KNOW-HOW

Gleiss Lutz

08.06.2021

## DATA PROTECTION

# NEW EU STANDARD CONTRACTUAL CLAUSES FOR THE TRANSFER OF DATA TO THIRD COUNTRIES – WHAT COMPANIES NOW NEED TO DO

**On 4 June 2021 the European Commission adopted new rules for the transfer of personal data to recipients in countries outside the EU. The so-called standard contractual clauses are intended as a tool to allow companies to exchange personal data beyond EU borders without breaching data protection law. The standard contractual clauses impose special obligations on the contracting parties designed to ensure that the data subjects retain control over "their" data abroad as well. Existing data protection contracts based on the old standard contractual clauses must now be adjusted to bring them in line with the new law. Companies do not have much time to make the necessary adjustments.**

### 1. Background

Many thousands of companies in the EU use the European Commission's standard contractual clauses as a basis for exchanging data with group companies, business partners and service providers in third countries. The clauses normally in use to date go back to 2001, 2004 and 2010, i.e. long before the General Data Protection Regulation (GDPR) came into force in May 2018. Over time, the standard contractual clauses have begun to show more and more signs of "old age": references to the now repealed Data Protection Directive, a lack of clarity as regards the interplay with the requirements for agreements for commissioned data processing and for joint controllership, and the question of their applicability to European processors processing data on behalf of controllers in third countries.

The decision handed down by the European Court of Justice (ECJ) on 16 July 2020 in *Schrems II* (C-311/18) finally brought home the need for the clauses to be updated. While the ECJ still found the standard contractual clauses to be basically suitable as a basis for data transfers to "unsafe" third countries, the grounds it gave for its decision revealed the weaknesses of the standard contractual clauses. Specifically, according to the ECJ, the clauses still in force do not contain any provisions that adequately protect the personal data of EU data subjects from access by foreign security authorities that is disproportionate by European standards. The grounds for the decision said that additional measures were therefore required if it was to be possible to lawfully transfer data. What measures it had in mind the ECJ omitted to say, leaving companies and supervisory authorities at a loss for how to proceed.

These new standard contractual clauses represent the European Commission's attempt to remedy the shortcomings of the old clauses and, as far as possible, bring about legal certainty.

### 2. The new standard contractual clauses

The new standard contractual clauses only partly fulfil the hope of a return to legal certainty for global data transfers, however:

- The way the standard contractual clauses work remains the same. The data protection obligations on EU companies set out in the GDPR are being transformed into contractual provisions, making them binding on the "data importer" in third countries. In particular, the data importer must cooperate in making data processing transparent and guarantee the data subjects' key data protection rights. The details of the data transfer and its purposes, as well as the technical and organisational data protection measures to be implemented by the data importer, are to be described in an annex to the clauses. Generally speaking, the

- requirements as to the level of detail are stricter than under the law as it stood before.

- Like the previous clauses, in large part the new ones also have the effect of according rights to third party beneficiaries, i.e. persons who are the subject of the data being processed can use the clauses as a basis to assert their rights against the contracting parties and, where applicable, enforce them in EU courts.

- The standard contractual clauses take into account the *Schrems II* ruling and the opinions published by the supervisory authorities on that ruling. They explicitly oblige users to check whether, given the legal situation in the third country, the data importer is in a position to comply with the contractual provisions, in particular to protect against disproportionate access by public authorities. The parties must document the results of these checks and any technical and organisational measures taken to protect the data (e.g. encryption) and submit them on request to the supervisory authority responsible for the EU company exporting the data. The data importer is also obliged to notify the data exporter if it considers itself unable (or no longer able) to protect the data from access by public authorities. Upon receipt of such notification, the exporter must stop transferring the data unless the supervisory authority allows it to continue.

- The data importer must also take all measures available by law to defend itself against requests by public authorities for information and inform the data exporter and data subjects thereof.

- The new standard contractual clauses are modular in structure. For each of the following situations, they take a different format:
  (i) Transfer from a controller in the EU to a processor in a third country
  (ii) Transfer from a controller in the EU to a controller in a third country
  (iii) Transfer from a processor in the EU to a controller in a third country
  (iv) Transfer from a processor in the EU to a sub-processor in a third country.

  Standard contractual clauses are now available for the first time for the latter two variants.

- One new pragmatic and likely useful feature is the so-called “docking clauses”, which will enable additional parties to accede to the standard contractual clauses.

- Another new feature is that the standard contractual clauses provide for liability on the part of the parties for breaches of duty not only vis-à-vis the data subjects, but also in relation to each other. Whether the parties can exclude or at least limit this liability in terms of their relationship *inter se*, e.g. in order to adapt it to the liability regime otherwise applicable between them, is unclear.

### 3. Outlook and need for action

The EU Commission's new standard contractual clauses bring up to date what is in practice by far the most important instrument for enabling data to be exchanged with third countries. They eliminate many ambiguities, and the modular format and the simplified possibility for additional parties to accede to the clauses create valuable flexibility.

However, the standard contractual clauses cannot fully alleviate the high level of legal uncertainty associated with the transfer of personal data to third countries since the ECJ’s ruling in *Schrems II*. Where, in a third country such as the USA, China or Russia, there is a – more than just theoretical – risk that security authorities may access the transferred data in a disproportionate manner, and if this risk cannot be eliminated by additional measures such as data encryption, then the new standard contractual clauses cannot legitimize the data transfer either. Companies that are reliant on the exchange of data with, for example, US group companies or (cloud) service providers therefore still face a dilemma that is difficult to resolve.

That apart, there is a need for action: While companies may still continue to conclude data transfer contracts on the basis of the old clauses for a transitional period of three months from publication of the new standard contractual clauses in the EU Official Journal, all contracts must be brought in line with the new standard contractual clauses within 18 months of publication of the new clauses at the latest. Especially for companies that maintain extensive business relations with non-EU countries, this represents an enormous challenge.

EXPERTISE

Data Protection

Digital Economy

EXPERTS

**Dr. Christian Hamann**

**Dr. Manuel Klar**

**Simon Clemens Wegmann**