

DATA PROTECTION LAWS OF THE WORLD

Ukraine



Downloaded: 28 April 2024

UKRAINE



Last modified 22 January 2024

LAW

The Law of Ukraine No. 2297 VI 'On Personal Data Protection' as of June 1, 2010 (Data Protection Law) is the main legislative act regulating personal data protection in Ukraine. On December 20, 2012, the Data Protection Law was substantially amended by the Law of Ukraine, 'On introducing amendments to the Law of Ukraine’ ’On Personal Data Protection' dated November 20, 2012, No. 5491-VI. Additional significant changes to Data Protection Law were introduced by the Law of Ukraine 'On Amendments to Certain Laws of Ukraine regarding Improvement of Personal Data Protection System' dated July 3, 2013, No. 383-VII which came into force on January 1, 2014.

In addition to the Data Protection Law, certain data protection issues are regulated by subordinate legislation specifically developed to implement the Data Protection Law, in particular:

- Procedure of notification of the Ukrainian Parliament's Commissioner for Human Rights on the processing of personal data, which is of particular risk to the rights and freedoms of personal data subjects, on the structural unit or responsible person that organizes the work related to protection of personal data during processing thereof (Notification Procedure)
- Model Procedure of processing of personal data (Model Procedure)
- Procedure of control by the Ukrainian Parliament's Commissioner for Human Rights over the adherence of personal data protection legislation

The Data Protection Law essentially complies with EU Data Protection Directive 95/46/EC.

The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, executed in Strasbourg on January 28, 1981 and the Additional Protocol to the Convention regarding supervisory authorities and trans-border data flows, executed in Strasbourg on November 8, 2001 were ratified by the Ukrainian Parliament on July 6, 2010 (Convention on Automatic Processing of Personal Data) and have become fully effective in Ukraine.

In addition, data protection is regulated by:

- The Constitution of Ukraine dated June 28, 1996
- The Civil Code of Ukraine dated January 16, 2003, No 435 IV
- Law of Ukraine 'On Information' No 2657 XII, dated October 2, 1992
- Law of Ukraine 'On Protection of Information in the Information and Telecommunication Systems' dated July 5, 1994 No. 80/94 VR
- Law of Ukraine ‘On Electronic Commerce’ dated September 3, 2015, No 675-VIII
- Some other legislative acts

Furthermore, on October 25, 2022 the new Draft Law “On Personal Data Protection” No. 8153 has been submitted to Ukrainian Parliament. The said draft law is aimed at harmonizing Ukrainian data protection legislation with the standards enshrined by the GDPR and Convention 108+ and is currently expecting to be considered by Ukrainian Parliament.

DEFINITIONS

Definition of personal data

Data Protection Law defines "personal data" as data or an aggregation of data on an individual who is identified or can be precisely identified.

Definition of sensitive personal data

There is no definition of "sensitive personal data";

However, there is general prohibition to process personal data with regard to racial or ethnic origin, political, religious ideological convictions, participation in political parties and trade unions, accusation in criminal offenses or conviction to criminal punishment, as well as data relating to the health or sex life of an individual.

Processing of such data is allowed if unambiguous consent has been given by the personal data subject or based on exemptions envisaged by Data Protection Law (eg. the processing is performed for the reasons of protection of vital interest of individuals, healthcare purposes, in course of criminal proceedings, anti-terrorism purposes, etc.).

NATIONAL DATA PROTECTION AUTHORITY

Starting from January 1, 2014, Ukrainian Parliament's Commissioner for Human Rights (Ombudsman) is the state authority in charge of controlling the compliance of the data protection legislation.

REGISTRATION

As of January 1, 2014, the requirement of obligatory registration of personal data databases has been abolished. However, according to new wording of Data Protection Law, personal data owners are obliged to notify the Ombudsman about personal data processing which is of particular risk to the rights and freedoms of personal data subjects within 30 working days from commencement of such processing. Pursuant to the Notification Procedure, the following types of personal data processing requires obligatory notification to the Ombudsman:

- Racial, ethnic, national origin
- Political, religious ideological beliefs
- Participation in political parties and/or organizations, trade unions, religious organizations or civic organization of ideological direction
- State of health
- Sexual life
- Biometric data
- Genetic data
- Criminal or administrative liability
- Application of measures as part of pre-trial investigation
- Any investigative procedures relating to an individual
- Acts of certain types of violence used against an individual
- Location and / or route of an individual

The Notification Procedure envisages that the application for notification shall contain, inter alia the following information:

- Information about the owner of personal data
- Information about the processor(s) of personal data
- Information on the composition of personal data being processed
- The purpose of personal data processing
- Category(ies) of individuals whose personal data are being processed
- Information on third parties to whom the personal data are transferred
- Information on cross-border transfers of personal data

- Information on the place (address) of processing of personal data
- General description of technical and organizational measures taken by personal data owner in order to maintain the security of personal data

Where any of information listed above is submitted to the Ombudsman and has changed, the owner of the personal data shall notify the Ombudsman on such changes within 10 days from the occurrence of such change.

Additionally, the Notification Procedure requires the owners of personal data to notify the Ombudsman regarding the termination of personal data processing which is of particular risk to the rights and freedoms of personal data subjects, within ten days of such termination.

The Notification Procedure requires owners and processors of personal data that process personal data, which is of particular risk to the rights and freedoms of personal data subjects, to notify the Ombudsman on establishing a structural unit or appointing a person (data protection officer) responsible for the organization of work related to the protection of personal data during the processing. Such notification shall be made within 30 days of establishing a structural unit or appointing a responsible person.

Information regarding the said notifications of the Ombudsman shall be published on the official website of the Ombudsman.

DATA PROTECTION OFFICERS

Data owners and processors processing personal data that is of particular risk to the rights and freedoms of personal data subjects, must establish a special department or appoint a responsible person (data protection officer) to be responsible for the personal data processing matters. Other owners and processors may either establish a department or appoint a responsible person on a voluntary basis.

There are no requirements for the data protection officer to be a citizen or a resident in Ukraine. However, if he or she is a foreign citizen under the general rule, a work permit must be obtained for him or her to hold such a position. There are no particular penalties for the incorrect appointment of Data Protection Officer.

COLLECTION & PROCESSING

The Data Protection Law requires obtaining the consent of data subjects for the processing of their personal data. According to the Data Protection Law, the consent of the data subject means the voluntary and intentional expression of will of the data subject to the processing of personal data for the identified purposes, expressed in writing or in some other form. In the area of e-commerce, consent may be granted in the process of registration of data subjects by "ticking" a consent box during registration, provided that such a system does not allow processing of personal data before the consent is obtained. Under certain circumstances, personal data may be processed without a data subject's consent (eg, legislative permission for processing of personal data, necessary to the conclusion and execution of a transaction or contract in favor of the data subject, protection of interests of data subject or data owner).

Pursuant to the Data Protection Law, as a general rule, personal data subjects shall be informed, at the moment of collection of their personal data of:

- The owner of their personal data
- The composition and content of their personal data being collected
- Their rights
- The purpose of their personal data collection, and
- The persons to whom their personal data will be transferred

However, in cases when the personal data of individuals have been collected based on the following grounds, the personal data subjects shall be informed of the above within 30 working days from the:

- Legislative permission of the owner of the personal data on the processing of personal data exclusively for the purposes of fulfilling its authorities

- Conclusion and execution of a transaction where the data subject is a party or the transaction has been concluded in favor of the data subject, which preceded conclusion of a transaction at the request of the subject of personal data
- Protection of vital interests of the data subject, or
- Need to protect the legitimate interests of the owner of personal data and third parties, except where a data subject requests that the processing of his/her personal data stops and the need to protect personal data prevails over such interest

In addition, the Data Protection Law provides the data subject with the following rights:

- To be aware of the sources of collection, location of his / her personal data, the purpose of data processing, the address of the owner or processor of the personal data or to obtain the said information through his / her representatives
- To obtain information in regards to the conditions of providing access to personal data, and in particular, information on third parties, to which his / her personal data are transferred
- To access his / her personal data
- To obtain a reply within 30 calendar days from the date of the receipt of his / her request, informing the individual whether his / her personal data is being processed and to receive the contents of such personal data
- To provide the owner of personal data with the reasonable request to terminate the processing of his / her personal data
- To provide a reasonable request to change or destroy his / her personal data by any owner and processor of the personal data if the data is processed illegally or is inaccurate
- To protect of his / her personal data from unauthorized processing and accidental loss, elimination or damage with respect to intended encapsulation, not providing or the untimely provision of personal data, and to protect from providing invalid or discrediting information regarding the individual
- To appeal violations in the course of personal data processing to the Ombudsman or to the court
- To introduce limitations as regards rights on its personal data processing while giving the consent
- To use the means of legal protection in the case of violation of rights to personal data
- To revoke its consent on personal data processing
- To be aware of the mechanism of automatic personal data processing, and
- To be protected from the automated decision that has legal effects

The owner of the personal data can entrust the processing of personal data to the processor pursuant to a written agreement requiring that the processor process the personal data only for the purposes and in the amount permitted under the agreement. The transfer of personal data to the processor is permitted only with consent of the data subject.

TRANSFER

In accordance with Data Protection Law, personal data may be transferred to foreign parties when there is an appropriate level of protection of personal data in the respective state of the transferee. Pursuant to the Data Protection Law, such states include member states of the European Economic Area and signatories to the EC Convention on Automatic Processing of Personal Data. The list of the states ensuring an appropriate level of protection of personal data will be determined by the Cabinet of Ministers of Ukraine.

Personal data may be transferred abroad based on one of the following grounds:

- Unambiguous consent of the personal data subject
- Cross-border transfer is needed to enter into or perform a contract between the personal data owner and a third party in favor of the data subject
- Necessity to protect the vital interests of the data subject
- Necessity to protect public interest, establishing, fulfilling and enforcing of a legal requirement
- Non-interference in personal and family life of the data subject, as guaranteed by the data owner

SECURITY

The data owners and processors must take appropriate technical and organizational measures to ensure the protection of personal data against unlawful processing, including against loss, unlawful or accidental elimination, and also against unauthorized

access. In this regard, owners and processors processing personal data which is of particular risk to the rights and freedoms of personal data subjects shall determine a special department or a responsible person to organize the work related to the protection of personal data during the processing thereof (other owners and processors may either establish a department or appoint a responsible person on a voluntary basis).

The Model Procedure stipulates that the owners and processors of personal data shall take measures to maintain the security of personal data in all stages of their processing, including organizational and technical measures for the protection of personal data. Organizational measures shall include:

- Determination of a procedure of access to personal data by employees of the owner / processor of personal data
- Determination of the order of the recording of operations related to the processing of personal data and access to them
- Elaboration of an action plan in case of unauthorized access to personal data, damage of technical equipment or occurrence of emergency situations, and
- Regular trainings of employees working with personal data

Personal data, irrespective of the manner of its storage, shall be processed in the way which makes unauthorized access to the data by third persons impossible.

With the purpose of maintenance of security of personal data, technical security measures shall be taken which would exclude the possibility of unauthorized access to personal data being processed and ensure the proper work of technical and program complex through which the processing of personal data is performed.

Additionally, the Data Protection Law requires establishing a structural unit or appointing a responsible person within the personal data owners / processors processing the personal data which is of particular risk to the rights and freedoms of personal data subjects. Such structural unit or responsible person shall organize the work related to protection of personal data during the processing thereof.

BREACH NOTIFICATION

There is no requirement to report data security breaches or losses to the appropriate state authority.

ENFORCEMENT

According to Data Protection Law, the Ombudsman and Ukrainian courts are responsible for overseeing the compliance of personal data protection legislation. Failure to comply with the provisions of Data Protection Law can lead to the penalties prescribed by the law.

Violation of personal data protection legislation may result in civil, criminal and administrative liability.

If the violation has led to material or moral damages, the violator may be required by the court to reimburse such damages.

The Code of Ukraine on Administrative Offenses envisages administrative liability for the following breaches of Ukrainian data protection legislation:

- Failure to notify or delay in providing notification to the Ombudsman regarding the processing of personal data or of a change to the information submitted, subject to notification requirements under Ukrainian legislation, or submission of incomplete or false information, which may lead to a fine of up to EUR 164;
- Non-fulfilment of legitimate requests (orders) from the Ombudsman or determined state officials of the Ombudsman's secretariat, regarding the elimination or prevention of violations of personal data protection legislation, which may lead to a fine of up to EUR 411;
- Non-observance of the established procedure for the protection of personal data which leads to the unauthorized access of the personal data or violation of rights of the data subject, which may lead to a fine of up to EUR 411.

The criminal liability, prescribed by the Criminal Code of Ukraine, envisages fines of up to EUR 411 or correctional works for a term of up to two years, up to six months arrest, or up to three years of limitation of freedom for the illegal collection, storing, use, elimination, or spreading of confidential information about an individual, or an illegal change of such information.

ELECTRONIC MARKETING

The Law of Ukraine "On Electronic Commerce" dated September 3, 2015 provides for certain legal requirements for distribution of commercial electronic messages in the area of electronic commerce (i.e. electronic messages in any form, the purpose of which is to promote, directly or indirectly, goods, works, services, business reputation of a party engaged in a business or self-employed professional activity). In particular, commercial electronic messages shall be distributed only subject to the consent given by individual to whom such messages are addressed. At the same time, commercial electronic messages may be distributed to an individual without his / her consent only if such individual has an option to object to receiving such messages in future.

In addition, commercial electronic messages shall satisfy the following criteria:

- Commercial electronic messages shall unequivocally be identified as such.
- The recipient shall have easy access to information regarding the person sending the message as stipulated by the Law of Ukraine "On Electronic Commerce"; in particular:
 - full name of legal entity / individual and place of registration / residence;
 - email / website of the online shop;
 - registration number or tax ID number / passport details (for individuals);
 - license data (in case if it is mandatory under the law);
 - inclusion of taxes in calculation of the price of goods / services; and
 - price of delivery of goods (in case if delivery is performed).
- Commercial electronic messages regarding sales, promotional gifts, premiums and etc. shall be unequivocally identified as such and the conditions of receiving of such promotions shall be clearly stated to avoid their ambiguous understanding as well as shall comply with advertising legislation.

In addition, under the Law of Ukraine "On Electronic Communications" dated December 16, 2020, end-users may use telephone numbers or other network subscriber identifiers obtained by any person in the course of selling goods or providing services to send advertisements for the purpose of selling goods or services only with the consent of the end-user, including in electronic form, and if the recipient is given the opportunity to refuse the use of his or her data at any time, free of charge, in a simple and understandable manner.

Furthermore, distribution of spam is generally prohibited. Spam is defined quite broadly as more than five messages (electronic, text and / or multimedia messages) sent to one recipient without the recipient's prior consent.

ONLINE PRIVACY

There is no specific legislation regulating online privacy in Ukraine. However, the Data Protection Law applies to the extent online activities involve the processing of personal data.

KEY CONTACTS



Natalia Kirichenko
Partner
Kinstellar Ukraine LLC
T +380 (44) 490 9575

natalia.kirichenko@kinstellar.com

DATA PRIVACY TOOL

You may also be interested in our [Data Privacy Scorebox](#) to assess your organization's level of data protection maturity.

Disclaimer

DLA Piper is a global law firm operating through various separate and distinct legal entities. Further details of these entities can be found at www.dlapiper.com.

This publication is intended as a general overview and discussion of the subjects dealt with, and does not create a lawyer-client relationship. It is not intended to be, and should not be used as, a substitute for taking legal advice in any specific situation. DLA Piper will accept no responsibility for any actions taken or not taken on the basis of this publication.

This may qualify as 'Lawyer Advertising' requiring notice in some jurisdictions. Prior results do not guarantee a similar outcome.

Copyright © 2022 DLA Piper. All rights reserved.