TUCA ZBARCEA
ASOCIATII

20 July 2020

# Legal Bulletin

## Data Privacy

**In this issue:**



## EU-U.S. Privacy Shield invalidated by the CJEU. Practical implications for businesses

On July 16th, the CJEU issued the *Schrems II* judgment which invalidates the Privacy Shield Decision and provides clarifications on SCCs.

A lot of noise and "fog" amongst organizations, particularly on the effects of the *Schrems II* judgement. It is expected for the EU supervisory authorities and EDPB to react soon and to shed more light on this issue for the organizations.

Until then, please find below some key aspects that you should consider.

### 1. What does it mean that the EU-U.S. Privacy Shield was invalidated?

The EU-U.S. Privacy Shield allowed organizations from the European Union to export data to U.S.-based organizations listed under the EU-U.S. Privacy Shield List. The EU-U.S. Privacy Shield was built around Article 45 GDPR, which grants the Commission the right to decide that certain third countries or territories ensure an adequate level of protection for data subjects and therefore organizations are allowed to transfer data to such countries or territories. Hence, the Commission found, in Article 1(1) of the Privacy Shield Decision, that the U.S. ensures an adequate level of protection for personal data transferred from the EU to organizations in the U.S. under the EU-U.S. Privacy Shield.

By way of *Schrems II* judgement, the CJEU found that, on the contrary, the U.S. does not ensure an adequate level of protection (substantially equivalent to that ensured by EU countries) and to this effect ruled out that Commission Decision on EU-U.S. Privacy Shield is invalid.

This means that **EU organizations should not be able anymore to rely on EU-U.S. Privacy Shield for transferring data to U.S.-based organizations.**

**2. What about the ongoing transfers under the EU-U.S. Privacy Shield?**

On this highly sensitive topic, the CJUE was quite blunt and ruled out that organizations should use the alternative data transferring means prescribed under Article 49 GDPR.

To be noted, the U.S. Secretary of Commerce, Wilbur Ross stated on 16 July 2020 that the U.S. Department of Commerce will continue to manage the Privacy Shield program, including processing submissions for self-certification and re-certification to the Privacy Shield Frameworks and shall maintain the Privacy Shield List.

While this is still a "grey" area and it is quite early to put conclusions on the table, unless a new adequacy decision for U.S. is to be adopted by the Commission, most likely the EU-U.S. Privacy Shield will become a "walking dead" and will finally die. We expect that, in line with the CJUE *Schrems II* judgement, **in the near future the EU supervisory authorities and EDPB shall issue (common) positions and further guidance to organizations not to further use the EU-U.S. Privacy Shield and to seek to rely on alternative valid data transfers means.**

**3. Is there any grace period for becoming compliant as regards ongoing transfers under the EU-U.S. Privacy Shield?**

No. Organizations should promptly consider alternative valid means for the transfer of data to the United States. This could be either putting in place adequate SCCs or BCRs (feasibility to be assessed on a case-by-case basis) or using any of the alternative transferring mechanisms described under Article 49 GDPR.

**4. Are standard contractual clauses (SCCs) still valid?**

Yes, in principle. Still, the key issue here would be for EU organizations exporting the data to third countries based on SCCs to be able to prove that the data importer from that third country is able to **actually** meet the safeguards undertaken under SCCs. This would entail that organizations relying on SCCs must verify that the legislation of the third country ensures a similar level of protection as under the EU law as regards the rights of the data subjects.

**5. What should organizations expect for future?**

Firstly, organizations should expect a **significant increase in the number of data subjects' requests for access** focused on data transfers to third countries. We may reasonably assume that the most exposed industries will be telecom, financial (banking included), insurance, health, retail, IT, etc.

Correspondingly, we anticipate an **increase in the number of data subjects' complaints and, to this effect, of investigations** initiated by EU authorities (ANSPDCP included) in relation to data transfers to third countries (irrespective if made based on EU-US Privacy Shield, SCCs or BCRs).

Also, we cannot exclude for the national authorities to open ***ex officio* investigations on the validity of the data transfer mechanisms** used by organizations, with a focus on data transfers

towards third countries. Notably, some of the EU supervisory authorities already called for the need of a unitary approach as regards the dealing with companies that transfer data to third countries.[1]

To be noted, however, maybe the most dramatic impact for the organizations is that as per Article 58 GDPR the EU supervisory authorities (ANSPDCP included) shall be able to **prohibit (temporarily or definitively) or to order the suspension of a data transfer or a set of transfers based on SCC**, if they find that the transfer is likely to have a substantial adverse effect on the guarantees providing adequate protection to the data subject (including where it would be found that the legislation of the data importer in fact prevents the latter to comply with the safeguards committed formally under the SCCs).

Finally, on the regulatory side it is expected that the Commission shall issue **updated versions of SCCs comprising harsher mechanisms** for ensuring adequate and effective protection of data subjects and, most likely, organizations will be bound to enter new SCCs based on these updated versions.[2]

**6. What should organizations do next?**

You may consider pursuing the following steps:

**a.** **Identify urgently and map** all data transfers to third countries for which you rely on EU-U.S. Privacy Shield, SCCs or BCRs.

**b.** For data transfers **towards US**:

i. **Temporary suspend or cease** any data transfers based on EU-U.S. Privacy Shield. Closely monitor any evolution on the topic, particularly the premise of issuance by the Commission of a new adequacy decision for US.

ii. **Seek alternative valid transfer mechanisms** under GDPR, such as SCCs, BCRs or the derogations listed under Article 49 GDPR.

iii. If none of the above is feasible, **assess the business impact** deriving from ceasing any such data transfers immediately **and use alternatives** (such as shifting the database in EU or in a third country recognized as ensuring an adequate level of protection).

**c.** For data transfers to **third countries other than U.S. made based on SCCs**:

---

[1] See, for instance, the statement issued by the German data protection authority HmbBfDI - *https://www.datenschutz.rlp.de/de/aktuelles/detail/news/detail/News/paukenschlag-eugh-schreddert-den-privacy-shield-datenuebermittlung-in-staaten-jenseits-der-eu-aber/*.

[2] In the Opening Remarks on CJUE *Schrems II* judgement Commissioner Reynders highlighted that "*we have been working already for some time on modernising [SCCs] and ensuring that our toolbox for international data transfers is fit for purpose. [...] We are now advanced with this work and we will of course take into account the requirements of judgement*"- see *https://ec.europa.eu/commission/presscorner/detail/en/statement_20_1366*.

i. **Evaluate if the third country's legislation ensures a similar level of protection as EU law does**. *Inter alia*, you should check the legal safeguards related to any potential access to data by the public authorities of that third country and the actual capacity of the data importer to comply with the commitments from the SCCs.

ii. If not the case, you could consider the following:

- ✓ Check if that **third country benefits of an adequacy decision** issued by the Commission. Where affirmative, **initiate negotiations for the termination of the SCCs and further rely on that adequacy decision**.
- ✓ If no adequacy decision exists, you may consider **putting in place additional safeguards to the SCCs** to render the protection of the data subjects effective.
- ✓ If no additional safeguards are available or feasible, you may be willing to **terminate the SCCs and consider alternative valid transfer mechanisms under GDPR (such as BCRs or one of the derogations listed under Article 49 GDPR)**.
- ✓ If none of the above is feasible, **assess the business impact** deriving from ceasing any such data transfers to that third country immediately and **use alternatives** (such as shifting the data base in EU or in a third country recognized as ensuring an adequate level of protection).

**d.** **Review the used information documents** (privacy policies, information notices, etc.) to ensure that you comply with all transparency requirements prescribed by GDPR in terms of data transfers towards third countries.

**e.** **Prepare an action plan** and **present the same to the management** from your organization.

**f.** **Document all steps** to ensure you are able to prove that you put in place effective controls to comply with the GDPR and the new framework set by CJUE *Schrems II* judgement.

*ciprian.timofte@tuca.ro*

# Editors

Țuca Zbârcea & Asociații has an all-embracing experience in providing legal advice in the area of **data privacy/ GDPR** to top companies in Romania and/or abroad, active in various commercial sectors, such as: telecom, financial services (banking, insurance, pensions, etc.), healthcare, pharmacy, e-commerce, IT, energy, food supply, etc.

The legal assistance provided covers all aspects of data privacy, from legal assistance before the local regulatory authority (The National Supervisory Authority for Personal Data Processing – **ANSPDCP**) in relation to various issues (such as notification of personal data breaches, consultation for high risk data protection impact assessments, consultation on sensitive legitimate interest assessments, etc.) to complex legal assistance in the field of data privacy/ GDPR, such as: full GDPR implementation; carrying out data privacy impact assessments (DPIAs) and legitimate interests assessments (LIAs); employee monitoring, geolocation, call history; cookies; cloud computing solutions; auditing of data processors; personal data sharing; negotiation of relevant terms of data processing agreements (DPAs); industry codes of conducts; GDPR/ data privacy trainings; handling of data subjects' complaints, etc. For further information and other recent news relating to Data Privacy, please feel free to visit our firm's blog – *dataprivacyblog.tuca.ro*

Ciprian Timofte
Partner
+40 374 136 341
ciprian.timofte@tuca.ro

TUCA ZBARCEA
ASOCIATII

Şos. Nicolae Titulescu nr. 4-8
America House, Aripa de Vest, et. 8
Sector 1, 011141, București, România
T + 4 021 204 88 90
F + 4 021 204 88 99
E office@tuca.ro
www.tuca.ro