Third Country Transfers – Potentials and Level Playing Field for Codes of Conduct

The adequate protection of data subjects when personal data is transferred to a Third Country must be maintained. Court decisions and GDPR provisions consider data subjects subject to additional risks, acknowledging such risk will be dependent on the Third Country. In the absence of adequate safeguards, also due to recent jurisdiction, some Third Country Transfers are significantly challenged currently.

This contradicts and prevents businesses' cross border activities in a globalized world and makes Third Country Transfers a highly debated topic. Against this background the industry has a strong need for safeguards putting Third Country Transfers on a solid legal ground. Due to the need for individual assessment of each transfer, all-in-one solutions will prove highly complex, overly burdensome, because the risks supposedly being addressed are potentially not applicable, and thus limitedly suitable to serve as safeguards. Instead, there is a need for tailored, yet cost efficient and therefore not individual-driven safeguards. As such, Codes of Conduct and Certifications lend themselves as solutions, but whose requirements to receive an approval should be equalized as both seem to converge in scope in practice. It can be noted that the industry is already working on its own solutions.

It is desirable that regulators perceive the needs of the industry and do not immediately cut their efforts considering that solutions will be developed further on an ongoing basis.

selbstregulierung
informationswirtschaft e.V.

1. Background

Third Country Transfers have been given more attention for some time now due to geopolitical tensions and growing sensitivity for personal data. The origins of the debate as to whether and under which conditions personal data may be transferred to Third Countries were related to authority and governmental access to personal data of European citizens by non-European authorities/governments without safeguards such as (prior) judicial review by European courts. Subsequently the ECJU decided upon adequacy decisions regarding the US with the result of twice voiding them. At the present time the discussions about Third Country Transfers become potentially counter indicative to the intensified need for digitalism and related cloudfirst strategies as well as overly simplified though addressing highly complex scenarios and eventually extending and shifting applicability of precedence to even further use cases due to a lack of legal certainty. The following article deals with the necessity of bringing these discussions to operationalizable solutions and the requirements for such.

2. Due protection of Data subjects

Undisputedly data subjects must remain protected regardless of the location of processing. Considering this, undermining applicable regulatory frameworks by reallocation of activities is undoubtedly to be prevented. The dilemma to be faced in this respect is that there is no undermining led by businesses, as the associated risks result from authorities' and governmental access. It is to be noted and taken into account that undue surveillance does hardly stop at territorial borders.

3. Need for adequate mechanisms adapting to transfer related risks

When assessing whether a Third Country Transfer may take place, it is necessary to refrain from mixing up of general risk associated with a certain sector, processing activity or outsourcing in general. Instead an individual analysis of Third Country specific risks is required which should be freed from political dimensions, as those should not be resolved neither by data subjects nor by businesses but rather by those stakeholders who are destined to do so.

In such an analysis the general legal risks respectively risk clusters and related measures are to be assessed rather than focussing on territories, as the legal framework (either literally or in its application) may constantly change. Ambiguities and the unfortunate mixup of several dimensions bring any existing mechanisms as safeguards for Third Country Transfers at risk. Third Country Transfers therefore are often safeguarded by redundant mechanisms, such as adequacy decisions pursuant to Article 45 GDPR, standard contractual clauses pursuant to Article 46.2 (c) GDPR and binding corporate rules pursuant to Article 47 GDPR.

As those three current main solutions sometimes require high individual expenses and their scope of application is limited, in practice, more tailormade solutions – as additional – alternatives appear needed. Such solutions could be Codes of Conduct pursuant to Article 40 GDPR ("Code of Conduct") and Certifications pursuant to Article 42 GDPR ("Certifications") as suggested by Article 46.2 (e) and (f) GDPR. However, the practical relevance of both measures crucially depends on what legal requirements are posed on them.

4. Level playing field

GDPR's requirement in the context of safeguards for Third Country Transfers for equivalency is not to be understood as identity. Unquestionably the requirements to be met by any solution should be generally comparable, as the object of protection remains identical.

Nonetheless, particularities of each mechanism should be endorsed allowing for effective but also efficient solutions. In relation to Codes of Conduct and Certifications those principles are not always consistently followed, as GDPR – and subsequent guidelines[19] – foresee differences between Codes of Conduct and Certifications; e.g. pursuant to Article 40.3 GDPR in conjunction with Article 40.5 to 40.9 GDPR Codes of Conduct require a general validity (including the involvement of the European Commission), whereas Certifications do not require such additional step (see Article 42.3 and 42.5 GDPR).

This may result from the fact that Certifications address a specific "processing" rather than a company or product in its entirety. Thus, the certified specific technical implementation in its specific version might allow for such a deviation. Practically, Certifications appear less bound to this level of detail, considering recently published schema. Schemas appear targeting a large range of different processing operations and providing rather for a management system as specific technical and organizational measures are only to be applied if an evaluation process has

[19] https://edpb.europa.eu/system/files/2022-03/edpb_guidelines_codes_conduct_transfers_after_public_consultation_en_1.pdf

shown that particular data are processed. In this sense, the differences in formalities should not result in significant mistreatment.

Saying, where Codes of Conduct and Certifications practically become almost identical from a material point of view, GDPR's requirements imposed on them should be equal – either equally simple or equally complex.

5. Expectations of the industry

Apart from the requirements defined by law and political stakeholders, also the industry makes demands on safeguards for Third Country Transfers. The industry expects that solutions to be developed will provide an additional level of legal certainty.

Certainly such solutions never will be a carte-blanche, but adhering to a Code of Conduct / Certification should indeed allow for positive statements that adequate supplementary measures are implemented. Where distinct measures cannot be determined it shall be clarified that following a defined methodology to assess Third Country Transfers and subsequently implement measures accordingly will suffice, even if – on a case by case basis – the measures will prove inadequate in future.

On the contrary, where there is any notion that implemented measures were intentionally or gross negligently determined wrongfully or where the defined assessment logic is not applied / documented, the benefits of legal certainty and protection should not apply either.

Solution-oriented initiatives from the industry exist, seeking for support and cooperation with authorities. One of them is the Third Country Initiative[20] of the General Assembly of the EU Cloud Code of Conduct ("EU Cloud CoC" or "Code")[21]. The EU Cloud CoC is a Code of Conduct managed by SCOPE Europe[22], which covers the requirements of the GDPR regarding cloud services and was approved by the Belgian data protection authority in May 2021 after a positive opinion of the EDPB[23]. The General Assembly of the EU Cloud CoC is currently working on a draft of an effective but accessible safeguard for Third Country Transfers by means of a separate on-top module to the Code.

Another example for an initiative from the industry is the Transfer Impact Assessment Tool ("BiTIAT") published by Bitkom[24] which is a software providing Bitkom members with a framework for conducting transfer impact assessments for international data transfers to the US, Brazil, India, Australia and Colombia by standardizing the analysis of the Third Country and the respective data transfer and also the necessary documentation. The software also suggests additional safeguards.[25]

In the context of current efforts of the industry it is expected that Data Protection Supervisory Authorities do not require more from them as what is being managed by public stakeholders themselves. Saying, current ambiguity and uncertainty create an ostrich approach, especially by SMEs.

Acknowledging and endorsing that data subjects shall be protected adequately at all time, pragmatic

[20] https://eucoc.cloud/3rdcountryinitiative

[21] https://eucoc.cloud/en/home

[22] SCOPE Europe b.v.b.a/s.p.r.l. was founded in February 2017 as a subsidiary of Selbstregulierung Informationswirtschaft e.V. (Self-Regulation Information Economy). It is an association supporting the co-regulation of the by acting as a think tank to discuss and debate key issues in digital policy and providing an umbrella organisation for a range of co-regulatory measures in the digital industry. In May 2021 SCOPE Europe became the first Monitoring Body to be accredited under the GDPR pursuant Article 41. More information can be found here: https://scope-europe.eu/en/home

[23] Opinion 16/2021 on the draft decision of the Belgian Supervisory Authority regarding the "EU Data Protection Code of Conduct for Cloud Service Providers" submitted by Scope Europe, 19.05.2021, at: https://edpb.europa.eu/system/files/2021-05/edpb_opinion_202116_eucloudcode_en.pdf

[24] https://www.bitkom.org

[25] https://www.bitkom.org/Themen/Datenschutz-Sicherheit/Transfer-Impact-Assessment-TIA

approaches are appreciated, as well as openness to stakeholders' suggestions, which may allow for dynamic yet effective solutions. In this regard it is to be taken into account that a general resignation eventually provides less protection, as a general endorsement and implementation of good measures, even if such measures are allegedly perfect.

An area as complex as Third Country Transfers, as continuously evolving as legal frameworks, should rather seek for best effort solutions, and continuous improvement, acknowledging that true perfection does not exist. One should not limit the good for the sake of the (potentially never operationalised) better.

selbstregulierung
informationswirtschaft e.V.

About the Authors

The SRIW (Selbstregulierung Informationswirtschaft e.V.) is a non-profit association that was established in 2011 as an umbrella organisation, supporting credible self-regulation and co-regulation in the information economy. Focusing on, but not limited to, data and consumer pro-tection, the SRIW takes a modern regulatory approach that aims to align regulatory requirements with market realities and industry practicalities while protecting consumers interests.

The SRIW has been able to gain valuable practical experience on the extent to which different solutions and processes are at all amenable to economic implementation and approved by the Data Protection Supervisory Authorities.

Moreover, the SRIW has established a subsidiary in Brussels called SCOPE Europe . SCOPE Europe plays a crucial role in strengthening the European perception of the approaches advocat-ed by SRIW and also serves as an officially accredited Monitoring Body under GDPR by more than one Data Protection Supervisory Authority for more than one Code of Conduct.