Schrems II: What is (or should be) on your to-do list for international data transfers?

Mr. Peter Craddock
Local Partner
peter.craddock@nautadutilh.com

Today, on 16 July 2020, the Court of Justice of the European Union (CJEU) handed down its Schrems II judgment invalidating the European Commission's adequacy decision with respect to the EU-US Privacy Shield Framework, a little less than five years after doing the same with respect to the US Safe Harbour (Privacy Shield's predecessor). At the same time, the CJEU confirmed the validity of the controller-to-processor "standard contractual clauses" (SCCs) decision by the European Commission (the reasoning appears to be also relevant for the "controller-to-controller" SCCs). This judgment is relevant for any organisation transferring personal data to organisations outside of the EU.

Pursuant to the General Data Protection Regulation (GDPR), personal data may in principle not be transferred (e.g. also giving access) to recipients outside of the EU, unless (i) the European Commission has determined through an 'adequacy decision' that the destination (non-EU) country offers an adequate level of data protection (Article 45 GDPR), which currently applies to the countries listed here,or (ii) appropriate safeguards are put in place (Article 46 GDPR), such as the SCCs (the most widely used data transfer tool).

Many other newsletters and posts over the coming days will describe the judgment in detail. For this reason, we have chosen to focus on the key practical implications for organisations.

What then is the practical outcome of this "Schrems II" judgment?

1. SCCs: no silver bullet, verification of compliance still required

If you (wish to) rely on the SCCs, both the EU controller and the recipient need to verify whether the destination country's laws will allow compliance with the GDPR, the SCCs themselves and also the EU Charter on Fundamental Rights.

If any circumstances arise that prevent compliance:

- the recipient must notify this to the EU controller; and
- the EU controller must suspend the transfer / terminate the contract. If the EU controller decides not to do this, it must forward the recipient's notification to the supervisory authority.

If the laws of the destination country are likely to prevent compliance with the SCCs themselves or the other rules mentioned above, the CJEU suggests it may be necessary to supplement the guarantees contained in the SCCs with other clauses or additional safeguards. It is useful here to work in a framework agreement, so that the content of the SCCs is left intact wherever possible (for ease of verification of compliance) and to ensure that any other contractual provisions provide for a higher level of protection than the SCCs.

One should always bear in mind that, as the CJEU itself states, "breach of those [SCCs] will result in a right for the person concerned to receive compensation for the damage suffered" (para 143 of the judgment).

A particular point of concern will relate to transfers to the United States of America. Based on the CJEU's considerations regarding Privacy Shield (see below), the choice to transfer personal data to a recipient in the USA would appear to come at a risk if there is any likelihood of surveillance of or through the recipient. It will be important for organisations to monitor how supervisory authorities take position over the next few weeks, to determine how to best manage this particular risk.

SCCs remain an incomplete set of tools, as there are types of SCCs currently only with respect to personal data transfers from EU controllers to non-EU controllers (i.e. controller-to-controller) or non-EU processors (i.e. controller-to-processor). For other types of transfers, such as processor-to-subprocessor, there are no official SCCs available. In addition, the (official) SCCs have not yet been updated in view of the GDPR. In its 2020 GDPR evaluation report, the European Commission mentioned that it is currently in the process of modernising the SCCs, covering all relevant transfer scenarios and better reflecting modern business practices, and expanding its 'transfer toolbox'.

All in all, the incomplete and apparently insufficient nature of SCCs in the CJEU's view raises questions in terms of liability and risk management, and may make organisations more hesitant to transfer data under the SCCs.

2. Privacy Shield: alternative required

Before all else, it is important to check whether you rely on Privacy Shield for certain international data transfers. To do so, examine your records of processing activities and data protection notices. We also recommend checking the Privacy Shield website, which lists the companies that

self-certified under the EU-US Privacy Shield framework.

If you transfer personal data from the EU to such companies and rely upon Privacy Shield in relation to the data transfer, check first whether your contract with them provides for the application of SCCs in the event of invalidation of Privacy Shield. If not, you will need to put other “appropriate safeguards” in place, such as SCCs.

First, as far as SCCs are concerned, do bear in mind again that they might not be a miracle solution for the reasons set out above (specifically in relation to the USA, but also due to the limited types of transfers covered).

Next, alternative appropriate safeguards such as ad hoc contractual clauses or binding corporate rules (BCRs) often require approval of the supervisory authority, which can be a lengthy and costly process.

Finally, Article 49 GDPR sets out conditions under which international data transfers may take place in the absence of an adequacy decision or appropriate safeguards, but these conditions should be reserved for exceptional circumstances and not be systematically relied upon.

In other words, action will be required, but the process of switching to another mechanism may prove complex.

Closing comments

The Schrems II judgment is a call to review international data transfer mechanisms used by your organisation. Your to-do list should include (i) checking the basis for all transfers, (ii) taking follow-up actions to ensure compliance and (iii) adapting related internal and external documentation (privacy statements, internal data protection policies and records of processing activities). And if this sounds daunting, the NautaDutilh data protection team is there to lend a hand.