GIR
Global Investigations Review

JUST ANTI-CORRUPTION

As companies learn to navigate GDPR, the cost of cooperation increases

Clara Hudson
30 August 2018

istockphoto.com/lucadp

The General Data Protection Regulation (GDPR), the new EU-wide data privacy law which came into effect in May, threatens significantly increased penalties for companies sending an individual's data across borders. The law, which mandates robust privacy rules, gives EU citizens more control over how their personal data is stored and processed by businesses. Companies that violate GDPR can be fined €20 million, or 4% of annual turnover, whichever is greater.

As GDPR became law, questions arose over how companies can process criminal data on individuals, such as whether a person has any previous convictions, and how the new rules affect a company's ability to collect or share personal data. What counts as personal information under GDPR is incredibly broad, and encompasses any data that can be used to identify an individual, such as an email or address.

Now a few months in, the restrictions have dredged up a wave of practical issues for lawyers and businesses alike. While lawyers say it's too early to assess the impact of GDPR, they warn that providing US authorities with overseas documents in cases will take more time and be more expensive.

Lawyers are well aware that they are expected to find other ways of providing the Department of Justice with evidence blocked by data laws, and that if they don't, their client

won't be awarded with full cooperation credit under the Foreign Corrupt Practices Act corporate enforcement policy, for example. The policy offers companies the presumption of a declination if they self-report foreign bribery, cooperate and remediate.

As part of that cooperation, the US government requires that companies deliver incriminating data on their own employees such as email exchanges and instant messages – a GDPR nightmare, lawyers say. Cooperation credit is not taken lightly by companies, which – if obtained – can result in considerable fine reductions.

But across the pond, questions remain over how aggressive data protection authorities in Europe will be now that they are empowered by GDPR, and whether they will have the resources to pursue each and every potential violation. For example, Ireland's data protection commissioner leads the agency out of a townhouse in Dublin, but has the power to investigate and potentially impose massive penalties on major companies with operations in the country such as Facebook, Microsoft and Google.

If companies can navigate GDPR by kowtowing to US authorities and avoiding penalties from EU data protection authorities, they can have their cake and eat it too.

Raising the bar on data privacy

Lawyers noted that they have been grappling with data privacy and transfer issues across the globe for years – it's nothing new. In particular, one lawyer pointed to South Korea as an example of a country with strict data privacy laws – some of the toughest in the world – that are fairly similar to GDPR. While GDPR itself isn't drastically different to prior EU legislation, it's the increasing fines that ramp up pressure on lawyers and companies alike. GDPR isn't even the whole story, as EU member states could impose additional data privacy hurdles that companies should be aware of.

Baker McKenzie partner Terry Gilroy in New York, who was previously in-house counsel at UK bank Barclays, said that data privacy has in the past several years been as much of a concern as protecting privilege.

"As a first year associate, my greatest fear was that I'd miss privileged content in a document, and that document would go out the door. Now, for document reviews concerning data in [foreign] jurisdictions, you have the same types of concerns," he said.

The GDPR shield

US officials have made clear that they won't be sympathetic to companies that don't rise to the challenge of bypassing GDPR.

First published on the *Global Investigations Review* website, August 2018

An assistant chief of the DOJ's FCPA unit, Ephraim Wernick, recently said at a Washington, DC, conference that he doesn't believe GDPR is an obstacle that can't be circumvented. Wernick added that restrictive foreign laws are "not going to stand in the way of us doing our job".

At the conference, both Wernick and an assistant director in the Securities and Exchange Commission's FCPA unit, Robert Dodge, said they will be looking out for companies attempting to sweep evidence behind GDPR's vast net. Dodge said the SEC will ask itself: "Is the company using this [GDPR] as a shield to keep us at arms length?"

While the DOJ is "not ever going to ask a company to break the law," Wernick said, prosecutors have to discern whether a company is trying to stonewall them.

Murphy & McGonigle partner Joseph Facciponti in New York, who previously worked in-house at UK bank HSBC, said: "Any company that thinks it could use GDPR as an excuse not to produce data to a US authority is going to be in trouble". In the past, the DOJ has asserted that it will challenge the merits of reluctant company's claims.

Companies will have to prove that they have "explored and exhausted numerous legal grounds" in transferring data to the US, Facciponti said.

One way to alleviate the DOJ's scepticism of "raising the data privacy flag," Gilroy said, is to be an open book. Companies should clearly explain the data privacy issues that they face, and spell out what risks employees could be exposed to, he said.

Sidestepping stringent data laws

GDPR states that data transfers across borders must be conducted through an established mutual legal assistance treaty (MLAT), an agreement which allows governments to share information. MLATs are a last resort, lawyers say, as companies who propose the often long and drawn-out process can be met with hostility by US authorities.

GDPR offers exemptions, which allow data transfers with the consent of the individual in question, or if the transfer is necessary to establish or defend against legal claims. But as GDPR is still in its early days, these avenues may not have been tested yet.

To work around stringent data protection laws across the world, Gilroy said, companies can conduct a very detailed review of documents and make redactions. By blacking out text that could risk violating laws outside of the US, companies can mostly give authorities what they want. This document-by-document process can take time and be expensive, as much as

doubling or tripling costs of collection and review. However, Gilroy clarified that the process is preferable to receiving a hefty US settlement for lack of cooperation.

“It’s cheaper than a big fine,” he said. “Cooperation credit will trump additional time and money spent on review and redactions.”

If MLATs are the only option, Gilroy said that offering additional help to US authorities may encourage them.

“You could say [to a US authority], here’s the person in our UK subsidiary who the request should be directed to. And by the way, we’re going to start collecting and reviewing the material now so that we’re ready when the request comes through,” Gilroy explained.

Increased cooperation between US and EU authorities could also benefit companies navigating GDPR, Facciponti said. He pointed to the DOJ’s formalised policy, announced in May by Deputy Attorney General Rod Rosenstein, that encourages coordination with other agencies.

If US and EU authorities are working together on an investigation, an EU authority may be able to pass data on to the US. This transfer could be made through data sharing agreements, including the 2006 agreement forged between the UK’s Financial Conduct Authority (back when it was known as the Financial Services Authority) and the SEC.

Collecting evidence “to the full extent permitted”

Prosecutors recently formalised that companies working tirelessly to minimise the effect of restrictive data laws will be rewarded.

In Société Générale’s June deferred prosecution agreement, the French bank received cooperation credit for “collecting and producing voluminous evidence located in other countries to the full extent permitted under applicable laws and regulations”. The agreement resolves charges that the bank used corrupt means to solicit business from state-owned financial institutions in Libya during the regime of dictator Muammar Gaddafi.

The phrase appears to break away from the boiler plate language which the DOJ has used in these agreements over the past few years: that companies can receive cooperation credit for “collecting, analyzing, and organizing voluminous evidence and information”. It is, however, worth noting that the French bank was not awarded full cooperation credit by the DOJ over unspecified “issues that resulted in a delay” during the early stages of the investigation.

First published on the *Global Investigations Review* website, August 2018

Lawyers for Société Générale did not clarify the circumstances behind the text, but former prosecutors confirmed to GIR Just Anti-Corruption that the language is a change from the previous standard regarding cooperation. The phrase clarifies that companies who bend over backwards to cough up evidence from foreign jurisdictions will be credited.

The Société Générale language is particularly notable because the DOJ no doubt relied on evidence in France, which has a particularly tough blocking statute. Under French law, moving commercial information to another country for foreign legal proceedings is a crime unless permission was granted by a French court.

French law has often tripped up companies under investigation in the US. At GIR's June Women in Investigations conference, Sidley Austin partner Karen Popp said the DOJ and SEC were once "furious" that a company she represented couldn't hand over data from France.

Lawyers noted, however, that when guiding a non-US company through a US investigation, there may be some resistance to the DOJ's cooperation demands. These companies – far away from the Washington, DC bubble – can be ambivalent to the fury of US prosecutors, and might not see them in the same light as those who have dealt with them before.

First published on the *Global Investigations Review* website, August 2018