VAN BAEL & BELLIS

CLIENT ALERT MEMORANDUM

14 January 2020

Advocate General Confirms Validity of EU Standard Contractual Clauses

On 19 December 2019, Advocate General Henrik Saugmandsgaard Øe delivered his opinion in the *Facebook Ireland and Schrems* case (C-311/18, ***Schrems II case***). In the Advocate General's view, the validity of Commission Decision 2010/87/EU cannot be called into question, as the mechanism of standard contractual clauses (***SCCs***) laid down in this decision ensures a sufficient level of protection of the data transferred to processors established in third countries. At the same time, the Advocate General indicated that controllers and supervisory authorities have an obligation to suspend transfers on the basis of SCCs if the obligations contained in the clauses cannot be guaranteed under the laws of the data importer.

International transfers under GDPR

The General Data Protection Regulation (***GDPR***) permits personal data transfers to a third country subject to certain conditions. First and foremost, the transfer is allowed to countries considered by the European Commission to provide for an adequate level of personal data protection by way of a so-called "adequacy decision". If no such decision is taken by the European Commission, data controllers (i.e., the party determining the purpose and means of the processing) should consider implementing other appropriate safeguards to transfer data from the EU to a third country.

In most cases, these appropriate safeguards take the form of a contractual arrangement between the exporter and the importer containing standard clauses set out by the European Commission and aimed at ensuring adequate protection of personal data transferred outside the EU. The *Schrems II* case concerns the validity of the SCCs adopted by the European Commission in Decision 2010/87/EU. The case questions the adequacy of the level of protection related to the SCCs mechanism.

History of the case

In 2015, the Court of Justice of the European Union (***CJEU***) delivered its judgment in the *Schrems I* case (C-362/14), which concerned the validity of the Commission adequacy decision on the US data protection system (also known as the "*safe harbour scheme*").[1] The

[1] Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (OJ 2000 L 215, p. 7).

case originated from a complaint filed in 2013 by Mr. Schrems with the Irish Data Protection Commission (***IDPC***) challenging the transfer by Facebook Ireland of its users' data to the parent company, Facebook Inc., located in the United States. In view of the then recent revelations by Edward Snowden on the methods used by US national security agencies, Mr. Schrems argued that US legislation did not offer adequate protection against surveillance of the data transferred to that country and asked the IDPC to suspend the data transfer to the US. Following the *Schrems I* judgment in which the CJEU declared the safe harbour scheme invalid, Facebook continued its transfers of personal data, now relying mainly on SCCs. Therefore, the proceedings initiated by Mr. Schrems continued before the Irish High Court to determine the validity of the SCCs adopted by Facebook Ireland. The Irish High Court subsequently referred the case to the CJEU asking, *inter alia*, whether the US ensures adequate protection of EU citizens' personal data and whether the EU SCCs mechanism offers sufficient safeguards for the protection of EU citizens' freedoms and fundamental rights.

The Advocate General's Opinion

The Advocate General notes that it is not necessary to assess whether the country to which the data are transferred offers an adequate level of protection in order to appraise the level of protection afforded by the SCCs. Indeed, the SCCs adopted by the Commission provide a general mechanism applicable to transfers irrespective of the third country of destination. In this regard, the fact that SCCs are not binding upon third countries' authorities does not imply that they do not offer sufficient safeguards. The validity of the contested decision depends on the existence of mechanisms ensuring that transfers are suspended or prohibited where the SCCs are breached or impossible to honour. According to the Advocate General, that is the case "*in so far as there is an obligation – placed on the data controllers and, where the latter fail to act, on the supervisory authorities – to suspend or prohibit a transfer when, because of a conflict between the obligations arising under the standard clauses and those imposed by the law of the third country of destination, those clauses cannot be complied with*". The Advocate General points out that the obligations under the SCC include an obligation for the data importer to process the personal data that it receives only on behalf of the data exporter and in compliance with its instructions and the SCC.

In other words, the Advocate General's opinion suggests that companies and data protection authorities should follow a case-by-case analysis in assessing the consistency of SCCs with Commission Decision 2010/87/EU. By his opinion, the Advocate General clearly seeks to preserve the data transfer mechanism laid down by the GDPR and relied on by most organisations. In that regard, in the Advocate General's view, the SCCs remain a valid mechanism for the transfer of personal data from the EU to third countries.

If the opinion is confirmed, companies and businesses can continue to rely on SCCs, but must closely monitor possible breaches and suspend transfers if it becomes clear that the data importer can no longer guarantee the compliance with its obligations.

No need to assess Privacy Shield

The Advocate General holds that the main issue in these proceedings is the validity of Commission Decision 2010/87, thus he is not required to assess the validity of the new EU-US *"Privacy Shield"* framework, adopted following the *Schrems I* judgment and implemented at EU level by Commission Decision 2016/1250/EU.[2] Nevertheless, the Advocate General expresses some concerns about the Privacy Shield framework, stating that it does not provide for an effective remedy by which individuals may challenge the use of their personal data by US intelligence services, or obtain access to, or rectification or deletion of that data.

It must be noted that the Privacy Shield is under scrutiny in another case, pending before the EU's General Court, where the appellants challenge, *inter alia*, the Commission finding that the EU-US Privacy Shield assures protection equivalent to that guaranteed within the European Union.[3]

It remains to be seen whether the CJEU's judgment (to be issued within the following months) will follow the AG's opinion or deviate from it. Whatever the outcome will be, data controllers are advised to map out their international data flows, including whether these transfers rely on SCCs or have another justification under the GDPR.

---

2 The framework has replaced the previous and invalid safe harbour scheme and is enshrined in Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to [Directive 95/46] on the adequacy of the protection provided by the EU-U.S. Privacy Shield (OJ 2016, L 207, p. 1).

3 Case T-738/16, action brought on 25 October 2016 — *La Quadrature du Net and Others v Commission*.

VAN BAEL & BELLIS

CLIENT ALERT MEMORANDUM

Authors

Thibaut D'hulst	tdhulst@vbb.com
Justine Van den Bon	jvandenbon@vbb.com

Get in touch

If you have any questions concerning this memorandum, please call us at	+32 2 647 73 50
or send us an e-mail at	brussels@vbb.com