

## Data protection concerns over using servers in the US

Many UK organisations transfer data to the US in a variety of ways, without necessarily realising that they are doing so. For example, a data transfer could happen where an organisation uses systems (for example, HR, accounting, CRM) hosted by a company using servers in the US or where contracts are outsourced to a company with a US connection.

Following a recent European Court of Justice case, transferring data to the US carries a much greater risk of contravening data protection law than it used to.

Organisations in contravention of the law could be subject to the Information Commissioner's Office's (ICO) enforcement powers (which include prosecutions and monetary penalties) along with the adverse publicity that inevitably couples any breach of data protection law.

### Change in the law

It used to be the case that organisations could rely on the 'Safe Harbor' regime as the legal basis on which data could be transferred to the US. EU privacy law prohibits the movement of personal data outside of the EU, unless it is transferred to a location which is deemed to have 'adequate' privacy protections in line with those of the EU. The Safe Harbor agreement that was made between the European Commission and the US Government allowed US organisations to self-certify their compliance with certain principles. US organisations signed up to the Safe Harbor regime were deemed to provide adequate protection for the purposes of EU privacy law.

This agreement was declared invalid in October 2015 by the European Court of Justice in the case of [\*Maximilian Schrems v Data Protection Commissioner\*](#). Concerns about the security of individuals' data were raised and reference made to the US authorities' extensive ability to access personal information.

The European Commission has urged organisations to consider putting in place legal and technical solutions to mitigate the risks faced when transferring data to the US. Any organisation transferring data to the US will need to review its processes accordingly.

A deadline of the end of January 2016 has been put in place for a new Safe Harbor agreement to be concluded with the US authorities and the European Commission has stated that if no such political agreement is reached, national enforcement agencies (in the UK, the ICO) will take all necessary and appropriate enforcement action in tackling any breach of the law.

### How to comply with the law

The first question to ask is whether there is a transfer of data to the US. Where US servers are concerned, if the data is merely 'passing through' those servers, it is not considered to have been transferred to the US. However, if the data is accessed or manipulated at all, a transfer will have occurred.

Where data is transferred, there are still a number of ways to do this within the law. Most of these have limited application and so we have not detailed them all here.

The most common ways of ensuring compliance are as follows:

- (1) the data subject gives their consent;
- (2) the use of an agreement incorporating standard contractual clauses.

### **Option 1 – Consent**

Enshrined at the heart of data protection law is the concept of consent and that, generally, a transfer of data from one party to another will be legitimate, if the individual to whom the data relates consents to that transfer.

However, the concept of 'consent' is tricky and the threshold required can be difficult to meet.

Consent should be freely given, specific and informed. To meet this standard, the data controller (i.e. the person who determines the purposes for which and the manner in which any personal data is to be processed) must provide the individual with full details of the proposed transfer of data to the US – to whom the data is being transferred and the purpose of this. Furthermore, efforts will need to be made to ensure that this information is made clear to the individual and that they clearly consent to the transfer on this basis. For example, including this information in the small print is unlikely to be sufficient.

Some commentators have speculated that for the consent to be valid, the individual must be informed that their data could be accessed by US authorities.

Clearly the context of the transfer will be important and we would recommend that any organisation seeking to rely on consent alone to justify a transfer of data to the US seeks advice on their processes and whether they are likely to be compliant.

### **Option 2 – Standard contractual clauses**

The European Commission determines that the use of certain approved standard contractual clauses can provide an adequate level of protection. To include the relevant clauses in any contract with a US entity will often be the simplest way for an organisation to be compliant with data protection law.

Many existing contracts will not include these provisions, as there was no need when the Safe Harbor regime was in place. Contracts should therefore be reviewed on this basis.

Organisations will need to consider the chain through which data flows and how to appropriately draft their contracts in light of this.

### **The future**

Negotiations have been ongoing between the US authorities and the European Commission with the goal of a political agreement similar to the Safe Harbor regime. However, as detailed above, if nothing is agreed by the end of January 2016, the European Commission has stated that national authorities will take all necessary and appropriate enforcement action.

**James Sinclair Taylor**

Partner

+44 (0)20 8394 6480

[James.Taylor@russell-cooke.co.uk](mailto:James.Taylor@russell-cooke.co.uk)

**Gareth Roy**

Associate

+44 (0)20 8394 6493

[Gareth.Roy@russell-cooke.co.uk](mailto:Gareth.Roy@russell-cooke.co.uk)

This material does not give a full statement of the law. It is intended for guidance only and is not a substitute for professional advice. No responsibility for loss occasioned as a result of any person acting or refraining from acting can be accepted by Russell-Cooke LLP. © Russell-Cooke LLP. January 2016

**[www.russell-cooke.co.uk](http://www.russell-cooke.co.uk)**