

Why Does This Have To Be So Difficult?

Joel Harrison bemoans the unnecessary hurdles placed in the way of transfers to data processors outside the EEA. He suggests a way to end the 'burden' on gleeful bureaucrats and ease the life of the data protection lawyer.

There comes a point in almost all global outsourcing projects when compliance with EU data protection law, and specifically the restrictions on transborder data flows in Chapter IV of the Data Protection Directive, is addressed. This should ideally happen before the technical solution has been agreed, the contracts have been signed and data transfers have already commenced, but data protection lawyers have come to be grateful that they are consulted at all.

The format of these discussions is by now well-known. Someone will ask, no doubt perfectly innocently, whether data subjects can't just be asked to consent to their data being transferred outside the EEA; this will be swiftly discounted, the Article 29 Working Party having effectively neutralised Article 26(1)(a) of the Directive beyond all practical use. The parties may make a brief foray into more exotic territory, such as Binding Corporate Rules and the US Safe Harbor, but will invariably return dazed and very confused as to whether, and how, these could ever apply to transfers to data processors. The customer's privacy officer might even perform his own assessment of the safeguards in the third country, but then again he might perform his own assessment of the safeguards on the next aircraft he flies on – it would be roughly as safe and, according to several national regulators, about as lawful. Eventually, as with so many things in life, the parties will be won over by the homely charms of the old-fashioned and functional rather than the superficial glitz of the new-fangled and glamorous, and will settle for signing agreements incorporating the model clauses for transfers to processors in third countries.

But the matter doesn't end there, for a brief investigation reveals a remarkable divergence in practice between national regulators. Whilst our own ICO is content for data controller and data processor simply to sign the model clauses, many other regulators take a far more hands-on approach, and some are – how to put this? – less than wholly pragmatic. Austria, France and Spain are particularly notorious in this respect, as are several of the new accession countries. In some cases, transfers cannot proceed until the national authority has given its consent, even when the model clauses are used (these authorities having enthusiastically noted that the restrictions in Article 4(1) of the Commission Decision adopting the model clauses are without prejudice to the authorities' powers to ensure compliance with all the other provisions of the Directive). Were this not bad enough, these authorities routinely demand an array of documents and information in support of their deliberations, much of which has to be translated. The overall effect is to add anything from four weeks to six months (sometimes more) to the overall deal timetable.

This is a pointless waste of time and money, and does nothing but add cost, delay and uncertainty to commercial transactions. It is based on the flawed assumptions that the regulation of processing of personal data in third countries, or the technical and organisational measures adopted by processors in third countries, somehow offer data subjects fewer safeguards than in the EEA. These assumptions deserve careful scrutiny.

To be clear, we are concerned here only with transfers to *data processors* in third countries. There are good reasons why personal data should not be transferred to *data controllers* in third countries – essentially, taking the processing of that data altogether outside the protections afforded by the Directive – without the parties being required to adopt additional safeguards. But in the case of transfers to data processors, where the data controller remains responsible for compliance with the Directive, this is wholly unwarranted.

It is true that there are certain countries in which the activities of data processors are unregulated. These include the lawless badlands of the United Kingdom, where the activities of data processors fall almost entirely outside the scope of the Data Protection Act. If a data controller established in another EU Member State outsources the processing of personal data to a data processor based in the UK, that processor can behave in the most negligent way imaginable and the ICO will be powerless to intervene. The ICO can serve neither an information notice nor an enforcement notice on the data processor, and the data processor cannot be the subject of a monetary penalty notice. In fact, the most the ICO could do is write a strongly-worded letter to the national authority of the other EU Member State with a recommendation that the authority take action against the data controller. Viewed from this perspective, the UK affords about as much protection to a data controller established in another EU Member State as does any third country with which that Member State enjoys cordial diplomatic relations.

The approach adopted by the UK in implementing the Directive is admittedly at one end of the scale (other EU Member States impose greater obligations on data processors), but in this respect (if in no other) it is

consistent with the Directive. And this exposes the fallacy inherent in Chapter IV of the Directive as it applies to data processors – from a legal point of view, a data controller engaging a data processor in another EEA Member State is not guaranteed *any* safeguards over and above what it might expect from a data processor in a third country, because the Directive does not impose *any* mandatory requirements on data processors. So, why on earth treat transfers to data processors in third countries any differently from transfers to data processors in EEA Member States?

As to the technical and organisational measures adopted in third countries, we Europeans flatter ourselves if we think we really are better at protecting personal data than countries outside the EEA. IT outsourcing providers in leading offshore outsourcing jurisdictions such as India and the Philippines operate to the highest standards seen anywhere in the world. Many are certified as CMMI level 5 compliant; most are certified to comply with ISO/IEC 27002. Global service providers such as Accenture, CSC, EDS and IBM, as well as offshore providers such as Cognizant, Genpact, Infosys, Tata and Wipro, all have offshore delivery centres that are certified to CMMI level 5, whereas very few are certified to the same level in the EEA. And EU data protection law has, let us not forget, failed to prevent personal data from being exposed on unprotected public websites, lost in the post on unencrypted CD-ROMs and, in some cases, unashamedly sold to the highest bidder.

So, what's to be done to end this needless bureaucracy? Simple: amend Chapter IV of the Directive to limit its scope to controller-to-controller transfers, treat transfers to processors outside the EEA in exactly the same way as transfers within the EEA, and deal with breaches of security by processors in third countries as breaches of data protection law in the usual way. This would, at a stroke, reduce transaction costs, shorten the time taken to complete deals and make it easier for customers and suppliers to agree reliable plans for transition and transformation of services, and would not reduce the protections afforded to data subjects one iota. It would also eradicate what is probably the most irritating part of the data protection lawyer's job - which must surely figure somewhere between climate change and banking regulation in the list of pressing issues facing European legislators.

Joel Harrison is an associate in the Communications, Technology & Outsourcing group of Milbank, Tweed, Hadley & McCloy LLP, and is based in the firm's London office.