Data Protection perspective

In the case of transferring, even temporarily, a business from Ukraine to Poland, all databases are usually transferred as well, including databases in which personal data is processed. How to ensure that these databases can continue to be used legally? Does the change of the country where data processing actually takes place so significantly affect the possibility of using databases that had previously been used entirely lawfully? And what if the processed data does not concern citizens of the EU, but only citizens of Ukraine? Below we answer some of the key questions by presenting a practical approach to data processing in the new legal reality.

Ukraine legal framework

Ukraine, not being a member of the European Union or the European Economic Area, has its own regulations that provide the legal framework for personal data processing. The crucial regulation is the "Law on Protection of Personal Data" dated 1 June 2010 No. 2297-VI, which in terms of its material provisions is compliant with and derives from the predecessor of GDPR - EU Data Protection Directive 95/46/EC.

Moreover, in Ukraine there is no separate, specialized data protection authority, as required by the GDPR. On 1 January 2014, the Ukrainian Parliament Commissioner for Human Rights (Ombudsman) was designated the public authority responsible for monitoring compliance with data protection legislation, and since then the Commissioner has enacted several generally applicable orders efficiently performing the assigned role.

Transfer of personal data outside of Ukraine

Under Ukraine legislation personal data may not be processed for purposes other than those for which it was collected. Therefore, in this regard, Ukrainian law operates in the same way as in the EU territory.

Furthermore, Ukrainian legislation requires that personal data can only be transferred to countries which provide an adequate level of data protection. Notably, the legislation specifies that an adequate level of data protection is ensured by:

1. the members of the European Economic Area,
2. countries that joined the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) – the list of signatory states to the Convention is available on the official website of the Council of Europe: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=108.

Therefore, personal data transfers to Poland do not require additional prerequisites to be met other than a legitimate legal basis for the processing.

Importantly, Ukrainian data protection legislation does not have an "extraterritorial effect" (i.e. does not apply to entities outside of Ukraine). Ukrainian legislation does not include any reference to the nationality/residence of persons whose personal data is to be protected – it is therefore assumed that the territorial principle applies, meaning that personal data relating to all individuals within Ukraine only is subject to protection.

Processing data transferred from Ukraine under GDPR

If a cross-border transfer of personal data is planned, the prerequisite of a legitimate legal basis for such a transfer must be met. However, this applies not only to a legal basis under Ukrainian law, but, as the data transfer is made to an EU country, a relevant legal basis for processing under GDPR should also be found. This is regardless of the fact that in many cases no data of EU residents is processed.

This is due to the fact that the GDPR applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the European Union. Whenever personal data is transferred due to the establishment of a company or a subsidiary in Poland, such data should be processed in compliance with the GDPR.

This means that if personal data database has been created in Ukraine and now is being transferred with an intention to be used by an establishment in Poland, a legal basis for the processing of such data which was valid in Ukraine should now be subject to verification under the GDPR standards.

This concerns in particular sensitive data such as data concerning health. Under the GDPR it can be processed in limited cases especially in the field of employment, social security and social protection law in so far as it is authorised by the European

legislation or a Member State's law. If an employment contract is subject to Ukrainian law, then this legal basis is invalid and most likely consent (or another legal basis) in needed.

Another important matter is the provision of sufficient information under art. 13 and 14 of the GDPR due to the fact that information provided to data subjects under GDPR is quite different and broader than information that ought to be presented based on Ukrainian regulation. In particular, under Ukrainian law, the data subject should be informed of his/her rights, which does not include data subjects rights under GDPR, such as e.g. right to be forgotten.

Return transfer to Ukraine

A return transfer of personal data to Ukraine most likely might fall into the strict GDPR regime of data transfers to third countries, as under the GDPR and according to current decisions of the EU Commission, Ukraine is not considered as providing an adequate level of protection.

When assessing the data transfers to "non-adequate jurisdictions" under the GDPR such as the Ukrainian jurisdiction, in order to ensure their security and reliability, one can follow the European Data Protection Board recommendations which provide step-by-step guidelines:

- Step 1: Know your transfers,
- Step 2: Verify the transfer tool,
- Step 3: Assess the law and the practices of the third country (Ukrainian) recipient.

Following these steps will most likely lead to a conclusion that the Standard Contractual Clauses (SCCs) are the simplest solution to govern the return data transfers.

Summary

In each case of transferring personal data from Ukraine to an EU Member State, e.g. Poland, there are steps to be taken to assess the full compliance and, if needed, to comply with requirements set forth not only by Ukrainian legislation, but also the GDPR. We recommend conducting such an analysis at the earliest possible stage. This will ensure a peace of mind not only in case of intervention of the Polish Office for Personal Data Protection, but most of all in case of further development of a company, especially if due diligence of a company is to be conducted with the intention of finding an investor or selling the company.

Contact :

In case of additional questions, we encourage you to get in touch with our experts:

Anna Matusiak-Wekiera
Radca prawny (Attorney-at-law)
Head of Data Protection/
Compliance Practice

anna.matusiak-wekiera@jdp-law.pl

Krzysztof Bąk
Radca prawny (Attorney-at-law)
Associate

krzysztof.bak@jdp-law.pl