DataGuidance
GLOBAL GUIDANCE IN ONE

GUIDANCE NOTES


## About The Author

**Olga Belyakova** is a Senior Lawyer at CMS Cameron McKenna. Her practice includes telecommunications media and technology (TMT), as well as competition and general commercial issues. Olga regularly advises national and foreign telecommunications and IT companies, media houses and other international and local companies on issues relating to the Ukrainian telecommunications, IT, media and technology law areas. She has over seven years' experience on various aspects of doing business in the TMT sector. Olga represented international mobile operators on regulatory telecommunications matters related to obtaining Ukrainian telecommunications licenses (both business and radio-frequency licenses). She also advised multi-national telecommunications and media companies on issues related to digital terrestrial TV.

E-mail: Olga.Belyakova@cms-cmck.com


# Ukraine - Data Protection Overview


## Olga Belyakova


4 July 2014

The Ukrainian Law on Personal Data Protection ('**the Law**') - which was adopted by the Ukrainian Parliament on 1 June 2010 and became effective on 1 January 2011, regulates, inter alia, personal data processing.

In addition to enacting this Law, the Ukrainian Parliament also ratified the Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data, on 6 July 2010.

Following the adoption of the Law, other legislative acts providing clarification and support for the Law were approved by different governmental bodies of the Ukraine.

On 3 July 2013, the Parliament of Ukraine adopted amendments to the range of laws related to data protection, including the Law. The Amendments have been effective since 1 January 2014 and have fundamentally changed the substance of the whole data protection system of Ukraine.

Some other changes to the Law have been recently introduced and came into force at the very end of May 2014.

**Scope of the Law**

The Law aims to protect personal data during its collection, storage and processing, and where personal data is used for purposes other than in private or certain professional circumstances.

Firstly, the Law defines personal data as data, or the collection of data, relating to an identified or specifically identifiable natural person.

Furthermore, the Law provides that any individuals concerned have to give their consent to the processing of their personal data (except for anonymised data) where such is deemed to be restricted-access information.

Importantly, the definition of consent to data processing has been reintroduced to the Law at the end of May 2014 (it had been removed for some time). Now consent is defined as the voluntary informed permission of individuals with respect to the processing of their personal data according to the defined purpose of processing. This permission must be expressed in writing or in a form which enables verification that such consent was actually provided.

Further, the Law is clear about the cases when consent is not required, specifically:

1. when it is explicitly provided for by law; and
2. where the data is necessary for the purposes of maintaining national security, economic welfare and for the protection of human rights.

In relation to the processing of personal data, the following are specially exempted from the ambit of the law:

1. individuals processing data for their personal or household needs; and
2. processing of personal data exclusively for journalistic and creative purposes provided the balance between the right to respect of personal life and right to freely express the views are duly balanced.

**Supervisory Authority**

Until 1 January 2014, the Law required the establishment of a special authority with responsibility for supervising compliance with the Law's provisions.

Such an authority was established by the President's Order (1085/2010) on 9 December 2010. Under this Order, the State Service of Ukraine for Personal Data Protection ('the Authority') enjoys the status of a central governmental body.

However, according to the Amendments, starting from 1 January 2014, the Ombudsman took over the Authority, and became in charge of almost all issues related to data protection. The Authority is to be abolished as a result of proposed changes; however, formally, no governmental decision has been passed in that regard. Therefore, in fact the Authority continues to exist, although it does not really perform the data protection functions any longer.

The above changes are claimed to bring the Ukrainian law into compliance with the EU standards, specifically in relation to the independent functioning of a state body regulating data protection. It is believed that the Ombudsman is considered to be sufficiently independent from the government bodies and other state bodies and is able to perform data protection functions, while the Authority, being a government authority which was coordinated by one of the Ministries, lacked the necessary level of autonomy.

To date, the Ombudsman seems to be active in the sphere of data protection and has passed a couple of important regulations (please see the overview below).

**Requirements for Processing Personal Data**

1. General requirements

Mere notification of the processing of certain personal data about individuals will not be sufficient; the controller of the personal data must always obtain their explicit consent. There is no specific requirement for the strict 'working' form of consent. In the meantime, the Ombudsman released an indicative consent form, which, however, seems to be appropriate for written consent only (it seems to be excessive for electronic consent). In any event the business is free to use its own corporate templates for consent provided it they comply with the requirements of the Law.

When giving their consent to the processing of personal data, data subjects are entitled to limit the scope of the data processing undertaken by the database owner.

2. Special categories of data

Notably, the processing of sensitive personal data is explicitly prohibited , i.e. data which relates to racial or ethnic origin, political, religious or philosophical beliefs, political party or trade union membership, as well as data concerning the health or sex life and biometric and genetic data of the data subjects.

The Law further provides for a range of exemptions from the rule relating to the processing of sensitive personal data, some of which mirror those set out in Paragraph 2 of Article 8 of the EU Data Protection Directive (95/46/EC), although it also offers some additional grounds for exemption from the restriction. In particular, the restriction does not apply to cases where the processing of personal data concerns, inter alia:

1. sentences in criminal cases;
2. provision of some medical services by medical practitioners bound by professional non-disclosure obligations;
3. personal data which was made publicly available by the data subject.

Interestingly, the Law also operates a definition of another type of data: 'data which comprises a special risk for the rights and freedoms of individuals' ('Special Risk Data'). In turn, the Ombudsman set up the list of the types of Special Risk Data, which is not to the same as sensitive data.

Specifically, in addition to sensitive data, the following are recognised as Special Risk Data:

1. nationality;
2. an individual's location and routes of movement;
3. whether an individual has suffered from violence or other abuse.

The Law provides for a slightly different regime for the Special Risk Data. In particular, a data controller must notify the fact of processing of the Special Risk Data to the Ombudsman. This is a post-factum notification, which should be made within thirty days after the beginning of processing of that category of personal data. The notification is subject to a formal procedure adopted by the Ombudsman. At the same time, some exemptions apply (e.g. processing of certain Special Risk Data for employment purposes).

**Database Registration Abolished**

The Law initially introduced a mandatory requirement to register any database with the State Register of Personal Data Databases.

However, since 1 January 2014, businesses no longer have to register their databases which contain personal data. Instead, data controllers have to notify the Ombudsman about the processing of Special Risks Data.

**Third Party Access to Personal Data**

Third party access to personal data should be governed by the terms and conditions of the data subjects' consent to the processing of their personal data. If the consent provided by the data subjects covers the possibility of the database owner providing access to third parties, then the provision of such access will be permitted.

Further to this, the Law explicitly states that a third party may not be granted access to certain personal data if it refuses, or is unable to, commit to, or is unable to fulfill the provisions of the Law - including those regarding the protection of personal data.

In order to access personal data, third parties must make an official request to the database owner. The request must contain information relating to:

1. the full name and contact details of the third party;
2. the name and other details of the individual whose personal data is requested which enables the owner to identify the individual;
3. the database from which the request is being made, or the owner/manager of the database;
4. the list of personal data requested; and
5. the purpose and/or legal grounds of the request.

Third party access to personal data may be chargeable in an amount to be decided by the Ukrainian Government for the state authorities, and by the companies themselves in the private sector.

Unlike third parties, individuals should have free access to their personal data stored in a database.

**Cross-Border Transfers**

The Law requires that personal data is transferred only to countries which provide an adequate level of data protection. Specifically, the Law refers to the members of the European Economic Area, as well as all other countries who joined the Convention of the Council of Europe on Protection of Persons in Connection with Automated Personal Data Processing

(‘**the Convention**’).

The above list is not exhaustive and the Law provides that other countries that provide an adequate level of data protection (i.e. non-EEA members and non-members of the Convention) will be defined separately by the Cabinet of Ministers of Ukraine. This is really important in terms of business activity in Ukraine where important business relations have been developed with, inter alia, the USA and Canada, those countries being outside the EEA and the Convention. There is a chance they will be included in the additional list.

The Law offers five alternative grounds which may serve as a legal justification for cross-border data transfer and gives business entities some room to process personal data internationally.

These grounds are:

1. providing unambiguous consent by the data subject;
2. necessity to conclude or fulfill an agreement between the data controller and the third party for the benefit of the data subject;
3. necessity to protect vital interests of the data subject;
4. necessity to protect public interest or pursue legal remedies; and
5. providing relevant guarantees by the data controller regarding non-interference with the private and family life of the data subject.

**Liability for Infringement**

In June 2011 the Parliament of the Ukraine adopted the law strengthening administrative and criminal liability for failure to comply with the data protection laws (‘**the Liability Law**’). Before the enactment of this law, the regulation of such liability was vague, and the strength of the sanctions which could be imposed was too weak to be a deterrent for any infringers.

The Liability Law has become fully effective since mid 2012 and has been further altered by the Amendments with effect from 1 January 2014.

Although the Amendments narrowed the administrative liability for infringements in the data protection area is (mostly due to abolition of the data controller’s obligation to register personal databases), some sanctions for noncompliance with certain data protection rules still exist. For example, failure to inform the Ombudsman of processing of eligible personal data may be subject to fine in an amount of up to UAH 24,000 (ca. €2,300). Further, illegal collection, storage or dissemination of personal data could even lead to criminal liability, including the imposition of large fines, or even imprisonment for a term of up to five years.

**Case Law Interpretation**

On 20 January 2012 the Constitutional Court of Ukraine adopted its Decision (‘the Decision’) which provided official interpretation regarding the position of information concerning the personal and family life of an individual, and also confirmed the rule regarding the mandatory obtaining of the data subject's consent for collection, storage, use and dissemination of such information by any person, including state and local bodies. The Decision has a status of law and compliance with it is mandatory.

**Acts by the Ombudsman**

As mentioned above, the Ombudsman started her activity as the data protection watchdog on 1 January 2014. Since then, she has been active in issuing new regulations required by the Amendments.

Specifically, the following legislative acts in the data protection area have been adopted by the Ombudsman:

- The Sample Order of Personal Data Processing;
- The Order of Conducting by the Ombudsman of Supervision over Compliance with the Personal Data Protection Laws
- The Order on Notification of the Ombudsman About Special Risk Data.

In addition to these pieces of legislation, the Ombudsman produced several guidelines which bring clarity to how certain provisions of the Law should be used.