

Newsletter

July 2010

In This Issue:

European Union

[EU - European Commission updates controller to processor model clauses](#)

[EU - Data protection issues associated with WEEE Directive](#)

[Spain - Spanish Data Protection Agency issues its 2009 Annual Report](#)

[Spain - Outsourcing of certain services may fall outside of the scope of Spanish data protection regulations](#)

[UK - Final Code of Practice for assessment notices published](#)

North America

[Canada - New anti-spam and personal information protection bills proposed](#)

European Union

EU - European Commission updates controller to processor model clauses

The European Commission has updated the standard contractual model clauses for the transfer of personal data from controllers to processors based in countries outside the EEA that are not recognised as offering an adequate level of data protection. (The EEA is all EU countries plus Iceland, Liechtenstein and Norway.) The main change to the model clauses is to allow sub-processing, a practice which is extremely common particularly in IT and outsourcing industries, to take account of the business trend and practice towards more globalised processing activity.

Background

The EU Data Protection Directive 95/46 put in place controls on the transfer of personal data from the EEA to a country outside the EEA (other than one of the handful of countries which the European Commission has approved as having adequate laws to protect personal data). These controls are intended to ensure that data protection rules cannot be circumvented by transferring personal data to a place where the relevant data processing will not benefit from legal protection and where individuals will have no rights in respect of the processing. Transfers can still be made to countries which do not have equivalent data protection legislation where adequacy is ensured by other means in the particular circumstances of the transfer. The model clauses are one of several possibilities for lawfully transferring personal data outside of the EEA. Other methods include the adoption and approval of Binding Corporate Rules.

In 2001 the Commission adopted two decisions setting out standard contractual model clauses for the transfer of personal data to third countries. The first decision (2001/497/EC) applied to transfers from data controllers in the EEA to data controllers in third countries outside the EEA (amended in 2004 by a decision adopting a second set of model clauses) and the second decision (2002/16/EC) applied to transfers from data controllers in the EEA to data processors in third countries outside the EEA.

Sub-processors

The main change to the controller to processor model clauses is the inclusion of new provisions to allow non-EEA processors to sub-contract their processing activities to sub-processors, provided certain conditions are fulfilled. This modification takes account of the expansion of processing activities and new business models for the international processing of personal data.

The appointment of sub-processors is subject to a number of conditions:

The data processor must have informed the data controller of its intention to sub-contract its data processing and obtained the data controller's prior written consent.

The data processor must ensure that the sub-processing is carried out under a written contract which imposes the same obligations on the sub-processor as it does on the data processor.

The data processor must send to the data controller a copy of any sub-processing contract that it concludes.

A copy of the contract for sub-processing must also be made available, on request, to any data subjects. Commercial information can be removed from the contract before it is made available to data subjects.

The data controller is also required to keep a list of all sub-processing contracts which are concluded and notified by the data processor to it. This should be available to the data controller's data protection supervisory authority (eg in the UK this would be the Information Commissioner).

The model clauses also provide that a data subject who has suffered any loss as a result of any breach by a sub-processor of its obligations is entitled to receive compensation (in the first instance), from the data controller, but if the data controller has disappeared or become insolvent, the data subject can issue a claim against the data processor as if it were the data controller. The data processor cannot rely on a breach by a sub-processor of its obligations in order to avoid its liabilities.

Application of new clauses

The revised model clauses apply from 15 May 2010. A contract concluded between a data controller and a data processor under the old model clauses will remain in force provided that the contract remains unchanged. If, however, the parties decide to make changes to the contract or to sub-contract the processing operations under the contract, they must enter into a new contract which complies with the new standard contractual clauses.

The clauses apply where a data controller within the EEA transfers personal data to a data processor in a third country outside the EEA and that data processor enters into a sub-processing contract with a third party outside the EEA. It does not apply to the situation where a data processor in the EEA is processing for an EEA data controller and sub-contracts the processing to a sub-contractor established in a third country outside the EEA. However the recitals to the Decision do provide that Member States are free to take account of the fact that the principles and safeguards set out in the new model clauses have been used in any sub-contract.

For a copy of the decision please see [here](#). The updated clauses are attached as an Annex.

EU - Data Protection issues associated with WEEE Directive

The European Data Protection Supervisor (EDPS) has adopted an [Opinion](#) on the Proposal for an EU Directive on waste electrical and electronic equipment (WEEE) (the Proposal). According to the EDPS, the Proposal raises significant data protection issues that are not addressed in the text, namely it does not take into account risks to individuals and organisations that may arise from the disposal, reuse or recycling of WEEE. The data protection risks occur when personal data remains stored in IT and telecommunications equipment (e.g., computers, laptops) at the time of disposal or recycling.

The EDPS points out that the Directive on data protection is applicable at the disposal stage of the WEEE that contains personal data. Data controllers are therefore required to comply with their security obligations to prevent the improper disclosure or dissemination of personal data. To this end and in order not to be held liable for breach of security measures, the data controller or, where present, the data processor should have in place appropriate Data Destruction Policies for disposal of WEEE containing personal data.

In addition, the EDPS notes that some national data protection authorities have published guidelines to minimise the risks which may result from the failure to take the necessary security measures, such as the [Landesbeauftragter für Datenschutz und Informationsfreiheit Bremen, Entwicklung eines Konzeptes zur Löschung und Datenträgervernichtung durch Behörden und Unternehmen](#) and the [Garante per la protezione dei dati personali, Electrical and Electronic Waste and Data Protection](#).

In concluding, the EDPS advises that the Proposal should include the following specific provisions: (i) a statement that the Directive on WEEE applies without prejudice to the Directive on data protection; (ii) a prohibition on the sale of used electronic devices where appropriate security measures, in compliance with state-of-the-art technical standards, have not been used to delete any personal data they may contain; (iii) a requirement that, as far as possible, data-wiping technology should be integrated into the design of electrical and electronic equipment "by default" in order to allow users to delete personal data on their devices.

Spain - Spanish Data Protection Agency issues its 2009 Annual Report

On 2 June 2010, the Spanish Data Protection Agency (SDPA) published its 2009 Annual Report. Based on the Report, the most common privacy claims that were made to the SDPA involved disclosure of data on the internet, closed-circuit television (CCTV) and debtors' lists. Last year, the number of claims filed before the SDPA increased by 75%. The SDPA opened 709 investigation procedures, 621 of which ended in the imposition of sanctions - the total amount of which reached €24.8 million. The sectors with the highest number of claims were telecommunications, financial entities and CCTV. A total of 156 investigations were launched against internet service providers (including social networking sites), mainly for the disclosure of personal data without consent. The Report also includes a section on the SDPA's recommendations to public bodies, public

administrators and specific sectors. One of the SDPA's recommendations is to ask for a modification of the e-ID Card regulations so that minors are able to acknowledge their identity online and yet avoid access to services that are not suitable for them.

Spain - Outsourcing of certain services may fall outside of the scope of Spanish data protection regulations

In May 2010, the Spanish Data Protection Agency (SDPA) stated in a [Legal Opinion](#) that in cases where a data processor is only provided by the data controller with the first and last names of data subjects, their job positions as well as their business addresses, email, phone and fax numbers, such disclosure of data falls outside the scope of Spanish data protection regulations. The SDPA clarified that the exemption introduced under Royal Decree 1720/2007 applies to the processing of business contact data used in a business-to-business (B2B) relationship.

UK - Final Code of Practice for assessment notices published

The Information Commissioner's Office has recently published the final code of practice which details how the Information Commissioner will use his right to serve assessment notices for compulsory audits on certain data controllers under the new powers provided for by the Coroners and Justice Act 2009.

From 6th April 2010, the Information Commissioner has had the right to serve assessment notices on government departments, designated public authorities and other persons designated by the Secretary of State to establish whether they are complying with data protection principles. An assessment notice requires the recipient to permit the Information Commissioner access to any specified premises to inspect any documents and information and to observe the processing of any personal data that takes place on the premises.

The Information Commissioner has acknowledged that currently the scope of these powers relatively modest; as they only apply to government departments. He has however said that where the evidence supports it, he will seek to extend his powers to undertake 'compulsory' audits in both the public and private sectors.

Code of Practice:

http://www.ico.gov.uk/upload/documents/library/corporate/detailed_specialist_guides/assessment_notices_code_of_practice.pdf

Americas

Canada - New anti-spam and personal information protection bills proposed

The Government of Canada introduced two bills to protect internet users from spam and theft of personal information. The anti-spam Fighting Internet and Wireless Spam Act (Bill C-28) is a reintroduction of the Electronic Commerce Protection Act (ECPA) that was passed in the House of Commons but "died" when Parliament was prorogued in December 2009. The bill reintroduces anti-spam measures to regulate unsolicited electronic communications, including

email and text messages. Bill C-28 features a "multi-faceted" approach to enforcement involving the Canadian Radio-television and Telecommunication Commission (CRTC), the Competition Bureau of Canada and the Office of the Privacy Commissioner of Canada (OPC). If Bill C-28 is adopted, the CRTC would have the authority to impose administrative monetary penalties reaching C\$1 million for an individual and \$10 million for a business violation. Bill C-28 does not significantly change the language of the ECPA and is generally expected to pass through the legislative process quickly.

On the other hand, the proposed Safeguarding Canadians' Personal Information Act (Bill C-29) is likely to be more contentious. Bill C-29 amends the federal Personal Information Protection and Electronic Documents Act (PIPEDA), in particular by introducing mandatory breach notification rules. Currently, only the province of Alberta has mandatory breach notification requirements. Under Bill C-29, an organization that suffers a data breach that is deemed material would be required to report such breach to the OPC. In its proposed form, Bill C-29 leaves it up to the organization to decide what constitutes a "material breach of security". Materiality is assessed based on specific criteria which include the sensitivity of the information, the number of individuals affected and whether the breach is indicative of a systematic failure of security. Another notification provision under Bill C-29 requires the company to notify affected individuals if the breach poses "a real risk of significant harm to the individual", where "real risk" is defined non-exhaustively as including "bodily harm, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property". Thus, under the proposed language of Bill C-29, a breach could result in a company notifying the affected individual and not the OPC, or vice versa. As proposed, however, Bill C-29 would contain no clear penalties for the failure to notify data breaches.

In addition to the mandatory breach notification requirements, the proposed Bill C-29:

- changes the definition of "business contact information" to include work contact details, including a person's email address (business contact information is currently excluded from the scope of PIPEDA if it is collected, used or disclosed solely for the purpose of communicating with an individual in relation to his or her work);
- makes consent valid if it is reasonable to expect that the individual understands the nature, purpose and consequences of the collection, use or disclosure of personal information to which he or she is consenting;
- establishes an exception with regard to disclosure of personal information for a "prospective business transaction" without knowledge or consent of the individual, if the information is required to be used or disclosed for the purposes of the transaction;
- establishes an exception for the collection, use and disclosure of information in witness statements where it is necessary to assess, process or settle an insurance claim; and

www.bakermckenzie.com

- attempts to clarify the definition of "lawful authority", as PIPEDA allows organizations to disclose personal information to a lawful authority without a court order.

For further information please contact

EU Contact:

Ilana Saltzman

Tel: +44 (0)20 7919 1867

ilana.saltzman@bakermckenzie.com

Americas Contact:

Brian Hengesbaugh

Tel: +1 (312) 861 3077

brian.hengesbaugh@bakermckenzie.com

©2010 Baker & McKenzie. All rights reserved. Baker & McKenzie International is a Swiss Verein with member law firms around the world. In accordance with the common terminology used in professional service organizations, reference to a "partner" means a person who is a partner, or equivalent, in such a law firm. Similarly, reference to an "office" means an office of any such law firm.

This may qualify as "Attorney Advertising" requiring notice in some jurisdictions. Prior results do not guarantee a similar outcome.