WILMERHALE

Updated EU Model Clauses for International Data Transfers Enter into Force

2010-06-07

On May 15, an updated version of the European Union's standard contractual clauses for the transfer of personal data to data processors located in countries outside the EU entered into force. Companies need to be aware of the changes and the circumstances under which use of the new version is required. Given the heightened current awareness of the need for improved compliance with privacy requirements, they should also review their existing arrangements for ensuring compliance with data protection law in the context of international data transfers in general.

General Background. The EU's data protection laws restrict the transfer of personal data to countries outside the European Economic Area (EEA) (EU plus Iceland, Norway and Liechtenstein). Such transfers are permitted only if the recipient is located in a country with an "adequate level of data protection". The number of countries that have been found to fulfill this requirement is limited; notably, it does not include the United States (with the exception of US companies that have self-certified under the US-EU "Safe Harbor Agreement") or popular outsourcing destinations such as India and China.

Other options are available for data transfers to countries that do not

generally provide "adequate" protection. One of them, under Article 26 of the EU Data Protection Directive 95/46, is to implement contractual agreements between the parties exchanging personal data to ensure that the privacy rights of individuals are respected. Article 26 of the European Union's Data Protection Directive 95/46/EC also lists several derogations that would permit transfer to a country without adequate data protection laws. Companies transferring personal data out of the European Union need to review the specific advantages and disadvantages of each solution to identify the most appropriate means of ensuring compliance.

Standard Contractual Clauses. Under the Directive, the European Commission may decide that certain standard contractual clauses offer sufficient safeguards, with such a decision being binding on the EU member countries.

In 2001, the European Commission published two sets of standard contractual clauses – one for a so-called "controller to controller" transfer, and one for a so-called "controller to processor" transfer. A "controller" as defined in the Data Protection Directive is an entity that determines the purposes and means of the processing of personal data. A "processor," on the other hand, acts only on behalf of and at the direction of a controller as a service provider. (The so-called "Article 29 Working Party", which consists of representatives of the data protection authorities of the EU member countries, has recently issued a working paper that discusses these definitions in detail.)

Transfers of personal data in the course of outsourcing relationships will frequently be considered transfers to a processor, while a transfer to a recipient that is entitled to decide independently why and how to process the data is considered to be a transfer to a controller. Using pre-approved

standard contractual clauses for such data transfers can be a speedy and certain way to comply with European data protection requirements. For that reason, it has become a preferred option for many data exporters.

In practice, the 2001 "controller to controller" clauses were frequently considered to be too far-reaching and therefore not a viable option. The European Commission reacted in 2004 by approving another set of standard contractual clauses for these transfers that had been drafted by the International Chamber of Commerce, among others. Both of these sets of clauses remain valid and may be used by interested parties.

With respect to "controller to processor" transfers, the Commission approved one set of clauses in 2001. Recently, the European Commission updated the 2001 clauses because of the continuing growth of international transfers of personal data, and an increased interest in using sub-processors. The new version of the clauses entered into force on May 15 and replaces the old version.

Main Changes. The most relevant change of the new version of the clauses is express language regarding sub-processors. A processor (the data importer) planning to subcontract any of its processing obligations performed on behalf of the controller (the data exporter) may only do so with the prior written consent of the controller. Subcontracting requires a written agreement, imposing the same obligations on the subcontractor as are imposed on the processor. The controller is required to keep a list of all sub-processing agreements and make it available to its data protection supervisory authorities upon request. The supervisory authorities may also audit any sub-processors.

Companies relying on the standard clauses for transfers of personal data to

data processors outside the EU are required to use the new version of the clauses for transfers of personal data starting on or after May 15. Any existing contract under the old version needs to be changed if the transfers and data processing operations that are the subject of such contract change or if there are changes to subcontractors.

Suggested Actions. We suggest that companies use the recent entry into force of the new clauses as a trigger to review compliance with European data protection obligations, especially regarding the transfer of personal data from the EEA to third countries. The recent changes may make the "controller to processor" clauses more attractive, but other options such as the Safe Harbor regime may also be appropriate. Companies that have used the standard clauses in the past need to make sure that they update to the new version when required. The greater attention that compliance with privacy and data protection requirements has received with the media recently highlights the importance of attention to this issue.

Compliance with applicable data protection law also includes making the required filings with the competent national supervisory authorities regarding general processing activities and data exports. Since these requirements vary among the different EEA member states, a country-by-country analysis is generally required, followed by an implementation plan.

Companies using the standard clauses also need to bear in mind that the clauses need to be used without any changes. Changes will trigger a legal requirement to seek approval with the local supervisory authorities, which may take a significant amount of time.

About WilmerHale. WilmerHale has a premier EU Regulatory Group that deals with the full range of regulatory and government affairs issues facing

companies doing business in Europe. Our data protection, data security and privacy lawyers have been advising on data protection issues since the earliest legislative proposals for an overarching EU-wide privacy regime were made. We help clients navigate the thorny issues often raised by the interplay of commercial objectives, compliance needs and data protection and data security laws. Our interdisciplinary team is comprised of lawyers with a broad mix of regulatory, counseling, litigation and transactional expertise. Our lawyers work on privacy, data protection and data security issues with clients across all sectors of the economy. We have particular expertise in cross-border data transfers and international data protection/privacy laws, compliance, data protection/privacy policies and data security.

Additional information about WilmerHale's privacy, data protection and data security practice is available here. More information about WilmerHale's European Regulatory Group can be found here.

Authors

Dr. Martin Braun

PARTNER

martin.braun@wilmerhale.com

+49 69 27 10 78 207

Christian Duvernoy

RETIRED PARTNER

christian.duvernoy@wilmerhale.com

+32 2 285 49 06