Schrems II case - the data importer perspective

Francesca Gaudino and Valeria Benedetti del Rio

Following our previous analysis of the consequences of the opinion of the advocate general Hendrik Saugmandsgaard Øe (a.g.) in the Schrems II case, from the data exporter perspective (available here), we now focus on the implications of the same with respect to the position of the data importer.

Indeed, in the following paragraphs, we will turn our attention to the content of the Controller to Processor Standard Contractual Clauses (SCC) and, in particular, to some of the obligations imposed on the data importer, notably, Clauses 4(d); 5(a); 5(b) and 5(d). We will consider these obligations in light of the a.g.'s opinion in order to explain their 'new' meaning and scope.

Appropriate Security Measures - Clause 4(d)

Although the content of the obligation under Clause 4(d) is directed to the data exporter, its text has an impact on the activities of the data importer as well. Indeed, the exporter is required to agree and warrant that "after assessment of the requirements of the applicable data protection law, the security measures [put in place by the data importer] are appropriate" to protect the data that the latter is processing on its behalf. The clause, therefore, implies that (following a periodical request from the data exporter) the data importer regularly supplies a report indicating all the security measures that the importer has in place, in order for the exporter to be able to assess whether said measures are appropriate to its purposes. In light of the principle of transparent and accurate processing, in fact, the analysis on the importer/processor shall be performed or at least reviewed on a regular basis.

Moreover, the data importer has a number of additional information requirements towards the data exporter, including:

Non-Compliance - Clause 5(a)

The main obligation of the importer is enshrined under Clause 5(a) that requires the same to agree and warrant that it will process personal data only on behalf of the exporter and in compliance with its instructions and the Clauses. Clause 5(a), quite frankly also considers the possibility that the importer may not be able to comply with its obligations: indeed if "for whatever reasons" the importer cannot honour its obligations, Clause 5(a) requires it to inform promptly the data exporter. It is indeed not an easy task for the importer. In line with the principle of good faith in contractual relationship, the importer shall make the exporter aware of any and all circumstances that may hinder the protection of personal data in the course of the processing activities it performs. Clause 5(a) is a prerequisite for the accountability of the exporter/controller, which, following the receipt of said information, can

decide the consequent actions. The range of said actions is the widest possible, up to the termination of the contract.

Changes in Legislation - Clause 5(b)

This clause is structurally similar to the one just mentioned and imposes an obligation on the data importer to notify the data exporter when a change in the applicable legislation is likely to negatively affect the capacity of the importer to comply with its obligations. Again, the consequences of said notification are for the exporter to define, being the data controller the one in charge of deciding purposes and modalities of data processing (including data transfers). What is relevant in all those circumstances is that the exporter is made aware of such changes, so that it can act accordingly and in a timely fashion.

Requests for Disclosure - Clause 5(d)

Another similar obligation is the one included in Clause 5(d), according to which the importer has a duty to inform the exporter, without undue delay, on all those circumstances where it is the addressee of specific requests or actions - i.e. a legally binding request for disclosure by a law enforcement authority; any accidental or unauthorised access; a data subject request. The idea behind this Clause is for the exporter to be in control of what happens on the importer side; indeed, it is relevant to remember that the importer is a data processor and the exporter/controller is responsible before data subjects for its compliance with the data protection laws.

Finally …

In conclusion, the a.g. suggests increasing the exporter's scrutiny on the importers data processing activities. It is indeed the importer's obligation to facilitate the data exporter in performing its analysis of the importer's factual compliance. Following this line of thoughts, the importer will be expected to provide all necessary information to support the exporter in this effort.

It is of paramount importance, for the data importer, to make sure to set up an assessment and reporting process, to enable a timely identification of all non-compliance situations, and to become aware of circumstances relating not only to the data processing itself, but also to external factors. For example, the disclosure of requests from national security agencies, or changes in national legal regime. In parallel, the data importer should also make sure to open and maintain proper communication channels with its exporters and effectively comply with its duties under the SCC.