How accenture created a global approach to data transfers

Pérez Asinari, María Veroníca

Published in:
Privacy Law and Business International Newsletter

Publication date:
2002

Document Version
Publisher's PDF, also known as Version of record

How Accenture created a global approach to data transfers

By María Verónica Pérez Asinari

SPEAKING AT PL&B's Annual International Conference in July, Bojana Bellamy, Global Data Privacy Compliance Lead for Accenture, outlined her organisation's approach to transfers of personal data outside the EU.

Accenture is a global organisation doing business within a number of areas - including consulting, technology, and outsourcing - and operating across 49 countries, 29 of which have national data privacy laws. Finding an efficient, compliant and uniform means of processing personal data on a global scale, in particular transferring personal data within the organisation worldwide, is paramount to the day-to-day running of the organisation.

Two years ago, Accenture initiated a data privacy compliance programme to help it meet national requirements, while minimising any restrictions that regulatory obligations might have on the efficiency of its global operations. Accenture initiated its global strategy by carrying out an analysis of the data flows within sixteen global processes in the organisation and the various privacy laws of the countries in which it maintains a presence. In addition to meeting the strict requirements regarding cross-border data transfers, Accenture's objective was to establish an ongoing compliance culture across the organisation, which involved observing the individual privacy rights of its employees, clients and third party vendors and suppliers.

As a central part of its privacy programme, Accenture created a Global Data Privacy Policy to provide an adequate and uniform level of protection for internal transfers of data on a global level. Describing the policy as more of an internal code of practice, Bojana Bellamy said: "We think that it is workable, it can provide a very good solution." However, she cautioned that while it is a solution that suits Accenture, this self-regulatory approach is not necessarily the right option for all organisations. "I am not saying that codes of practice are better than laws. I don't think it would be workable for every organisation."

Accenture's privacy policy is based-on the high standard of the EU Data Protection Directive. The reason for this, explained Bellamy, is because it is the most pervasive privacy law. Even organisations located outside the EU can find themselves subject to the directive. "Even for our US controlled websites - if they are accessible by job applicants in Europe, or by employees in Europe - it will be the EU law that applies, according to the official interpretation of Article 4 of the directive."

In addition to the global policy, Accenture developed country specific policies to reflect the variations in national data protection laws. However, these country policies must not lower the standard of the global policy.

Finally, the policy is backed up by additional documentation, guidelines and templates, which include precise instructions and advice to employees dealing with personal data.

FINDING A LEGAL BASIS FOR DATA TRANSFERS

Accenture found a legal basis to justify international transfers on the basis of its code of practice through Article 26(2) of the EU Data Protection Directive. Article 26(2) relates to the transfer of personal data to countries outside the EU that have not been deemed to provide an adequate level of data protection. So long as the organisation that wishes to transfer data ensures adequate safeguards, there is scope to use codes of practice as an alternative to contractual agreements. However, the article does specify that member states are required to authorise these policies or codes of practice.

The code of practice approach taken by Accenture, said Bellamy, can offer a truly seamless, practical and workable solution to suit the global nature of its business in an environment where functional boundaries have replaced national boundaries. But, while there is a legal basis for a code of practice, the real problem is getting it approved by each EU Member State. Bellamy explained that Accenture has already conducted informal discussions with the national data protection authorities, and is now committed to making formal submissions for approval at a later date.

RESTRICTIONS ON DATA FLOWS

Bellamy continued to explain the reasons for deciding to adopt this approach and analysed other possible options. One of these options was to rely on derogations from Article 25 contained in Article 26(1). She argued that the derogations are not sufficient to cover everyday transfers in the normal course of their global business operations. For example, under the directive, there is no legal ground, other than consent, to allow the transfer of clients' contact details to non-EU approved countries for marketing and business

development purposes. She also said that it is impossible to examine every single transfer *a priori* to determine whether these derogations apply.

Another option was to obtain consent from individual data subjects. However, said Bellamy, the Article 29 Working Party says there are limits as to how valid a consent is in the employment field. For example, the Working Party has suggested it would be difficult to rely on consent for the processing of human resources (HR) details in situations where an employee is unlikely to have any choice in the matter. Despite this interpretation, Accenture obtained consent from its existing and future employees globally, both via employment contracts and separate notice and consent. "Is it going to stand legally in a court of any Member State," asked Bellamy? "I don't know, maybe not...but at least we have tried and raised awareness."

Alternative solutions

The main alternative, proposed by the European Commission, is its Model Clauses for data controllers. Bellamy, however, explained that this approach was not suitable for Accenture's style of business for a number of reasons. Most importantly, Model Clauses would create a dual regime for EU data and non-EU data. "Our systems do not allow us to do that...our global policy is applicable to all data, all citizens, wherever they and we are."

Organisations could also consider entering the US Safe Harbor scheme. It's another option, said Bellamy, but as a bilateral arrangement, it does not offer a truly global solution. On the whole, she regards Accenture's approach as the best solution for the organisation, as it is lawful, privacy friendly, and most importantly, workable.

María Verónica Pérez Asinari is a researcher at the Centre de Recherches Informatique et Droit, University of Namur, Belgium.