INTERNATIONAL LAWYERS NETWORK

2024 ILN DATA PRIVACY GUIDE

An International Guide

www.iln.com

ILN Cybersecurity & Data Privacy Group and ILN Technology Media & Telecommunications Group

Disclaimer

This guide offers an overview of legal aspects of data protection in the requisite jurisdictions. It is meant as an introduction to these marketplaces and does not offer specific legal advice. This information is not intended to create, and receipt of it does not constitute, an attorney-client relationship, or its equivalent in the requisite jurisdiction.

Neither the International Lawyers Network or its employees, nor any of the contributing law firms or their partners or employees accepts any liability for anything contained in this guide or to any reader who relies on its content. Before concrete actions or decisions are taken, the reader should seek specific legal advice. The contributing member firms of the International Lawyers Network can advise in relation to questions regarding this guide in their respective jurisdictions and look forward to assisting. Please do not, however, share any confidential information with a member firm without first contacting that firm.

This guide describes the law in force in the requisite jurisdictions at the dates of preparation. This may have been some time ago and the reader should bear in mind that statutes, regulations, and rules are subject to change. No duty to update information is assumed by the ILN, its member firms, or the authors of this guide.

The information in this guide may be considered legal advertising.

About the ILN

The ILN is a non-exclusive network of high-quality mid-sized law firms, which operates to create a global platform for the provision of legal services, particularly for clients with international needs. With a presence in 67 countries, it is exceptionally well placed to offer seamless legal services, often of a cross-border nature from like-minded and quality legal practices. In 2021, the ILN was honored as Global Law Firm Network of the Year by The Lawyer European Awards, and in 2016, 2017, 2022, and 2023 they were shortlisted as Global Law Firm Network of the Year. Since 2011, the Network has been listed as a Chambers & Partners Leading Law Firm Network, increasing this ranking in 2021 to be included in the top two percent of law firm networks globally. Today, the ILN remains at the very forefront of legal networks in its reach, capability, and depth of expertise.

Authors of this guide:

1. Cybersecurity & Data Privacy Group

Co-chaired by Jim Giszczak of McDonald Hopkins and Stuart Gerson of Epstein Becker & Green, the Cybersecurity & Data Privacy Specialty Group provides an international platform for enhanced communication, enabling all of its members to easily service the needs of their clients requiring advice.

2. Technology, Media & Telecom (TMT)

Co-chaired by Alishan Naqvee of LexCounsel in New Delhi and Gaurav Bhalla of Ahlawat & Associates in New Delhi the TMT Group provides a platform for communication on current legal issues, best practices, and trends in technology, media & telecom.

www.iln.com

Ukraine

PETERKA & PARTNERS is a full-service law firm operating in Central and Eastern Europe, providing one-stop access as an integrated regional service. The firm provides legal services to multinational companies active in the region, as well as leading local groups, providing them with complex legal solutions with exceptional commercial value.

Introduction

Below is a brief outline of the legal regulation of personal data protection in Ukraine.

Governing Data Protection Legislation

2.1. Overview of principal legislation

The main legal act governing data protection in Ukraine is the Law of Ukraine on Personal Data Protection No. 2297-VI dated 1 June 2010 as amended (the "PDP Law").

2.2. Additional or ancillary regulation, directives or norms

Apart from the PDP Law, the main additional regulations for data protection are established by the legal acts adopted by the Ukrainian Parliament Commissioner for Human Rights (the "Commissioner"), such as the Model Procedure on Processing of Personal Data; the Procedure on Notification of the Commissioner on the Processing of Personal Data that Constitutes a Special Risk for the Rights and Freedoms of Personal Data Subjects, On the Structural Unit or Responsible Person that Organises the Work related to Protection of Personal Data during its Processing and the Publication of Such Information (the "Procedure on Special Risk Data"); others.

2.3. Upcoming or proposed legislation

Since Ukraine is on track to join the European Union, it has to ensure the protection of personal data in accordance with the highest European and international standards. In that respect, Ukraine is constantly working on draft laws aimed at harmonising current legislation on data protection, particularly with the standards provided for by the General Data Protection Regulation (Regulation (EU) 2016/679). Currently, no draft law in this respect has yet been adopted.

Scope of Application

3.1. Legislative Scope

3.1.1. Definition of personal data

The PDP Law defines "personal data"

Contact Us

+380 44 581 11 20

https://www.peterkapartners.com/en/local/kyiv/

utiralov@peterkapartners.ua

45/85 Saksahanskoho St.
Kyiv, 01033 Ukraine

as information or a set of information on a natural person who is, or may be, explicitly identified.

3.1.2. Definition of different categories of personal data

The PDP Law contains special requirements for processing certain personal data that constitutes a special risk to the rights and freedoms of data subjects ("Special Risk Data").

Under the PDP Law, the Special Risk Data includes personal data on racial or ethnic origin, political, religious or philosophical beliefs, membership in political parties and trade unions, criminal convictions, health, sex life, biometric, and genetic data.

The Procedure on Special Risk Data expands the list of Special Risk Data provided by the PDP Law and includes personal data about national origin, membership in political organisations, religious organisations or public organisations with an ideological orientation, being brought to administrative or criminal liability, application of measures to a person within the framework of a pre-trial investigation, the taking of measures against a person provided for by the Law of Ukraine on Operative Investigation Activity, committing certain types of violence against a person, location and/or routes of movement of the person.

3.1.3. Treatment of data and its different categories

Personal data processing is defined under the PDP Law as any operation or set of operations, such as collection, recording, accumulation, storage, adaptation, alteration, renewal, use and distribution (dissemination, realisation, transmission), depersonalisation, destruction of personal data, including with the use of information (automated) systems.

Personal data must be accurate, reliable and updated as necessary for the purpose of its processing. The composition and content of personal data must be appropriate, adequate and not excessive in relation to the purpose of its processing.

The processing of personal data is carried out for specific and lawful purposes, determined by the consent of the personal data subject or in cases provided for by the laws of Ukraine, in the manner established by the legislation. It is not allowed to process the personal data of a natural person without his/her consent if such data is confidential information, except for those cases determined by law, and only in the interests of national security, economic welfare, and human rights.

The procedures for processing, timeline of processing and composition of personal data must be proportional to the purpose of processing. The purpose of personal data processing must be explicit, legitimate and determined before collection begins. If a specific purpose for personal data processing is changed to a new purpose that is incompatible with

the previous one, for further data processing, the data controller, except in cases specified by law, must obtain the consent of the data subject to process the data in accordance with the new purpose.

As to the Special Risk Data, its processing is allowed only if unambiguous consent has been given by the data subject or based on exemptions envisaged by the PDP Law (e.g., for employment and healthcare purposes, protection of the vital interest of the data subject, law enforcement intelligence or counterintelligence activity, anti-terrorism). Under the general rule, the data controller must notify the Commissioner of processing Special Risk Data within 30 business days from the start of such processing. There is also an obligation to notify the Commissioner in cases of the alteration of Special Risk Data or termination of its processing.

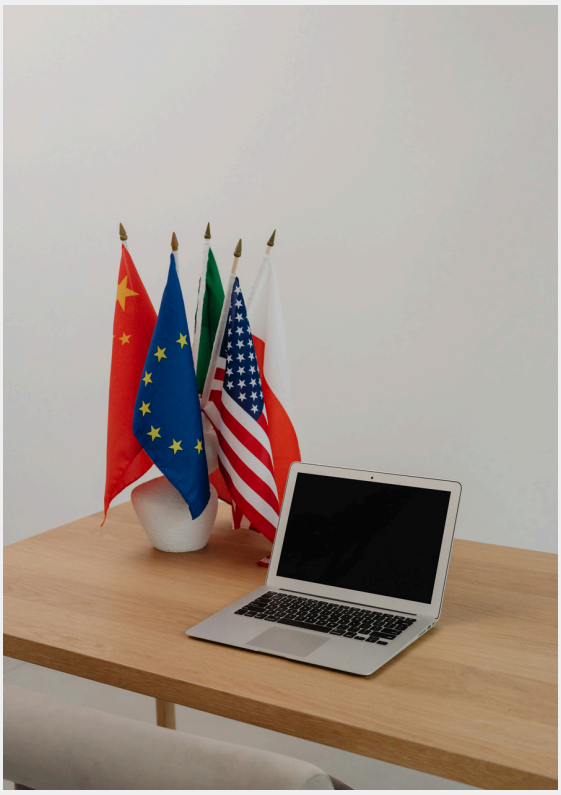
3.2. Statutory exemptions

The processing of personal data is allowed without adherence to the provisions of the PDP Law if such processing is made: (a) by a natural person purely for personal or household needs; (b) exclusively for journalistic and creative purposes, given a balance is ensured between the right to respect the private life and the right of freedom of expression. The PDP Law also does not cover relations on the receipt of archival information from repressive bodies.

In specific cases, i.e., in cases provided by law to the extent required in a democratic society in the interests of national security, economic welfare or protection of the rights and freedoms of data subjects or other persons, certain provisions of the PDP Law may be limited.

3.3. Territorial and extra-territorial application

The PDP Law does not specify the territory of its application. However, according to the general principles of Ukrainian law and practice, it may be interpreted to apply to all personal data processed in the territory of Ukraine.



Legislative Framework

4.1. Key stakeholders

- "Data Controller" is a natural person or legal entity who determines the purpose of personal data processing, the composition of this data and the procedures for its processing unless otherwise specified by law.

- "Data Processor" is a natural person or legal entity who is granted with the right by the data controller or by law to process this data on behalf of the data controller.

- "Data Subject" is a natural person whose personal data is processed.

4.2. Role and responsibilities of key stakeholders

The data controller and processor solely determine the procedure for processing personal data, taking into account the specifics of the processing of personal data in various areas.

In particular, the data controller determines the:

- purpose and grounds for processing personal data;
- categories of data subjects;
- composition of personal data;
- procedure for processing personal data, namely the:
  - method of collection and accumulation of personal data;
  - timeline and conditions for storage of personal data;
  - conditions and procedure for alteration, deletion or destruction of personal data;
  - conditions and procedure for the transfer of personal data and a list of third parties to whom personal data may be transferred;
  - procedure for access to the personal data of the persons carrying out the processing, as well as to the data subjects;
  - measures to ensure personal data protection;
  - procedure for storage of information on operations related to the processing of personal data and access to them;
  - obligations and rights of persons responsible for organising work related to personal data protection during its processing.

The data controller may entrust the personal data processing to the data processor under a written agreement. The data processor may process personal data only for the purposes and to the extent specified in such agreement.

Requirements for Data Processing

5.1. Grounds for collection and processing

-Consent
The consent of the data subject is the voluntary expression of the will of

https://www.peterkapartners.com/en/local/kyiv/

a natural person (subject to his/her awareness) to grant permission to process his/her personal data in accordance with the stated purpose of its processing, expressed in written form or in a form that makes it possible to conclude that consent has been granted.

The consent may be prepared as a separate document to be signed by the data subject, or a corresponding indication in electronic form, a term and condition of the agreement, or it may be prepared in any other form that allows the conclusion that consent has been provided (writing an application, filling in a questionnaire, etc.).

In the field of electronic commerce, the data subject's consent may be provided when registering in the information and communication system of the electronic commerce subject by ticking the granting of permission to process his/her personal data in accordance with the stated purpose of its processing, provided that such a system does not create opportunities for personal data processing until the tick is made.

As a general rule, at the time of collection of personal data, the data subject shall be informed about the data controller, composition and content of collected personal data, the data subject's rights defined by the PDP Law, the purpose of collecting personal data, and the persons to whom the relevant personal data may be transferred.

-Consent Notice

The consent notice should be in a simple and understandable form and contain the full scope of information that must be provided by the data controller to the data subject before receipt of the consent

-Withdrawal of Consent

The data subject has the right to withdraw consent to processing personal data without specifying motives if the only basis for processing is his/her consent. From the moment of withdrawal of consent, the data controller is obliged to stop personal data processing.

-Other grounds prescribed by law

Apart from the consent, the PDP Law establishes a list of other grounds allowing the processing of personal data without the consent of the data subject (such as the conclusion and performance of a transaction to which the data subject is a party or which is concluded in favour of the data subject or for the implementation of measures preceding the conclusion of the transaction at the request of the data subject, etc.).

5.2. Data storage and retention timelines

The personal data is processed no longer than necessary for the legitimate purposes for which it was collected or further processed; in any case, no longer than provided for by the legislation in the field of archival affairs and record keeping. Further processing of personal data for

historical, statistical or scientific purposes may be carried out subject to ensuring its proper protection.

5.3. Data correction, completion, updation or erasure of data

The personal data shall be changed based on a substantiated written request of the data subject or in other cases prescribed by law (e.g., upon a court decision that has entered into force). If information about a person is found to be untrue, such information must be immediately changed or destroyed. Personal data shall be updated if necessary, determined by the purpose of its processing.

Personal data shall be deleted or destroyed in the case of:

- expiration of the data storage period determined by the consent of the data subject or by law;
- termination of the legal relationship between the data subject and controller or processor, unless otherwise provided for by law;
- issuance of an appropriate order of the Commissioner or officials of its secretariat;
- entry into force of a court decision on personal data deletion or destruction;
- personal data collected in violation of the requirements of the PDP Law.

5.4. Data protection and security practices and procedures

The data controllers, processors and

https://www.peterkapartners.com/en/local/kyiv/

third parties are obliged to ensure personal data protection from accidental loss or destruction, and from illegal processing, including illegal destruction or access to personal data. The data controllers and processors take measures to maintain the security of personal data in all stages of their processing, including organisational and technical measures. They independently determine the list and composition of security measures, taking into account the requirements of the legislation and informational security.

The organisational measures include:

- establishment of a data access procedure for employees of data controllers/processors;
- establishment of the procedure for recording operations related to personal data processing and access to them;
- elaboration of an action plan in case of unauthorised access to personal data, damage to technical equipment, or emergencies;
- regular training of employees working with personal data.

Technical security measures are taken, in particular, to exclude unauthorised access to personal data and ensure the proper working of the technical and program means through which the personal data is processed.

Data controllers and processors processing Special Risk Data are obliged to (1) create/define a structural unit or responsible person for organising the work related to personal data protection during its processing and (2) notify the Commissioner about such unit/person.

5.5. Disclosure, sharing and transfer of data

Sharing of personal data is allowed according to the data subject's consent or in cases specified by law and only (if required) in the interests of national security, economic welfare, human rights and for conducting the all-Ukrainian population census.

The data controller shall notify the data subject of the personal data transfer to a third party within ten working days if required by the conditions of his/her consent or otherwise not provided for by law. The specified notifications are not made in the case of:

- transfer of personal data upon requests made within the performance of the tasks of law enforcement intelligence or counterintelligence, anti-terrorism activities;
- exercise by state and local authorities of their powers provided for by law;
- personal data processing for historical, statistical or scientific purposes;

https://www.peterkapartners.com/en/local/kyiv/

- notification of the data subject on such transfer while collecting personal data in accordance with the PDP Law.

5.6. Cross-border transfer of data

The transfer of personal data to foreign subjects is carried out only if the relevant state ensures adequate personal data protection. The following states are recognised as doing so: (i) European Economic Area (EEA) member states; (ii) states-signatories to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28.01.1981; and (iii) other states defined as such by the Cabinet of the Ministers of Ukraine.

Additionally, cross-border transfer of personal data is allowed if the:

- data subject grants unambiguous consent to the transfer;
- need exists to conclude or perform an agreement between the data controller and the data subject for the benefit of the data subject;
- need exists to protect the vital interests of the data subject;
- need exists to protect public interest, establish, implement and ensure the legal claim;
- data controller has provided relevant guarantees of non-interference in the personal and family life of the data subject.

Personal data may not be shared with a purpose other than the one for which it was collected.

https://www.peterkapartners.com/en/local/kyiv/

5.7. Grievance redressal

Data subjects can submit complaints regarding their personal data processing to the Commissioner or a court.

Rights and Duties of Data Providers/Principals

6.1. Rights and remedies

-Right to withdraw consent

Please see the related information in para 5.1. above.

-Right to grievance redressal and appeal

Please see the related information in para 5.7. above.

-Right to access information

In particular, the data subject has the right to (i) access to his/her personal data; (ii) no later than 30 calendar days from the date of receipt of the request, except in cases provided for by law, and receive a response on whether his/her personal data is being processed, as well as receive the content of such personal data; (iii) know about the sources of collection, location of his/her personal data, the purpose of their processing, location or place of residence of the data controller and processor, or authorise persons to receive such information, except in cases established by law; (iv) receive information on the conditions for

granting access to personal data, in particular, information on third parties to whom his/her personal data is transferred; (v) know the mechanism for automatic personal data processing.

-Right to nominate

The PDP Law does not explicitly provide for the right to nominate.

6.2. Duties

The PDP Law does not set out specific duties for data subjects, except for implicit general ones such as an obligation to comply with personal data protection legislation.

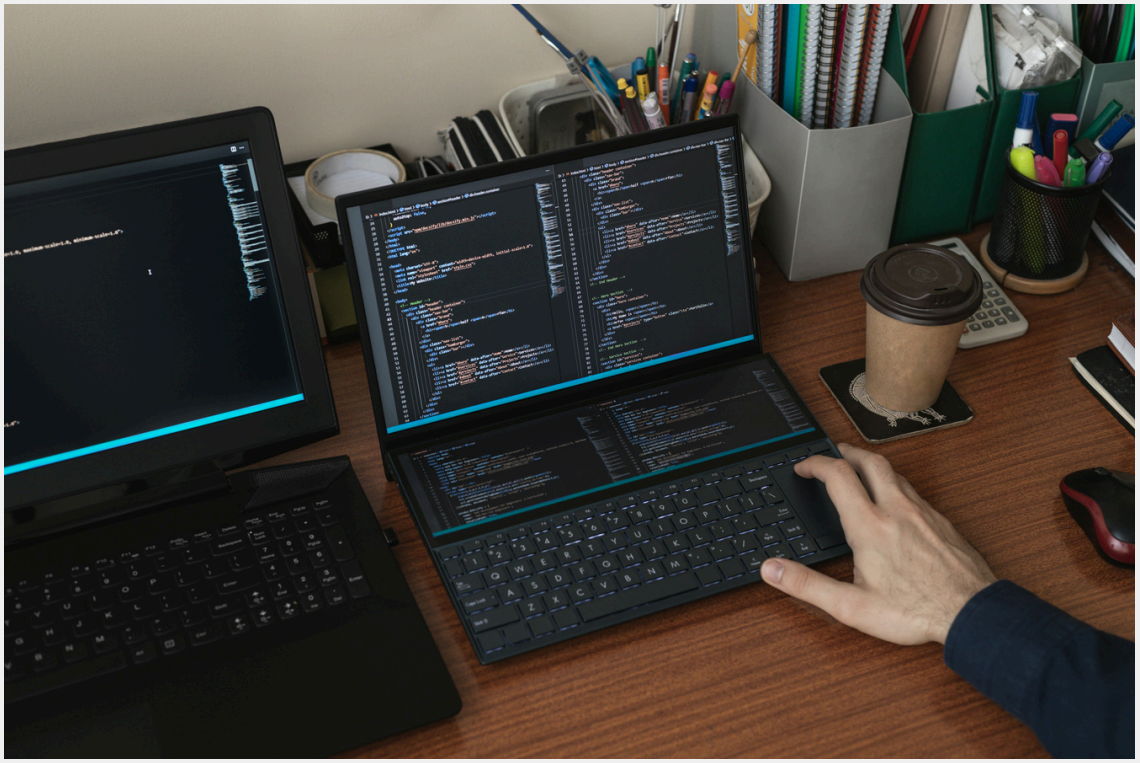
Processing of Children or Minors' data

The PDP Law does not regulate the processing of the data of children or minors. Under general civil law, parents or guardians may act on their behalf, including providing the consent required for personal data processing.

Regulatory Authorities

8.1. Overview of relevant statutory authorities

According to the PDP Law, the Commissioner and courts are



https://www.peterkapartners.com/en/local/kyiv/

8.1. Overview of relevant statutory authorities

According to the PDP Law, the Commissioner and courts are responsible for checking for compliance with personal data protection legislation.

8.2. Role, functions and powers of authorities

The key powers of the Commissioner are the following:

- to receive and decide on proposals, complaints and other requests from natural persons and legal entities related to personal data protection;
- to conduct inspections of data controllers or processors;
- to issue binding demands (instructions) on the prevention or elimination of violations of personal data protection legislation, to draw up protocols on bringing one to administrative liability and sending them to the court in cases provided for by the law;
- to approve regulations in the field of personal data protection;
- to provide recommendations on the practical application of personal data protection legislation, to clarify the rights and obligations of the relevant persons, to provide, at the respective request, opinions on draft codes of conduct in the field of personal data protection;
- to propose amendments to legislation on personal data protection, to monitor new practices, tendencies and technologies regarding personal data protection, etc.

8.3. Role, functions and powers of civil/criminal courts in the field of data regulation

In respect of being brought to liability, civil courts consider and decide on protocols for bringing one to administrative liability, submitted by the Commissioner or officials of its Secretariat. Criminal courts consider and decide on cases related to being brought to criminal liability for committed criminal offences.

Apart from the above, the courts also protect the rights of relevant participants in data protection relations. In particular, the data subjects may file lawsuits to the courts related to a breach of personal data protection legislation and recover compensation for damage, including moral damage, caused by such a breach.

Consequences of non-compliance

The following violations can be subject to administrative liability in the sphere of personal data protection:

- ·for failure to notify or late notification of the Commissioner on the processing of Special Risk

https://www.peterkapartners.com/en/local/kyiv/

- Data, or amendments to such data, and the provision of incomplete or unreliable information, a fine of up to approximately EUR 170 is envisaged

- for failure to execute demands (instructions) of the Commissioner or officials of its

- Secretariat on the prevention or elimination of violations of personal data legislation, a fine of up to approximately EUR 420 is envisaged

- for non-compliance with personal data legislation resulting in unauthorised access to personal data or violation of the rights of a data subject, a fine of up to approximately EUR 420 is envisaged

- For repeated (within a year) of the above violations, a fine of up to approximately EUR 840 may be imposed.

Certain violations may also involve criminal liability. In particular, for the illegal collection, storage, use, destruction, or distribution of confidential information on a natural person or an illegal alteration of such information a fine of up to approximately EUR 420 is envisaged or correctional works of up to two years, arrest of up to six months, or restraint of liberty of up to three years. For the same actions committed repeatedly, or in cases where they have caused substantial harm to the person's rights, freedoms, and interests, arrest of up to six months, restraint of liberty of up to five years, or imprisonment for the same term is envisaged.

Conclusion

Currently, it may not be concluded that Ukrainian legislation fully ensures personal data protection in compliance with the best international standards and practices in this area. However, Ukraine is constantly working on the harmonisation of its legislation with European and other international standards.

***

The above information is provided for general understanding and informational purposes only.

In general, this information is provided according to the standard legislation of Ukraine and does not focus on specific regulations that may, from time to time, be introduced into the legislation of Ukraine due to the martial law introduced in Ukraine since February 24, 2022 in response to the military aggression of the Russian Federation against Ukraine.

On no account can the provided information be considered as either a legal opinion or advice on how to proceed in particular cases or on how to assess them.

The protection of personal data may also involve other legal aspects. We strongly advise that legal advisors be involved in order to ensure that each specific case is dealt with comprehensively. Should you need any further information on the issues covered by this overview, please contact Mr. Taras Utiralov (utiralov@peterkapartners.ua) or Ms. Halyna Melnyk (melnyk@peterkapartners.ua).

Contact Us

+380 44 581 11 20

https://www.peterkapartners.com/en/local/kyiv/

utiralov@peterkapartners.ua

45/85 Saksahanskoho St.
Kyiv, 01033 Ukraine