NOBLES

GENERAL DATA PROTECTION REGULATION: MAIN TERMS AND COMPLIANCE

The reform of the EU data protection legislation led to the adoption of the General Data Protection Regulation (Regulation (EU) 2016/679 of April 27, 2016, "**GDPR**") in April 2016.

The GDPR, which applies from May 25, 2018, has replaced the Data Protection Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data **("Data Protection Directive").**

The GDPR preserves and develops the core principles and rights of the individuals provided for in the Data Protection Directive. Furthermore, it introduces new obligations requiring organisations to implement data protection by design and by default; to appoint a Data Protection Officer ("DPO") in certain circumstances; to comply with a new right to data portability; to comply with the principle of accountability. Importantly, the GDPR is also meant to operate extraterritorially in certain cases.

The GDPR applies to EU controllers (organizations that determine the purposes and means of the processing of personal data), processors (organizations that process data on behalf of data controllers, e.g. cloud service providers, SaaS vendors, or payroll service providers), as well as to companies outside the EU which offer goods or services to individuals in the EU or monitor their behaviour within the EU.

Controllers/processors which have 250 or more employees are required to maintain a record of all processing activities.

Consent of an individual concerned is one of the six legitimate grounds for processing personal data. An indication of consent must be unambiguous and involve a clear affirmative action. For companies this means an overhaul of sign-up forms. The GDPR specifically bans pre-ticked opt-in boxes and gives a specific right to withdraw consent. Controllers shall inform individuals about this right and offer them easy ways to withdraw consent at any time.

From now on, EU residents are also entitled to have their personal data transmitted directly from one controller to another. To facilitate this, a controller shall develop interoperable formats that enable data portability for individuals.

The GDPR requires personal data to be processed in a manner that ensures its security. This includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage by using the appropriate technical or organisational measures.

Such measures shall be implemented at the earliest stages of the processing operations design, in a way that safeguards privacy and data protection principles right from the start ('data protection by design'). It can be done via the use of pseudonymisation (replacing personally identifiable material with artificial identifiers) and encryption (encoding messages so only those authorised can read them).

Personal data must be processed with the highest privacy protection (e.g. a short storage period, limited accessibility) so that by default personal data is not accessible to an indefinite number of persons ('data protection by default').

All controllers are obliged to report certain types of personal data breach to the relevant authority within 72 hours of becoming aware of the breach. If the breach is likely to result in a high risk of adversely affecting individuals' rights, the controller must also inform those individuals. There will be a personal data breach whenever, e.g., any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

Contacts:

Volodymyr Yakubovskyy
Partner

T +380 44 495 30 83
v.yakubovskyy@nobles-law.com

Liudmyla Gorodnycha
Senior Associate

T +380 44 495 30 92
l.gorodnycha@nobles-law.com

When a controller/processor is established outside the EU, that company needs to appoint, in writing, a representative (natural or legal person) within the EU. The representative will act as a point of contact for requests of EU regulatory authorities or individuals and represent the controller/processor regarding their obligations under the GDPR.

A controller/processor is exemptied from the obligation to appoint a representative only if the following conditions are met cumulatively: (i) personal data is only processed occasionally, (ii) the processing does not include a large-scale processing of special categories of personal data or personal data relating to criminal convictions and offences, and (iii) the processing is unlikely to result in a risk to the rights and freedoms of data subjects.

Moreover, controllers/processors must appoint a DPO when their core activities consist in large-scale, regular and systematic monitoring of individuals (e.g. online behaviour tracking) or large-scale processing of special data categories (i.e., sensitive data, such as health, religion, race, sexual orientation, etc.).

The GDPR also introduces a new obligation to perform a data protection impact assessment ("**DPIA**") before carrying out processing likely to result in high risk to individuals' interests/data protection rights.

How it will work for Ukrainian companies

The GDPR applies to a Ukrainian company when it: (i) has employees who are EU citizens; (ii) monitors behaviour of individuals in the EU; (iii) offers/sells goods or services to EU residents; (iv) uses EU residents' data for its products.

In this respect, offering goods or services might be evidenced by reference to a language or currency generally used in the EU with the possibility of ordering goods/services from Ukraine, and/or mentioning customers or users who are in the EU. Monitoring of behaviour will occur, e.g., where individuals are tracked on the Internet by techniques which apply a profile to enable decisions to be made/predict personal preferences, etc. If an EU citizen buys flight tickets from a Ukrainian airline, the latter must comply with the GDPR for processing his/her personal data.

Fines for failure to meet data protection compliance obligations are considerable and reach up to EUR 20 million or 4% of total worldwide annual turnover of an undertaking in the previous financial year (whichever is greater). However, the enforcement of the fines with regard to non-EU companies remains questionable since no respective cross-border legal mechanism is provided.

Nevertheless, to be on a safe side, Ukrainian companies affected by the GDPR should audit their global data processing activities and update/develop operational policies and procedures, in particular:

(i) create a record of personal data processing activities;
(ii) reduce unnecessary data collection;
(iii) consider making some data anonymous or pseudonymous by replacing obviously personal details with another unique identifier, typically generated through hashing, encryption, or tokens;
(iv) determine the need to designate a DPO and/or representative in the EU;
(v) fulfill data access and delete requests (understand how the customer will reach out to the company to make data access or delete requests);
(vi) bring concent forms, data protection policies and privacy notices in line with the GDPR;
(vii) have in place a process for determining whether a DPIA is required;
(viii) develop procedures to detect, report and investigate a personal data breach

***

About Nobles

Nobles is a full-service corporate law firm that advises public and private companies, banks, financial institutions, private equity firms, funds, investment banks, government entities and private high-net individuals in multiple industrial sectors and practice areas of Ukrainian and international business law. In particular, the firm has market leading know-how and an extensive track record in areas such as: antitrust/merger control, insolvency and restructuring, corporate, mergers and acquisitions, real estate and land law, commercial and competition, employment, litigation and international arbitration, intellectual property, regulatory and governmental affairs.

LLC Nobles
7/11 Khreschatyk St.,
01001 Kyiv, Ukraine
T +380 44 495 30 80
F +380 44 495 30 90
Info@nobles-law.com
www.nobles-law.com