Data Protection in Poland and Ukraine: TOP-5 topics

The GDPR[1] aims to harmonize data protection laws in EU member states and better protect the rights of individuals. In a rapidly changing world, personal data flows within the EU (EEA), but more importantly between EU/EEA and other countries, are almost a daily occurrence. Relations between Poland and Ukraine have recently become more important, and the flow of data, including personal data, between the two countries has increased. However, their data protection frameworks differ. It is therefore worth knowing the basic rules involved, what is similar and what's not.

How close are we? What personal data protection regulations apply in Poland and Ukraine?

In Poland, the protection of personal data is regulated by EU regulation – the GDPR – directly applicable in Poland, on the one hand, and by the Personal Data Protection Act[2], as well as by 'sectoral' laws containing regulations on personal data protection (e.g. Labour code, Public procurement law, Banking law) – on the other hand.

Ukrainian Data Protection Law is to a considerable extent inspired by the EU Directive 95/46/EC. Sectoral laws govern some data protection aspects too. To deal with new challenges and to pursue the EU-integration path, Ukraine is now working on a new data protection law, which is essentially meant to implement the GDPR rules. Furthermore, the Ukrainian Data Protection Authority (DPA)[3] employs approaches aligned with EU practices to the extent it is possible under local laws.

Key similarities

- Both employ similar notions of "**personal data**", "**data subject**", "**data controller**" and "d**ata processor**", as well as the "**processing of data**".
- Hence, data controllers need to establish the purposes and grounds for data processing, as well as the relevant procedures and data security measures, normally done in an internal data protection policy.
- Recognized are such common legal grounds for data processing as **data subject's consent**, a need to **exercise an agreement with data subject** and a need to **comply with legal requirements.**
- Severer restrictions are in place as to processing of so-called **sensitive personal data**, including health, biometric and genetic data, data on ethnic and racial origin, political opinions and others. Although the scope of sensitive data under Ukrainian laws and the GDPR differs, e.g. under the GDPR, data on criminal convictions is not sensitive data while it is in Ukraine.
- There are **notification requirements**, namely a data subject must be notified regarding data controller, the scope of data collected, data subject's statutory rights, the purpose of data processing and the persons to whom the data is provided.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals concerning the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC
[2] Act of 10 May 2018 on the protection of personal data
[3] Office of the Ukrainian Parliament's Commissioner for Human Rights

What's different

Legitimate interest

Processing data where it '*is necessary for the legitimate interests pursued by the controller or by a third party*' is the legal basis for data processing often relied upon in the EU (Art. 6 (1) (f) of the GDPR).

Ukrainian law provides for *'a need to protect data controller's or a third-party data recipient legitimate interests*', **which is usually understood narrower**, such as allowing to process data for legal proceedings or similarly.

Data protection officer (DPO)

Under the GDPR, the appointment of a DPO is mandatory in three cases: (i) when the processing is carried out by a public authority, (ii) when the main activity of the data controller or data processor involves the large-scale processing of sensitive data or data relating to criminal convictions; and (iii) when the main activity of the data controller or data processor consists of processing operations that require regular and systematic monitoring on a large scale.

Appointment of a DPO (or data protection division) is only required from data controllers and data processors who process sensitive data.

Notification of processing sensitive data

Not required under the GDPR.

Controllers and data processors who process sensitive data must also notify the Ukrainian DPA of such data processing and appointment of the DPO.

Local representative

In certain cases specified in the GDPR, a data controller or data processor, that are not established in the EU, should appoint a representative in EU's member state to handle data protection matters.

There is no requirement for a foreign data controller or data processor to appoint a representative in Ukraine to handle data protection matters.

Reporting a data breach

Under the GDPR there is a requirement to notify the data protection authority of the data breach, and if the breach might result in a risk of violation of the rights or freedoms of natural persons, those affected persons must also be notified.

There is no requirement to report a data breach to the data protection authority. However, data controller shall notify data subjects and other persons to whom the data was provided, about changes, removals or destructions of, or restriction of access to personal data, regardless of whether a data breach was the reason.

Penalties

In **Poland,** the most severe sanction for violations of personal data protection and other provisions of the GDPR are administrative (financial) fines, which are imposed by the President of the Office for Personal Data Protection. The data controller (or the data processor) can be fined up to EUR 20,000,000 or up to 4% of the company's total worldwide annual turnover of the preceding financial year (with the higher amount applying) – depending on the type of violation.

In addition to an administrative fine, the Polish law also provides for criminal liability if the processing of personal data is not permitted or is processed without authorization. Where a person has suffered damages (both pecuniary and non-pecuniary) as a result of a data breach, the affected person may claim compensation from the data controller and data processor in civil proceedings.

In **Ukraine** penalties are considerably lower. Failure to (i) comply with the procedure on protection of personal data, which led to illegal access to such data or violation of data subjects' rights, or (ii) to make notification to the DPA regarding processing of sensitive data or (iii) to follow DPA's demands/prescriptions regarding prevention or elimination of data protection breaches may result in an administrative fine of up to around EUR 405[4]. A fine may be doubled for repeated infringement within a year. However, serious increase of the amounts of fines is to come with the new Data Protection Law.

In addition, a data subject or another party affected by an infringement is entitled to bring a civil action requiring cease of infringement and compensation of damages.

Cross-border data transfers from Poland to Ukraine and vice versa

Poland (GDPR) requirements for data transfer to third countries (non-EEA countries):

The GDPR allows transfers to third countries on the basis of, among other things, a decision by the European Commission (EC) confirming that the third country provides an adequate level of protection (such decisions have been issued in relation to, e.g. UK, USA, Japan), binding corporate rules, standard contractual clauses adopted by the EC, or approved codes of conduct and certification mechanisms.

Ukrainian requirements for international data transfers:

- Data transfer to the EU and Convention 108[5] member states is allowed on general legal grounds for data processing, as these countries are recognized to provide sufficient level of data protection. However, for transfer to other countries additional grounds may need to be invoked, e.g. express consent for such transfer or a need for defending public interest, or for the establishment, exercise or securing of a legal claim.

- There is neither express requirement to have a data transfer agreement, nor any guidance on the relevant contractual terms. However, based on general data protection rules, would be needed for the parties to agree on the terms of data transfer, including the scope, purpose and duration of data processing, as well as the obligation of the receiving party to take data security measures.

[4] Under current exchange rate
[5] Convention for the Protection of Individuals on Automatic Processing of Personal Data of 1981

ASTERS

SOŁTYSIŃSKI KAWECKI SZLĘZAK

Contact us!

Julia Semeniy
Partner, Head of Intellectual Property at Asters Law Firm (Ukraine)
julia.semeniy@asterslaw.com
+380 44 230 6000

Sylwia Macura-Targosz
Senior Associate, attorney-at-law at SK&S Law Firm (Poland)
sylwia.macura-targosz@skslegal.pl
+48 694 415 447