Schrems II case: The data exporter perspective

Authors: Francesca Gaudino and Valeria Benedetti del Rio

In this blog post we further analyse the impacts of the opinion of the advocate general Hendrik Saugmandsgaard Øe (a.g.) in the Schrems II case.

We will focus, more specifically, on what it means for data exporters and what consequences there may be for them, if the decision of Court of Justice of the European Union (CJEU) on the case is consistent with the a.g's opinion. Data importers will be the focus of another blog post, so keep following us for more updates.

You can check our analysis of the decision here, and our preliminary evaluation of the impacts of the opinion here.

From the indications of the a.g., and also from the interpretation of the accountability principle, an exporter transferring data outside of the EU cannot simply rely on signing an agreement based on the Standard Contractual Clauses (SCC) to be sure to comply with the applicable data protection requirements on data transfer. Indeed, this approach is light years away from the ratio of the GDPR itself, which clearly shifted the heavy lifting from authorities to controllers, in terms of decision-making.

The to-do list for the diligent exporter starts long before the signing of the agreement. Indeed, since the selection phase, the exporter is responsible for choosing a reliable counterparty, whether the data importer is a service provider acting as data processor or a business partner acting as an autonomous data controller. This translates, from an accountability perspective, into the ability to demonstrate the reasoning behind the choice and defend it, if need be.

Note that the importers may also be indirectly engaged, i.e., when a data processor of the company relies on sub-processors established outside of the EU to provide its services. This means that the exporter is required to perform accurate checks of the sub-processors prior to providing its green-light to their engagement and to periodically verify (or have its processors verify) their activities and their compliance with the data protection requirements. Indeed, it is good practice, during the performance of the agreement with a data importer, to perform periodical checks on the importer, regardless of whether the relationship is a long-term or a rather new one. A system of automatic audits and random verifications can represent a useful tool for the exporter that wants to be sure to have control over its data transfer - to this end, a number of means can be used, from questionnaires to interviews, investigations on publicly available sources or certifications.

Furthermore, from a practical perspective, for those jurisdictions that are identified as critical or vital to its business activities, the exporter should make sure to perform a detailed analysis of the same, engage in legal advice if needed and make sure to have respected voices in support of its most critical decisions regarding data transfers.

Indeed, even though the clauses of the SCC impose on the importer the obligation to inform the exporter when the former believes it is no longer able to comply with the provisions of the SCC, the diligent exporter should not take the importer's word for it. There are cases, in fact, in which the exporter is almost required to act proactively and independently -- think of those circumstances when word is out that a new bill, under discussion, may introduce government control over or indiscriminate access to the data the importer holds. Whenever there are indications that the ability of the importer to honour its contractual obligations under the SCC is impacted, the exporter should make sure to seek legal advice from local counsel and anticipate the effects of the changes in the legal scenario, or at least prepare for them. More

generally, the prudent exporter will want to document that and how it has assessed the risk of a breach of the SCC obligations by its data importer as that will enable it to defend its position if ever challenged.

In addition, from a compliance point of view, there may be circumstances in which the exporter is required or suggested to perform a data protection impact assessment, so as to analyse the options available to him and be certain to consider their consequences over the rights and freedoms of the people involved. This would guarantee compliance with the accountability principle and leave the exporter best equipped to face the possible consequences of its decisions in case of claims or investigations.

In conclusion, data transfer, as well as any other aspect of data processing, is to be read in conjunction with and according to the principles of the GDPR, and notably with the principle of accountability. And although the burden on the controller/exporter is higher than before, relying on expert advice and thorough preparation represent a good recipe for success.