Oksana Zadniprovska,
CIPP/E and CIPM, partner at Axon Partners

Transfer of data from the EU to Ukraine: is it safe?

Ukraine is in the middle of the war. This means there is martial law, which influences the status of essential equivalence for the purpose of data transfers from the European Union. This article intends to help in assessing the safety of transfers to Ukraine.

1. Transfer of data to Ukraine from the EU: what is the status of Ukraine?

In June 2022, the European Council **granted** candidate status to Ukraine. However, Ukraine is not an EU member yet, and it will take years to get that status. Ukraine is also not in the European Commission's **list of the countries** which provide for an adequate level of personal data protection.

This results in only one quick and practical way for the EU data exporters who transfer data to Ukraine to comply - to conclude the standard contractual clauses under **Art.46 GDPR** (SCCs). But before that, to make sure the SCCs are working as they should - the data exporter (with the help of the data importer) shall make a transfer impact assessment (TIA).

The TIA is required in response to the ECJ decisions in **Schrems I** and **Schrems II cases**, and should be based on the EDPB **recommendations on European Essential Guarantees** and **on measures that supplement transfer tools**.

Let's remember that In the Schrems II case, the ECJ decided that surveillance measures in the U.S. were not sufficiently limited, and there was no effective redress available to data subjects to enforce their rights. As a result, the level of protection in the U.S. was not "essentially equivalent" to that guaranteed within the European Union, and the "Privacy Shield" was invalidated. Although the decision regarded the adequacy of the U.S. within the "Privacy Shield" framework, the "essential equivalence" is an important concept to discuss for the "appropriate safeguards", one of which is the SCCs. Before signing the SCCs, the level of protection in the country to which data is transferred shall be additionally assessed. If the laws and practices of a third country impinge on the guarantees established in the SCCs, the EU data exporter shall cease transfer.

Thus, in each particular case, before applying the SCCs for the transfer from the EU to Ukraine, the TIA should be made to assess whether the SCCs would work in Ukraine as intended.

Copyright PrivacyRules© - All rights reserved 2016-2023

2. How should the TIA for the Ukrainian jurisdiction be done?

Referring to the **EDPB recommendations**, TIA shall help the data exporter to check if the SCCs are enforceable in Ukraine. If the analysis shows essential equivalence of protection - the SCCs could be used. Otherwise, the data exporter shall either apply additional technical/organizational measures to protect data or the data exporter shall not transfer data at all.

In practice, to make the TIA for Ukraine, the following steps shall be made:

1. **Analyze the details of a particular data transfer.** The data exporter shall know which data is transferred (sensitive, children's data or just usual personal data of adults, the amount of such data) and what is the purpose of the transfer (for storage or for the analysis; for support only or for including into the databases). Here, it is also important to make sure that there is a transfer. The EDPB, in its **guidelines** on the interplay between the application of Article 3 and the Chapter V GDPR, provided a wide definition of transfer. From the Ukrainian perspective, there should be a data exporter in the EU, the data importer in Ukraine, and the data exporter shall in any way make the personal data available to the data importer in Ukraine. This is not only about the physical transfer of databases or sending personal data via email - the mere access to data from Ukraine could be regarded as the transfer.
2. **Choose the appropriate transfer mechanism.** For the purposes of this article, let's choose the standard contractual clauses (SCCs).
3. **Describe the up-to-date Ukrainian laws and practices** on (1) personal data protection, (2) surveillance and disclosure of personal data on request of the law enforcement or other agencies, and (3) efficiency of the judicial system and enforcement of data subject rights in general.
4. **Decide if the protection is enough**. Nowadays, the laws and practices of Ukraine could impinge on the effectiveness of the SCCs. In most cases, the data exporter and the data importer shall apply additional safeguards that would minimize the risks.
5. **Remind the data importers that they have certain obligations**. It is crucial to monitor laws and practices for any changes. For Ukraine, this is indispensable, as Ukraine is a country with martial law in place.

Copyright PrivacyRules© - All rights reserved 2016-2023

3. Laws and practices on personal data protection and access to data by authorities: was there ever "essential equivalence" ?

Before the war, Ukrainian lawyers had never claimed in the TIA that Ukraine ensured the essentially equivalent level of personal data protection to that in the EU. But still, the SCCs could be enforceable. There were many reasons for that.

Starting from the bright side, human rights, including the right to privacy, are respected in Ukraine. The reasons are:

- Ukraine is a party to the **European Convention on Human Rights** and **Convention 108**.

- The principle of the **rule of law** is included into our Constitution, together with the protection of the **right to privacy**.

- As of 2010, Ukraine has a separate **Data Protection Law**, which is updated from time to time.

- Ukraine has a **data protection authority** (the department for Personal Data Protection of the Secretariat of the Verkhovna Rada of Ukraine Commissioner for Human Rights). The Commissioner may audit companies for compliance, handle data subjects' complaints and impose fines.

- Finally, Ukraine has an EU candidate status **from June 2022**, so it is getting closer to the EU standards of laws and principles. Ukraine has GDPR-like draft laws registered in the Parliament on the **independent DPA** and **data protection obligations**.

A general overview of the legal framework in Ukraine on personal data protection is available in our earlier **article for PrivacyRules**.

As to the restrictions on privacy rights and access to personal data by the authorities - there are both positive signs, but also certain gaps that do not allow us to conclude on the "essential equivalence" of the data protection to the EU level.

Copyright PrivacyRules© - All rights reserved 2016-2023

The good news

- The Data Protection Law **allows** the restriction of data protection rights only to the extent necessary in a democratic society in the interests of national security, economic well-being, or protection of the rights and freedoms of people.
- No laws allow silent or indiscriminate surveillance activities.
- The **Law of "On intelligence**, **"On law enforcement intelligence operations"** include some provisions on the necessity and proportionality of the restrictions.
- Also, before the war, the **Criminal Procedural Code** introduced the independent oversight mechanism - within the investigations, access to personal data could be granted only on the basis of the decision of the investigatory judge.
- Although law enforcement authorities and investigating judges had some discretion in defining the limits on the duration of the investigative activities, the **Criminal Procedural Code** set maximum periods of duration for the relevant measures.
- There were certain options to contest the procedural violations before the judge: in case of abuse of powers, e.g. during the search or seizure activities, the company or the data subject might object against the admissibility of the unlawfully collected evidence, initiate a criminal investigation for the abuse of powers, and then ask to compensate for the damages within the civil proceedings.
- The information received during the investigation shall not be disclosed and shall be protected, as well as shall be accessed only by those to whom this is strictly necessary for the investigation.
- A person may also exercise the rectification right before the court or the Commissioner (although the procedure is not clearly defined, the general principles of the Data Protection Law could be applied).
- Finally, the data importer can effectively inform the data exporter if the data importer is under surveillance or criminal investigations. This is because, to the extent possible, the **Criminal Procedural Code** requires that the individual should be informed of the interference if their rights can be interfered with due to the applied investigative actions or precautionary moves.

The problematic issues

Even before the war, were the following:

Copyright PrivacyRules© - All rights reserved 2016-2023

- There was no clear limit for the scope of personal data that could be accessed within the criminal proceedings.
- There was a lack of specific procedures for storing information in electronic form that would ensure the reliability and integrity of such information.
- A case file on the investigation could potentially contain data of other individuals, too, whose rights to access the data related to them are not defined.
- In practice, the investigators in their requests and investigating judges in their decisions were not always specific enough about the amount of information and the list of documents to be accessed and/or seized that leads to broad access to data by law enforcement authorities, in spite of limitations provided for by the laws.
- The overload of the investigating judges was a factor having a negative impact on the quality of the decisions and the performance of their oversight powers in the course of criminal investigation.

But in general, in many cases, the SCCs were enforceable subject to additional safeguards.

4. What has changed in accordance with martial law in Ukraine?

All the problematic issues described above are still applicable. In addition to that, there are new obstacles.

Decree of the President of Ukraine "On the introduction of martial law in Ukraine" allowed the restrictions on the constitutional rights. This includes the right to privacy. But such restrictions should be within the limits and to the extent necessary to ensure the measures within the legal regime of martial law, introduced by the **Law "On the Legal Regime of Martial Law"**.

Based on the Decree of the President, the Criminal Procedural Code was **updated**, together with the law on e-communications. The main change is related to the engagement of the investigatory judge to the oversight in cases when access to personal data is authorized.

Earlier, to apply measures aimed at interfering with the right to privacy of a person in criminal proceedings, the investigator with the prosecutor had to submit a request to the investigating judge to obtain a sanction for such measures. In the request, the investigator had to justify the need for a relevant measure.

Copyright PrivacyRules© - All rights reserved 2016-2023

The investigating judge verified the validity of such a request and defined the necessary limits of the measure. Investigative actions without the prior consent of the investigating judge could be done only in exceptional cases where the matter of saving lives and property or direct prosecution of suspected persons arose.

Now, the Criminal Procedural Code allows the prosecutor to temporarily access metadata on communications, medical, bank, or other personal data **without the investigating judge's decision** if there is no objective possibility for the investigating judge to exercise their powers. Although this is to ensure quick and effective investigation if the judge is temporarily unavailable in very important cases, there are no efficient safeguards in law that would limit the powers of the prosecutor. Unfortunately, this opens doors to abuse of powers and makes the independent oversight mechanism less effective.

5. Should the EU data exporter transfer personal data to the Ukrainian data importer in war times?

The answer is rather "yes", although a lot depends on the details of the particular transfer.

Except for the court oversight practice, the other "positive signs" shown above for the "before war" times are still available, even during martial law. In particular, even despite a higher need to protect national security, Ukraine still does not have a law that allows silent or indiscriminate surveillance activities.

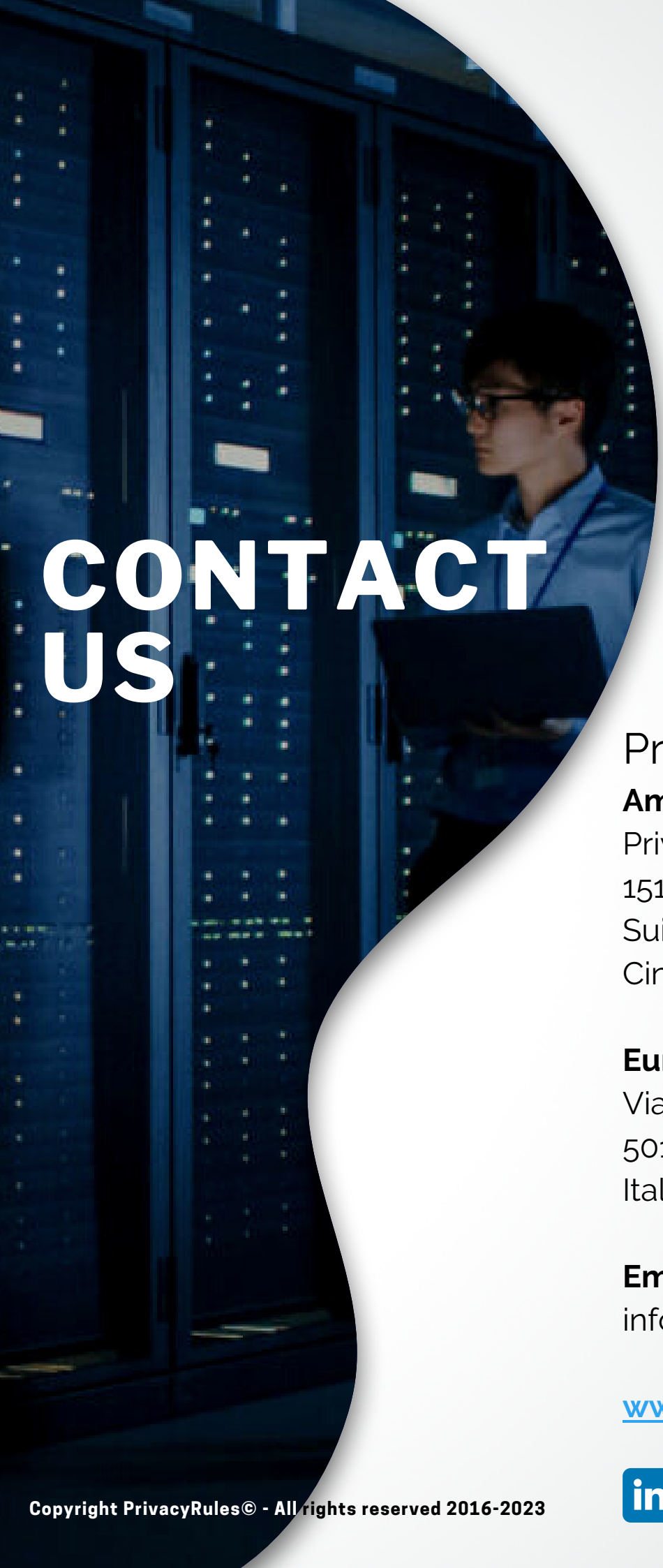
All this leads us to the conclusion that the SCCs may still be applied. Of course, the data exporter shall thoroughly, on a case-by-case basis, discuss with privacy experts which data protection safeguards to choose and how to apply the data minimization and security principles in practice.

Copyright PrivacyRules© - All rights reserved 2016-2023

OKSANA ZADNIPROVSKA,
CIPP/E AND CIPM, PARTNER
AT
AXON PARTNERS

ZADNIPROVSKA@AXON.PARTNERS

Copyright PrivacyRules© - All rights reserved 2016-2023



CONTACT US

PrivacyRules

American Headquarters:

PrivacyRules, Ltd.
151 West 4th Street
Suite 200
Cincinnati, OH 45202, USA

European Office:

Via dei Della Robbia 112,
50132, Firenze
Italy (IT)

Email

info@privacyrules.com

www.privacyrules.com

Copyright PrivacyRules© - All rights reserved 2016-2023