



SEPTEMBER 2018

AUTHOR

PATRICK HROMISIN

U.K.'s First GDPR Enforcement Action Against Non-E.U. Company Marks a Significant Milestone

SUMMARY

The European Union General Data Protection Regulation (GDPR) may be only four months old, but the regulators responsible for enforcing it are already testing the limits of their powers. The United Kingdom Information Commissioner's Office (the ICO) confirmed last week that it has issued its first extraterritorial enforcement notice under the GDPR. The subject of the action is **AggregatIQ**, a small Canadian company that provides targeted advertising services on social media and has no permanent presence in the E.U. Earlier this year, a whistleblower alleged that **AggregatIQ** was linked to **Cambridge Analytica**, the company that allegedly used Facebook data to aid Donald Trump's 2016 presidential campaign in violation of Facebook's policies. **AggregatIQ** was also hired by the supporters of **Vote Leave**, the 2016 referendum campaign that successfully persuaded U.K. voters to vote in favor of "Brexit," the decision to leave the E.U. It was the work on Brexit that brought **AggregatIQ** to the attention of the ICO.

The ICO's enforcement action doesn't impose a fine on **AggregatIQ**, but rather, requires **AggregatIQ** to "[c]ease processing any personal data of U.K. or E.U. citizens obtained from U.K. political organisations or otherwise for the purposes of data analytics, political campaigning or any other advertising purposes." If **AggregatIQ** violates this order, it could be subject to fines of up to 20 million Euros, or 4% of its worldwide revenue, whichever is greater. **AggregatIQ** has indicated that it will appeal the enforcement proceeding.

From a jurisdictional standpoint, this enforcement action is a critical milestone for the GDPR. While it is an E.U. law, it is intended to apply worldwide to the processing of data relating to individuals within the E.U. Article 3(2)(a) of the GDPR states that it "applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to ... the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union." The GDPR also applies to non-E.U. entities that process data in connection with monitoring the behavior of individuals within the E.U., under Article 3(2)(b). The ICO's enforcement of the GDPR against a company based in Canada, with no offices in the U.K. or elsewhere in Europe, is likely to be a critical test of the GDPR's jurisdictional scope. U.S.-based organizations and companies should follow this matter closely.

Brexit itself may also introduce a jurisdictional wrinkle to GDPR enforcement by the ICO. It is unclear how much time it will take for **AggregatIQ**'s appeal to proceed and whether there will be subsequent litigation over these issues. The U.K. is in continuing talks with E.U. authorities to negotiate the terms of its exit from the E.U., but at this stage, there has been no agreement on whether the terms of the GDPR will continue to apply to the U.K. post-Brexit. The exit is scheduled to take place on March 29, 2019, and if the U.K. leaves the E.U. without an agreement



on the GDPR's continued application, AggregatIQ might be able to argue that the ICO lacks the authority to enforce the GDPR's terms.

The outcome of this enforcement proceeding may also provide guidance on the substantive, not just jurisdictional, terms of the GDPR. According to the ICO, as part of its work on Brexit, AggregatIQ was "provided with personal data including names and email addresses of U.K. individuals. This personal data was then used to target individuals with political advertising messages on social media." The ICO's enforcement letter to AggregatIQ alleges that it violated five provisions of the GDPR by processing this data improperly.

First, the GDPR's key principles include the following three requirements:

1. That personal data be "processed lawfully, fairly and in a transparent manner" under Article 5(1)(a);
2. That it be "collected for specified, explicit and legitimate purposes" under Article 5(1)(b); and
3. That data collection be "limited to what is necessary in relation to the purposes for which they are processed" under Article 5(1)(c).

And a fourth requirement is that under Article 6 of the GDPR, at the outset of any processing activity, a data controller must designate the lawful basis for the processing.

The ICO alleges that AggregatIQ violated each of these provisions because it "processed personal data in a way that the data subjects were not aware of, for purposes which they would not have expected, and without a lawful basis for that processing. Furthermore the processing was incompatible with the purposes for which the data was originally collected."

Finally, a fifth GDPR requirement that AggregatIQ allegedly violated was the duty to provide notice to data subjects concerning the processing that a controller carries out. The ICO alleges that AggregatIQ violated this requirement because it provided no notice about its processing activities. AggregatIQ's strategy on appeal has not been made public, but it seems likely to challenge the merits of the ICO's allegations as well as the ICO's jurisdiction.

Accordingly, for both jurisdiction and substantive reasons, the ICO's initiation of proceedings against AggregatIQ merits close attention.

Saul Ewing Arnstein & Lehr's Cybersecurity and Privacy Practice is able to assist organizations in assessing their cybersecurity risks and taking proactive steps to mitigate and reduce those risks. For more information on these matters, please contact the author or the attorney at the Firm with whom you are regularly in contact.

This Alert was written by Patrick Hromisin, a member of the Cybersecurity and Privacy Practice. Patrick can be reached at (215) 972-8396 or patrick.hromisin@saul.com. This publication has been prepared by the Cybersecurity and Privacy Practice for information purposes only.

The provision and receipt of the information in this publication (a) should not be considered legal advice, (b) does not create a lawyer-client relationship, and (c) should not be acted on without seeking professional counsel who have been informed of the specific facts. Under the rules of certain jurisdictions, this communication may constitute "Attorney Advertising."