Data Protection Day 2019—the US CLOUD Act and what's at stake for UK and EU businesses

28/01/2019

Information Law analysis: The UK could be the first Member State to enter into an executive agreement with the US over the sharing of data between businesses across the two jurisdictions under the US Clarifying Lawful Overseas Use of Data Act 2018 (CLOUD Act). Dr Nathalie Moreno, partner in the technology, commercial and data privacy group at Lewis Silkin, considers the compatibility of the CLOUD Act with UK and EU data privacy legislation and how this will impact UK and EU business.

What is the background to and purpose of the US CLOUD Act?

European businesses cannot ignore the relentless determination of US law enforcement agencies to gain access to data, whether that data is 'located within or outside the United States' as demonstrated by the recently enacted US CLOUD Act.

The CLOUD Act entered into force on 23 March 2018 and regulates enforcement authorities' rights to compel electronic communications service providers, subject to US jurisdiction, to give access (via warrant or subpoena) to data within their 'custody, control or possession' to protect national public interests.

It is no coincidence that, two months later, another landmark piece of privacy legislation with significant extra-territorial effect also came into force across the Atlantic—the EU's General Data Protection Regulation (EU) 2016/679 (GDPR)

In 2018, in the case United States v Microsoft Corp 548 US (2018)—known as the 'Microsoft warrant case'—US federal agents served on Microsoft a search warrant requiring disclosure of customer data stored in their data centre in Ireland, as there were suspected links to drug trafficking. This case brought to light the fact that there was a delicate balancing of interests to be done between the need for a government to reach across international borders to prevent crime, versus the risk of undermining domestic privacy rules that protect personal data from interference by foreign governments. The Supreme Court vacated jurisdiction leading to the enactment of the CLOUD Act.

The primary purpose of the CLOUD Act—which amends US Stored Communications Act 1986 (SCA 1986)—is to support the US Government's efforts to protect public safety and combat serious crime, including terrorism, by gaining access to potentially vital data in the interest of national security, whether or not that data is stored 'within or outside of the US'. It also gives foreign governments the right to obtain data stored within the US, subject to certain requirements.

What are the implications for US-based service providers with operations in Europe, and UK based service providers?

The CLOUD Act grants an extraterritorial reach to US law enforcement agencies and will impact service providers with operations in the EU and the UK.

In order to facilitate access for the US authorities to data held on foreign soil (and vice versa), the US Government will enter into binding bilateral data sharing agreements, called 'executive agreements', with other countries.

The CLOUD Act applies to data that is in the 'possession, custody or control' of any US company or foreign companies with a presence in the US. However, some US-based service providers with operations in Europe may not be caught because the CLOUD Act distinguishes between companies that have their parent company in the US versus those that only have a subsidiary in the US. This includes:

- a service provider which simply has a subsidiary in the US will not be subject to the obligations under the CLOUD Act if all personal data relating to customers is stored in the EU and the subsidiary is not a controller of that data

- the CLOUD Act will apply to a parent company based in the US which stores data in the EU—although that company's EU data may be controlled by a EU-based subsidiary and wholly stored in the EU, the parent company will have to comply with disclosure requests as a deemed controller of the data

In addition, existing requirements (under SCA 1986) for gaining access to data are still applicable (eg requiring the law enforcement to obtain a warrant).

However, a US-based service provider has the right to challenge a disclosure request if it conflicts with foreign laws—the service provider may apply to modify or reject a law enforcement request, within 14 days of receipt, if it 'reasonably believes' that:

- the individual to which the data relates is not a US person nor resides in the US

- that disclosure would 'create a material risk' that the service provider would breach the foreign law

The possibility for a service provider to apply for a request to be modified or quashed is subject to an executive agreement been entered into between the US and the foreign state concerned. This is not the case, to date, with the EU or the UK or with any other state. Therefore, it is currently impossible to file a motion to quash or modify.

When an executive agreement has been entered into, a request may then be modified or quashed by the court if it finds that:

- the disclosure would cause the service provider to breach the foreign law

- the individual to which the data relates is not a US person nor resides in the US

- in the 'interests of justice' the legal process should be modified or quashed

Failing such executive agreement, courts can only rely on common law principles of comity under US case law to challenge the request. As a result, it is not clear whether a US court would uphold such a challenge.

It is also questionable how effective such a challenge raised by a service provider would be—courts may decide that only the individuals whose data is concerned should be able to appeal such a transfer.

To what extent does the CLOUD Act align with UK/EU laws and legislative initiatives? What action should UK businesses who share sensitive data as part of their work with US companies/partners take to ensure they comply with the US and UK legislation?

Conflict with the GDPR

The extraterritorial effect of the CLOUD Act may conflict with the GDPR. The CLOUD Act applies to 'US persons' who are within the US jurisdiction but whose data may be located outside of the US. The GDPR will equally apply to personal data relating to such US persons if they are resident in the EU or it relates to the business activities of an establishment in the EU.

The European Commission (the Commission) offered some insight in its amicus curiae letter addressed to the US Supreme Court in the Microsoft warrant case. It clarified that under the GDPR any data transfer outside the EU would be subject to concluding executive agreements and would be subject to additional conditions including suitable safeguards. It did not clarify whether the CLOUD Act in itself would provide suitable safeguards.

Beyond the Commission's letter, Article 48 of the GDPR prohibits the transfer of data to a third country (outside of the EEA) based on a court judgment, unless doing so is based on an international agreement, such as a mutual legal assistance treaty and, in this case, an executive agreement.

The question therefore remains open as to the lawfulness of any EU data transfers in response to a US court pursuant to the CLOUD Act.

For now, in the absence of executive agreements, service providers may be unable to file a motion to quash or modify disclosure requests and, therefore, find themselves in breach of the GDPR if they comply with a US Court order.

As the compatibility between the two pieces of legislation is still unclear, it would be advisable for a UK based service provider sharing EU sensitive data as part of their work with US companies/partners to document the data sharing arrangement in accordance with the GDPR and retain as much control as possible over the EU data so as to keep it out of reach of any US Court Order under the CLOUD Act.

Concerns with respect to UK laws

Serious concerns have been raised by US human rights and civil liberties organisations wary of the interpretation and application of human right standards adopted by UK laws should a US service provider be requested by the UK to give access to data of individuals based in the US.

In its letter to the US Department of Justice dated 26 November 2018, Human Rights Watch expressed concerns about the prospect of the conclusion of an executive agreement under the CLOUD Act which would allow the UK 'to acquire, or obtain access to, the content of communications, associated metadata, and other personal data held or transmitted by US companies' as it does not or may not 'adhere to applicable international human rights obligations and commitments' and may potentially violate US constitutional rights standards'.

This issue may affect people in the US as well as the intended foreign targets of any monitoring if the UK were to request access to data stored in the US in accordance with an executive agreement, as access may be provided to personal data belonging to people in the US, even if they are not targeted as such.

Understandably, the letter refers to the UK Terrorism Act 2006 and the UK Public Order Act 1986, as providing very broad prohibitions as to behaviours and words in respect of terrorism and expressions of 'hatred' on grounds of race, religion, or sexual orientation, both of which are deemed to be inconsistent with the First Amendment to the US constitution concerning freedom of speech.

Finally, the letter acknowledges that the UK government had backtracked on the Investigatory Powers Act 2016 provisions which would have allowed the government to require the 'bulk' retention of communications data. As such provisions were found to be non-compliant with EU law, the UK has very recently adopted the Data Retention and Acquisition Regulations 2018, SI 2018/1123.

There is another major controversy attached to the CLOUD Act in so far as it creates an exemption to the well-established mutual legal assistance system, which ensures cooperation between countries for obtaining assistance in the investigation or prosecution of criminal offences while complying with the data protections laws of both countries concerned. For example, it is possible under the CLOUD Act for the UK government to ask US companies for US-stored data—provided that such data does not belong to a US person or a person living in the US—without complying with US data privacy laws.

How has the legislation been received by the EU and in Member States?

The UK Parliament is likely to be the first Member State to execute an executive agreement under the CLOUD Act. The UK Parliament is currently considering the legal structure in the UK for such an agreement and is reviewing the Crime (Overseas Production Orders) Bill 2017-19 (the Bill). The Bill intends to provide law enforcement agencies and prosecutors with the power to apply for a UK court order to obtain stored electronic data outside of the UK for the purposes of UK investigations and prosecutions of criminal offences.

The Commission has also stated its intention to propose the adoption of a recommendation for a negotiating directive for an EU-US executive agreement. It has responded to queries relating to the CLOUD

Act by reiterating the prohibition under the GDPR of international data transfers based on a foreign request, unless there is a basis in EU law (including a possible international agreement).

Arguably, with the introduction of the CLOUD Act there is now an incentive and the framework for governments to assemble and put in place robust bilateral agreements allowing law enforcement agencies to access data across borders, to combat crimes lawfully.

Interviewed by Samantha Gilbert.

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