Special Report

New Standard Contractual Clauses for Data Transfers Out of EU Raise Concerns

By Mauricio F Paez, Gwendolynne M Chen and Abhishek Bapna, Jones Day, New York

In response to the increasing globalization, outsourcing and subcontracting of data processing activity, the European Commission adopted a new set of Standard Contractual Clauses ("SCCs")[1] governing the transfer of personal data to countries that are not recognized as providing adequate protection measures for such personal data processing,[2] which includes any information relating to an identified or identifiable natural person, outside of the European Union ("EU") or the European Economic Area ("EEA").[3] The new SCCs, effective as of May 15, 2010,[4] will replace the previous SCCs adopted under Commission Decision 2002/16/EC, which governed transfers of personal data from data controllers to data processors.[5] Beyond data controllers and data processors, the new SCCs also cover the transfer of personal data to one or more "subprocessors" outside of the EU or the EEA who receive and process personal data on behalf of data controllers and data processors. Given the broader scope of the new SCCs relative to the old SCCs, the new SCCs could affect nearly all companies that receive, use, or have access to personal data from EU or EEA entities.[6]

Legal Framework

SCCs are only one of several mechanisms for lawfully transferring personal data out of the EU or the EEA that would satisfy European laws, which otherwise prohibit the transfer of personal data to such countries. The EU's data protection Directive 95/46/EC ("Data Protection Directive") permits the transfer of personal data from the EU to a country outside of the EU ("third country") only if the third country provides "adequate protection" for such data, unless one of a limited number of specific exemptions under Article 26 of the Data Protection Directive applies.[7] For example, EU Member States can transfer personal data to a third country that does not provide an adequate level of protection where:

- The data subject provides informed consent for such transfer;[8]
- The data protection authority ("DPA") of the Member State determines that there are "adequate safeguards", such as appropriate SCCs or Binding Corporate Rules ("BCRs"), for protecting the personal data;[9]
- The data transfer agreement uses one of the three sets of SCCs approved by the European Commission;[10] or
- With respect to companies located in the United States, such entity self-certifies annually to the requirements of the EU and US Safe Harbor framework.[11]

Despite the various options available for complying with the Data Protection Directive however, many of the mechanisms listed above have either limited or no utility in many circumstances. For example, most financial services companies are not eligible to participate in the Safe Harbor programme[12] and, while SCCs and BCRs appear to be "off the shelf" solutions to international transfers, there is currently no equivalent fast-track method for obtaining DPA approval,[13] and DPAs can subsequently audit companies and find the enforcement of SCCs or BCRs to be inadequate. Therefore, the new SCCs represent the European Commission's latest compromise in balancing the privacy interests of individuals in an environment of rising offshore outsourcing activity with the commercial interests of companies and the EU in streamlining (or at least, not further complicating) the process of international data transfers.

Significant Changes

The new SCCs introduce, for the first time under the EU Data Protection Directive, the concept of a subprocessor, and delineate the rights and responsibilities of the data exporters, data importers, and the subprocessors, vis-à-vis each other.

Data Exporters

Data exporters are entities established in the EU or EEA that control and transfer personal data to data importers.[14] Under the new SCCs, data exporters must:

- Warrant that both data importers and subprocessor(s)[15] will provide an adequate level of data protection;[16]
- Keep a list of subprocessing agreements containing SCCs, including those executed by their data importer(s), and make this list available to any applicable DPA;[17] and
- Make available to data subjects a copy of the new SCCs and a copy of any subprocessing agreement upon request.[18]

The new SCCs provide that a data exporter may be liable to a data subject for any damage the data subject suffers as a result of any breach by itself, the data importer, or any subprocessors of their respective obligations.[19] Moreover, a data subject may bring a claim against data

  WCRR ISSN 1750-1784

importers or subprocessors only where the data exporter has ceased to exist.[20] Thus, data exporters are primarily responsible for any breach in the chain of data processing activity.

Data Importers

Data importers are data processors established in third countries that are engaged by data exporters for processing personal data on behalf of data exporters.[21] Because data importers often transfer personal data received from data exporters to subprocessors in the same or another third country for processing, storage, or technical support functions, data importers that use the new SCCs must:

- Inform data exporters of subprocessing activities and obtain the data exporter's prior written consent for each subcontract;[22]
- Subcontract their obligation only by way of written agreement with subprocessors that impose the same privacy and data protection obligations on subprocessors that the data exporter imposed on them;[23]
- Include a third-party beneficiary clause in any subprocessing agreement that allows the data subject to bring a claim for compensation against the subprocessor in a situation where both the data exporter and the data importer have disappeared or ceased to exist;[24]
- Send a copy of any subprocessing agreement they conclude under the SCCs to the data exporter;[25] and
- Offer data subjects a choice between mediation and litigation for resolving disputes.[26]

Under the new SCCs, the data importer may be liable to the data exporter for any breach by itself or any of its subprocessors for failure to perform their processing obligations or to provide the adequate level of data protection under the data importer's contract with the data exporter.[27] The data importer may also be liable for any damage the data subject suffers as a result of any breach by the data importer or its subprocessors of any of their respective obligations,[28] to the extent that the data subject cannot obtain adequate redress from the data exporter.

Subprocessors

Subprocessors[29] are entities established in third countries that are engaged by data importers or other subprocessors to process personal data on their behalf. Under the new SCCs, subprocessors must provide at least the same level of privacy and data protection that the data exporter provides,[30] which means that the laws of the data exporter's state may apply to the subprocessor's activities. In addition, subprocessors may be liable to data subjects for damage claims where the data subject is unable to bring a claim against the data exporter, the data importer, or a successor entity that has assumed their obligations under the SCCs.[31] In such a claim for damages, however, subprocessors are only liable for their own activities and would not be liable for any harm caused by either the data exporter or the data importer.[32]

Conclusion

The European Commission adopted the new SCCs to ensure that all entities in the data processing chain are subject to the same obligations of privacy and data protection. Under the new SCCs, data exporters and data importers must fulfill certain obligations that go above and beyond those required for data controllers and data processors under the original SCCs. The new SCCs also provide data exporters, data importers, and subprocessors certain rights and obligations with respect to data subjects and to each other.

Any company using the old SCCs may want to re-evaluate whether the old SCC regime is still its best option for transferring data out of the EU or the EEA. Any company that will be applying the new SCCs should review and negotiate their agreements, arrangements, and relationships involving personal data originating from the EU or the EEA with the new SCCs in mind. Specifically, these companies should:

- Perform thorough due diligence investigations of potential parties to agreements that involve the processing of personal data originating from the EU or the EEA to determine whether such parties are technologically and/or organizationally capable of satisfying the necessary privacy and data protections obligations under the new SCCs; and
- Negotiate indemnification clauses in new or existing data processing agreements that involve personal data originating from the EU or the EEA.

Companies should also be careful not to rely on an overly literal reading of the new SCCs. Although the textual definitions of "data exporter" and "data importer" cover only data transfers from a data controller within the EU to a data processor outside the EU, i.e. not transfers from a data processor in the EU to a subprocessor outside the EU, the distinction between a data controller and a data processor is not always clear in practice. While data controllers typically make decisions about what data to collect and how to use such data, and data processors typically manipulate data according to a data controller's instructions, a company can perform any and all of these duties, and thus may act as a data exporter, data importer, and/or subprocessor under different circumstances with respect to other companies. Moreover, DPAs may audit the chain of processing relationships at any time and determine appropriate roles and actions for a company that may be inconsistent with those that the company previously considered to be appropriate.

Lastly, any company wishing to execute or amend a valid agreement under the old SCC for processors must apply the new SCCs for processors. All SCCs for processors executed before May 15, 2010 will continue to be enforceable under the old SCCs.

[1] Commission Decision 2010/87/EU, 2010 OJ (L 39) 5-6, 11 (EU).

[2] "Personal data" means any information relating to a natural person

(a "data subject") who is identified or identifiable, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural, or social identity. Directive 95/46/EC, 1995 OJ (L 281) 31, 38 (EC).

[3] As at July 2010, the EEA includes EU member states plus Iceland, Lichtenstein and Norway.

[4] New SCCs at 5-6, 11.

[5] Commission Decision 2002/16/EC, 2002 OJ (L 6) 52, 59 (EC) (hereinafter "old SCCs").

[6] Companies that have used other legal mechanisms to enable the transfer of personal data for processing outside the EU or EEA do not need to adopt the new SCCs unless there will be new personal data transfers or the old SCCs have either been terminated or are no longer legally sufficient.

[7] Data Protection Directive Articles 25, 26. The primary purpose of the Data Protection Directive is to protect the privacy rights of individuals with respect to the processing of their personal data. Many countries have similar data protection regimes and some, such as India, Malaysia and Thailand, are considering similar models. See, e.g. Hong Kong Personal Data (Privacy) Ordinance, 33 § 2(a), 3 (1995), Article 8 of the Russian Federal Law No. 85-FZ of July 4, 1996, on Participation in the International Information Exchange; "Personal Data Protection Bill Passed By Dewan Rakyat", Bernama (April 5, 2010), available at http://www.bernama.com/bernama/v5/newsgeneral.php?id=488203.

[8] Data Protection Directive § 26(1)(a).

[9] Data Protection Directive § 26(2). BCRs are a set of rules adopted within a particular company or corporate group that provide legally binding protection for data processing within the company or group. BCRs can be legally binding on members of a corporate group through a variety of legal devices and may provide a legal basis for data transfers to other countries or regions. Most multinational corporations use BCRs for a variety of compliance requirements such as environmental, health and safety, money laundering and general corporate governance requirements.

[10] Data Protection Directive § 26(4). Commission Decisions 2001/497/EC and 2004/915//EC apply to transfers from data controllers to data controllers; Commission Decision 2010/87/EU (formerly, 2002/16/EC) applies to transfers from data controllers to data processors.

[11] See US Department of Commerce, Safe Harbor Home Page, www.export.gov/safeharbor/.

[12] See Status of Implementation of Directive 95/46 on the Protection of Individuals with Regard to the Processing of Personal Data, http://ec.europa.eu/justice_home/fsj/privacy/law/implementation_en.htm. The 2003 implementation report by the European Commission on the Directive showed "very patchy compliance by data controllers" with the national implementations of the Directive due, in particular, to the complex and burdensome nature of data protection law. Report from the Commission: First report on the implementation of the Data Protection Directive: Analysis and impact study on the implementation of Directive EC 95/46 in Member States, May 15, 2003, page 13.

[13] For example, a company may have to submit its BCRs for approval to a lead DPA, who then obtains approval from the DPA of each Member State from which the company intends to transfer personal data.

[14] "Data exporter" means "the controller who transfers the personal data". New SCCs § 3(c).

[15] "Subprocessor" means "any processor engaged by the data Importer or by any other Subprocessor of the data Importer who agrees to receive from the data Importer or from any other Subprocessor of the data Importer personal data exclusively intended for processing activities to be carried out on behalf of the data Exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract." New SCCs § 3(e).

[16] New SCCs at 12.

[17] New SCCs at 15.

[18] New SCCs at 12.

[19] New SCCs at 13.

[20] Ibid.

[21] "Data importer" means "the processor established in a Third Country who agrees to receive from the data Exporter personal data intended for processing on the data Exporter's behalf after the transfer in accordance with his instructions and the terms of this Decision and who is not subject to a Third Country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC." New SCCs § 3(d).

[22] New SCCs at 13.

[23] New SCCs at 14.

[24] Ibid.

[25] New SCCs at 13.

[26] New SCCs at 7. The old SCCs gave data subjects a choice among arbitration, mediation and litigation to solve disputes with data processors. The new SCCs deleted the mandatory arbitration clause because many business associations opposed this requirement. Old SCCs at 59.

[27] New SCCs at 14.

[28] New SCCs at 13–14.

[29] See Note 15.

[30] New SCCs at 14.

[31] New SCCs at 13.

[32] Ibid.

WORLD COMMUNICATIONS REGULATION REPORT is published monthly by BNA International Inc., a subsidiary of The Bureau of National Affairs, Inc., Arlington, VA 22202, U.S.A. Administrative headquarters: BNA International, 38 Threadneedle Street, London EC2R 8AY, England. Tel. +44 (0)20 7847 5801; Fax +44 (0)20 7847 5840; E-mail marketing@bnai.com.

Subscription price: U.S. and Canada U.S.$1,565/Eurozone €1,565/U.K. and rest of world £955. Additional copies of this publication are available to existing subscribers at half price when they are sent in the same envelope as a standard subscription.

 www.bnai.com *ISSN 1750-1784*