Are codes of conduct the answer to the global data transfer debate?

Report by Rosa J Barcelo

BUSINESSES HAVE STRUGGLED TO DEAL with the issue of cross-border data transfers. But despite the interest in codes of conduct for exporting data outside the EU, Rosa J Barcelo questions whether they are as good as they appear to be.

For multinational corporations, the possibility of having a single set of rules governing their worldwide data processing activities is an appealing prospect. For the processing of human resources data, for example, this would mean that a company operating both in the United States and in all EU Member States could apply just one principle or rule to govern employees' access to their data, rather than having to comply with the laws of 15 different Member States, plus the Safe Harbor principles if the company's headquarters in the US has joined the scheme. The same goes for other existing legal requirements under the EU Data Protection Directive (the Directive), such as notifying employees of how their data is used, informing them of potential transfers to third parties (and seeking consent from them, if necessary), establishing data retention periods, and formulating security measures.

This report summarises the state of play on this topic. After providing some background information, this report looks at the legal grounds for using codes of conduct to transfer data under the Directive, the problems derived from applying national law and possible ways of overcoming them.

Legal Bases for Data Transfer Under EU Law

The Directive restricts transfers of personal data to countries outside the EU unless they are deemed by the European Commission to provide an "adequate level" of data protection (Article 25.1). Until now, the Commission has deemed adequate the legislation of the US (but only to companies that abide by the Safe Harbor principles), Switzerland, Hungary and Canada. Transfers to countries whose legal framework is not adequate may occur under the following circumstances:

• When the individual to whom the data refer has consented unambiguously to the transfer of their personal data "to a country where there is no adequacy finding." (Article 26.1 (a)).

• When the transfer is deemed to be "necessary for the performance of a contract" between the data subject and the data controller (Article 26.1 (c)).

• Where an agreement is concluded between an EU data controller and a non-EU third party involving a transfer to the third party, if such transfer is carried out in the interest of the data subject (Article 26.1 (e)).

Member States may also authorise a transfer if the exporter and importer, through a contractual arrangement, provide adequate safeguards to protect the data once it is exported outside the EU (Article 26.2).

The content of such a contract can be negotiated between the parties, in which case the data protection authority (DPA) of the country where the exporter is located will decide whether the agreement ensures an adequate level of protection for the transferred data. Alternatively, the exporter and importer can adopt the Standard Contractual Clauses that have been approved by the Commission, in which case approval by the DPA is not necessary.

Codes of Conduct Under Article 26(2) of the Directive

The use of codes of conduct is foreseen in Article 27 of the Directive, which empowers national DPAs to approve codes of conduct that aim to provide a proper implementation of national data protection provisions within specific sectors. However, to the author's knowledge, these codes are not used as tools to transfer data outside the EU, but rather to set forth rules that apply within a particular EU country. The question is whether under existing law such codes could also be used as a legal tool for transferring data outside the EU, or whether the legal grounds for transferring data outside the EU described

above are the only solutions.

Article 26.2 of the Directive establishes that "a Member State may authorise a transfer or a set of transfers of personal data to a third country that does not ensure an adequate level of protection...where the controller adduces adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals…." The article adds that such safeguards "may in particular result from appropriate contractual clauses."

Searching for adequacy

The explicit reference to "contractual clauses" highlights that their use was the primary solution envisioned by EU legislators to ensure that exported data would be afforded the same legal treatment as if it had never left the EU country of origin. In line with the preeminence accorded to contracts in Article 26.2 of the Directive, the most common way heretofore to adduce such safeguards for data exporters and importers has been to enter into an *ad hoc* contract (or standard contract) that engages them to provide adequate safeguards for the transfer of such data.

However, the question is whether under the Directive it would be possible for exporters and importers to use alternative solutions, and in particular codes of conduct, to ensure "adequate safeguards." An interpretation based on the wording of Article 26.2 shows that contractual clauses offer one, but by no means the only way of providing such safeguards. Indeed, the use of the "may" followed by "result from appropriate contractual clauses" evidences that the Directive did not intend to limit the ways to achieve the goal of providing adequate safeguards only to "contractual clauses" but rather left the door open to other possibilities. Thus, one could argue that codes of conduct could fulfil the same role as contractual clauses in terms of providing the legally required safeguards.

However, any solution must provide the same safeguards that contractual clauses would offer. This issue is discussed in the following section.

Content of a Code of Conduct Dictated by National Laws

Under most Member State laws, those who have relied on *ad hoc* contracts as a way to export data from EU Member States must notify the transfer and the *ad hoc* contract to the national DPA, which will review the clauses and assess whether they afford the required protection. If they do not, the authorities will demand amendments to the contract until the desired level of protection is achieved. This procedure can take several months.

While the content required of such contracts varies from country to country, generally DPAs require the incorporation of obligations in the contract equivalent to those embodied in the data protection law of the country from which the personal data is being transferred. They may also require the inclusion of a joint liability provision. Furthermore, authorities will require the law of the exporter's country to apply to the contract, and they will insist on a jurisdiction clause ensuring that authorities in the exporter's country will be able to hear potential complaints.

If EU exporters decide to use codes of conduct as a tool to transfer data outside the EU, one should expect that DPAs of the different EU Member States would require them to follow a procedure similar to the one for contractual clauses. Thus, DPAs will exercise their competence to be notified of the transfer and to review the code of conduct. Equally, they are likely to require any code of conduct to have similar content or achieve the same results as when contracts are used for transferring data. Thus, *a priori*, the code of conduct would have to be based on the legal provisions of the law of the country where the data exporter is established.

For multinational companies that transfer data out of various EU Member States to countries that are found not to have adequate protection, this means that codes of conduct would have to be submitted to and approved by each Member State from which private data is exported. Further, if each DPA reviews the code of conduct, the likely result is that each one may have different requests and objections, so that ultimately the code of conduct may need different content for each Member State. If codes of conduct not only have to be adopted on a country-by-country basis, but also must have different content, it would render them impractical and worthless to pursue. To some extent, the use of codes of conduct would entail the same problems as those encountered when *ad hoc* contracts are used (as opposed to standard contracts). Not only would the content of the code of conduct have to be different for each Member State, but also the procedure for transferring the data would be as lengthy and cumbersome as when *ad hoc* contracts are used.

Making codes workable

The need for approval of a code by the DPAs of each Member State where personal data originates is a real problem that currently renders codes unworkable as tools for transferring data out of the EU.

The Commission is soon to issue a report on the implementation and application of the Directive in Member States. The report will consider whether there is any need for adoption of amendments to the Directive, and this seems a perfect occasion to address the issue of codes of conduct.

A one-stop-shop for approving codes of conduct for companies that process data in various Member States could provide a solution. Supranational bodies well positioned to carry out this job would be the Article 29 Data Protection Working Party (WP 29) and the European Commission. Because WP 29's agenda is quite full and because its *modus operandi* is not as flexible as the Commission's, one may wonder whether the competence for approval of codes of conduct should be taken over by the Commission. Alternatively, the Commission and WP 29 could jointly assume the responsibility for review. This solution might get a better reception from national DPAs, who would not feel

that the Commission had usurped their competency. If such competencies were taken up by the Commission, one should expect that they should be performed in a quick, open and flexible way. Anything different would deter companies from pursuing this avenue as a way to transfer data. It would also circumvent the purpose of achieving suppleness in the process of transferring data out of many EU Member States. In evaluating the code of conduct, one should hope that the Commission would require compliance with one set of rules only, probably the Directive (as opposed to 15 Member State rules). Furthermore, a company that is authorised to use a code of conduct as a global solution should also be exempt from having to file 15 notifications to DPAs at national level. However, the approval of codes of conduct on an *ad hoc* basis would be a major project that would require significant resources, which neither the Commission nor WP 29 have, thus rendering this possibility difficult in practice, unless the Commission is better staffed.

Another possible solution would be to empower the Commission to approve a set of model provisions for a code of conduct to which companies or groups of companies could adhere. Under the Directive, at the time of writing, it is uncertain whether the Commission has the authority to approve a code of conduct that is valid across the EU. It would appear that the Commission is looking into this question within the framework of the review of the Directive.

This solution would require the Commission to draft a single set of rules that, if complied with by companies, would be tantamount to compliance with national laws. For example, the code could provide an example of simple notices to data subjects which would be valid for all Member States, as opposed to the current situation where a company operating in the 15 Member States must draft 15 different types of notices. This approach should also eliminate the need for notification or further authorisation from DPAs.

Whatever solution is adopted, the approval of a standard code of conduct or the approval of *ad hoc* codes of conduct, should provide more flexibility to companies by reducing cumbersome administrative procedures.

Rosa J Barcelo is an associate at Morrison & Foerster (Brussels) and lecturer at the University of Namur (Belgium).

Information on the European Commission's Standard Contractual Clauses can be found at: www.europa.eu.int/comm/internal_market/en/dataprot/modelcontracts/index.htm

Genetic information rights? Of (vicious) mice and men

By Eugene Oscapella

A recent *Toronto Globe and Mail* report has raised anew the dilemmas that can flow from discoveries and knowledge about the genetic characteristics of individuals. Scientists have found an inherited gene mutation in mice that affects the brain and results in very vicious personalities. The report says that rodents with this mutation are prone to attacking their mates, siblings, surroundings, and even their lab handlers.

It is not yet known whether these findings will translate into a means for detecting increased genetic risk for violent behaviour in humans. The report says that the gene exists in humans but little is known about the role it plays except that it seems to kick in very early in human development, regulating a range of brain functions.

However, the findings highlight the frequent ethical dilemmas that flow from acquiring such information. If in fact human beings with a similar mutation are at greater risk of perpetrating violence, how should society react?

As a preventive measure, should all citizens be tested for the mutation? With whom will such information be shared? What are the consequences of carrying the mutation? Will mothers carrying foetuses with the mutation be encouraged or compelled to abort? Will those children and adults carrying the mutation be discouraged from procreating? Will employers be entitled to refuse to hire such individuals, and will children with the genetic trait be selected for special surveillance or schooling? How will the notion of "genetic determinism" affect traditional notions of criminal responsibility? Will individuals carrying the mutation be able to argue that they are not criminally responsible for their violent acts because of their genetic makeup?

On another front related to genetics, the BBC reported on May 3rd that Virginia has become the first American state to apologise for the forced sterilisation of thousands of its citizens as part of a eugenics, or selective breeding, programme in the last century. According to the report, Virginia conducted sterilisation programs until 1979 in an effort to wipe out hereditary deficiencies and vices.

Just months before Virginia made this apology, the *New York Times* reported another story involving Virginia that might cause concern about genetic privacy. The state was on the verge of requiring everyone arrested on suspicion of a violent crime to give genetic samples for possible matches in unsolved cases. Says the story, "The state already has the nation's largest bank of DNA because it takes saliva samples from each state convict. Expanding DNA swabbing to all those arrested in major felonies would be the most sweeping use of genetic testing by any state."