Data Protection Day—Schrems and Safe Harbor in the public sector

27/01/2016

Public Law analysis: Data Protection Day aims to raise awareness as to how data is used and explores the latest developments in data protection regulation. As part of our Data Protection Day series, Pulina Whitaker, partner at Morgan, Lewis & Bockius, considers the Schrems ruling and its impact on Safe Harbor from a public sector perspective in light of the forthcoming General Data Protection Regulations (GDPR).

What is the background to the invalidation of the Safe Harbor framework?

According to the European Commission, the United States is a country of 'inadequate' data protection. The European Commission and the US Department of Commerce, therefore, agreed in the year 2000 to a self-certification programme for US organisations to receive personal data sent from Europe. The self-certification programme provided that US organisations must certify that they adhered to standards of data processing that are comparable with EU data protection laws such that EU citizens' personal data was treated as adequately as if their data had remained within Europe. This Safe Harbor programme is operated by the US Department of Commerce and enforced by the Federal Trade Commission (FTC). Over 4,000 organisations have current self-certifications of adherence to Safe Harbor principles. In the course of Irish litigation, a question was referred to the European Court of Justice (ECJ) for a preliminary ruling on whether EU data protection authorities can investigate data transfers to organisations with Safe Harbor certification.

Mr Schrems complained in Irish legal proceedings that the Irish Data Protection Commissioner refused to investigate his complaint that the Safe Harbor programme failed to protect adequately personal data after its transfer to the US in light of revelations about the National Security Agency's PRISM programme. The question of whether EU data protection authorities have the power to investigate complaints about the Safe Harbor programme was referred to the ECJ (*Schrems v Data Protection Commissioner* [2015] All ER (D) 34 (Oct), C-362/14). Yves Bot, Advocate General (AG) at the ECJ, said in an opinion released on 23 September 2015 that the Safe Harbor programme does not currently do enough to protect EU citizens' personal data because such data was transferred to US authorities in the course of 'mass and indiscriminate surveillance and interception of such data' from Safe Harbor-certified organisations. AG Bot was of the opinion that the Irish Data Protection Commissioner, therefore, had the power to investigate complaints about Safe Harbor-certified organisations and, if there were 'exceptional circumstances in which the suspension of specific data flows should be justified', to suspend the data transfers pending the outcome of its investigation.

The ECJ followed AG Bot's opinion and, further, declared that the European Commission's decision to approve the Safe Harbor programme in 2000 was 'invalid' on the basis that US laws fail to protect personal data transferred to US state authorities pursuant to derogations of 'national security, public law or law enforcement requirements'. Furthermore, EU citizens do not have adequate rights of redress when their personal data protection rights are breached by US authorities.

How has the public sector reacted to the development?

The decision created significant uncertainty for EU-US data transfers. Technically, the decision also means that the EU-approved standard contractual clauses and binding corporate rules, two other options for EU-US data transfers, could be at risk if a similar challenge is mounted against their use for the same reasons that Safe Harbor was invalidated. Data transfers to the US have continued to take place since the decision. Safe Harbor-certified organisations have had to put in place alternative mechanisms, such as standard contractual clauses which currently remain valid. Additionally, organisations who engaged Safe Harbor-certified providers have had to discuss alternative data transfer options with these providers.

What has been the approach of, for example, the Information Commissioner's Office (ICO), the Article 29 Working Party and other European data protection authorities?

The ICO has adopted a muted approach to the decision. It reiterated that concerns over Safe Harbor were not new and that other options, as outlined above, are available to organisations. The Article 29 Working Party stated that it is important that EU data protection authorities take a unified stance to the decision and that EU Member States should

agree with the US authorities how best to protect European personal data. The European Commission called on Member States to work effectively with the US authorities to achieve this aim. It also reiterated the point highlighted in the *Schrems* decision that data protection authorities have independent powers to act against organisations undertaking unlawful data transfers by suspending data transfers and conducting their own investigations into suspected breaches of data protection laws. Some of the German regional data protection authorities launched investigations into the collection and international transfers of personal data by technology and telecoms companies. All bodies are, however, agreed that alternative, workable and certain solutions to achieve EU-US data transfers must be found and without undue delay.

What has been the approach of the US Department of Commerce and the FTC?

The Department of Commerce has stated that it will continue to administer the Safe Harbor programme for those organisations who wished to apply for certification in the interim while the European Commission considers its guidance for Safe Harbor-certified organisations. This guidance was due by the end of January 2016 but this now looks like to be expected during the course of February 2016. We understand that the Article 29 Working Party is scheduled to meet on 2 February 2016. The FTC has stated that it is committed to working with the European authorities to protect European personal data and these discussions are ongoing.

Have any of the rules in the GDPR taken into account the Schrems ruling?

No. The key concern regarding access to personal data by US authorities cannot be addressed by the GDPR. State-level discussions about this issue are taking place and progress has been made, for example under the Umbrella Agreement. The key changes in the GDPR for international data transfers are:

- standard contractual clauses will no longer need to be approved by data protection authorities (as is currently the case for some European countries)
- data transfers can be made upon certifications, seals or marks established to evidence appropriate safeguards provided by controllers or processors that are not subject to the GDPR and which allow these controllers or processors to make binding and enforceable commitments to apply these safeguards and adhere to individual data protection rights
- the removal of the current right of EU-based organisations to self-assess if a data transfer to an otherwise 'inadequate' country would be adequate because of the contractual requirements imposed on the data recipient to protect the data—instead, a code of conduct option is available for data transfers to 'inadequate' countries
- the binding corporate rules programme has also been expanded to cover third party data processors, and
- explicit consent can also be a lawful option to transfer personal data to an otherwise 'inadequate' country and this standard of consent is higher than the previous 'unambiguous consent'

Interviewed by Alex Heshmaty.

The views expressed by our Legal Analysis interviewees are not necessarily those of the proprietor