible to rely on alternative legal grounds (e.g., contractual necessity, legitimate interest) to use cookies strictly necessary for a website functioning.

Are there any local privacy policy requirements in Russia? How can global policies (*e.g.,* GDPR-based) be implemented locally?

Each data controller shall create and maintain a document explaining its personal data processing policy. Such document shall cover all aspects of data processing, including scope of personal data being processed, processing purposes, retention terms, etc. It shall be drawn up in Russian and compliant with the legal requirements and recommendations of the data protection authority ("**DPA**") regarding content. The policy shall be made available to the individuals concerned – in particular, it shall be communicated to employees against their wet signatures and posted on a website/app when it comes to data processing on such website/app.

It is possible to implement global privacy policy in Russia; however, such a policy shall be reviewed from the Russian data protection perspective – necessary updates may be reflected directly in the document, or attached as the Russian addendum to the global policy. In addition, it is possible to implement Russian and global policy in parallel, giving the priority to the Russian policy.

Are there any requirements to data disclosures/transfers to the third parties?

Data disclosures shall be described in the controller's respective policy and there must be appropriate legal grounds to do so. When it comes to cross-border data disclosures, legal grounds vary according to the adequacy of data protection legislation and practice of a recipient country.

In addition, data disclosures shall be formalized by way of entering into a data processing agreement. Formally speaking, the law lays down the material terms for such agreements concluded in case of a controller-to-processor assignment. However, in practice, similar terms are included in controller-to-controller agreements. There are no simplified, nor specific, rules regarding intra-group data disclosures.

Are there any specific requirements relating to personal data processing performed for direct marketing purposes?

Processing of personal data for direct marketing purpose requires each individual's prior opt-in consent. Each marketing communication shall contain a link allowing an individual to withdraw this consent (unsubscribe), or information as to how it can be done. Once an individual unsubscribes, the data controller must immediately terminate direct marketing communications and related data processing – the laws do not provide any grace period in such a case.

Are there any other data protection/privacy requirements companies in Russia shall comply with?

There are some additional obligations laid down by Russian data protection laws. In particular, they include implementation of security measures, appointment of a data protection officer, and registration with the DPA. Unlike in the EU, in Russia there is no general obligation to notify DPA, nor a data subject of a data breach. However, it is likely that such obligation will be introduced to the Russian laws due to the recent modernization of the Convention 108+.

What data protection/privacy rights do individuals enjoy in Russia?

Individuals are entitled to: withdraw their consent, to access personal data, to request that their incomplete, inaccurate, outdated or misleading data is modified, and that the data controller terminates data processing and destroys the data which is excessive, or processed unlawfully. For the moment, Russian laws do not set out a data portability right. Where individuals are not satisfied with a data controller's privacy practices, they can lodge respective complaints with the DPA, or a court.

What are the sanctions for non-compliance with data protection laws?

Privacy-related violations may entail administrative fines, which vary according to the type of violation. Separate fines are imposed for violations of different types and, in some cases, multiple fines may be imposed per breach (e.g., per data subject, where necessary consents are absent). In general, amounts of fines are up to 75,000 Roubles (approx. USD 1,000). However, higher fines may be imposed for direct marketing reasons – up to 500,000 Roubles (approx. USD 6,800), and for the data localization violation – up to 6,000,000 Roubles (approx. USD 81,400) for the first offence, and up to 18,000,000 Roubles (approx. USD 244,200) for a repeated one. Moreover, unlawful data processing practices may entail forced termination of respective data processing activities and blockage of a website/app, where they relate to personal data processing on such website/app.

Key contacts

Maria Ostashenko

ALRUD Partner, Commercial, Intellectual Property, Data Protection and Cybersecurity, the CIS and neighboring countries

Ranked in Chambers Europe, Chambers Global, Legal 500, WTR1000, Who's Who Legal.

E: mostashenko@alrud.com

ALRUD

ALRUD Law Firm
17 Skakovaya street,
building 2, 6th floor
125040 Moscow, Russia
T: +7 495 234 96 92
E: info@alrud.com