Google’s Move to Avoid Data Uncertainty is Unfairly Criticized as GDPR Evasion

Article By
Dominic Dhil Panakal
Womble Bond Dickinson (US) LLP

Communications, Media & Internet
Global
All Federal
United Kingdom
European Union

Tuesday, March 17, 2020

No, despite having exited the European Union the UK is not free of its GDPR obligations. However, businesses holding EU data in the UK will need to keep a watchful eye on negotiations between the EU and its breakaway state. If the UK is not deemed “adequate” for receipt of EU protected data once the the safe transition period ends, entities in the UK may need to alter their contracts.

To this end, Google is changing the data controller for its United Kingdom user data from Dublin to Google LLC, their United States headquarters. Google’s plans to move British user accounts out of the EU and into the United States was wrongly attacked as taking those protections outside of the GDPR’s scope. The action, instead, should be seen as a hedge against the uncertainty of data treatment from the EU to the UK, so that data arising in the UK will not be seen as protected in the EU (Dublin) before traveling to the UK, which may trigger “adequacy of protection” problems unnecessarily.
Complaints from sources like The Irish Times (no surprise), claim not only that the U.S. privacy laws are among the weakest in the world, but also that “If British Google users have their data kept in Ireland, it would be more difficult for British authorities to recover it in criminal investigations.”

With Google’s new administrative change, EU privacy rights will continue to be protected by the GDPR. The EU GDPR and the UK version in the Data Protection Act 2018 will apply to Google regardless of where their data center is located. UK law enforcement offices will still be able to take action against Google. But without the intervening Dublin classification, UK data will not automatically be penalized for moving within Google classification back to the UK.

On January 31, 2020 the UK officially left the EU, and a new transition period began. This transition period runs until the end of 2020. The Information Commissioner’s Office (ICO) stated that existing rules on GDPR will continue to apply in the UK, and says it will be “business as usual for data protection” because UK’s privacy rules are aligned with GDPR. Data protection in the UK is regulated by its 2018 Data Protection Act, the UK’s implementation of GDPR. The UK government has additionally issued the Data Protection, Privacy and Electronic Communications (EU Exit) Regulations 2019, which amends the Data Protection Act of 2018 and merges it with the requirements of the EU GDPR to ensure the law applies appropriately.

There is not a deal in place on post Brexit data transfers and if negotiations are unsuccessful, the transfer of data between the UK and EU could be subject to significant changes. One of the provisions of GDPR requires EU citizens’ data to be safeguarded to European standards regardless of where the data is stored. The GDPR only permits cross-border transfers of personal data to “third countries” where such transfers comply with the requirements laid down in Chapter 5 of the GDPR. A “third country” refers to any country not among the twenty-eight Member States of the EU, Norway, Iceland and Liechtenstein, three countries that belong to the European Economic Area.

GDPR restrictions will apply to personal data being transferred into the UK unless the EU establishes that the UK is an “adequate” country. This will require the European Commission to evaluate for approval the UK for adequacy. If the UK and EU fail to arrive at a consensus, entities may have to rely on alternative transfer mechanisms. One alternative is the integration of GDPR-like data protection standard contractual clauses into contractual agreements.

The European Commission can decide that the aforementioned standard contractual clauses provide assurance that the EU data is protected by sufficient safeguards when transferred internationally. There are two sets of standard contractual clauses for data transfers from data controllers in the EU to data controllers established outside the EU or European Economic Area (EEA). Additionally, there is one set of contractual clauses for data transfers from controllers in the EU to processors established outside the EU or EEA.

Adequacy decisions are shaped, at least in part, by the EU’s trust of foreign governments and their access to EU citizen’s data. There has been reporting lately dwelling on the UK’s surveillance overreach. Combine this concern with angry sentiments towards the UK for leaving the EU, we may be in for a tumultuous period
for entities in the UK who process or control EU data. These concerns are suspended during the transition period.

Copyright © 2020 Womble Bond Dickinson (US) LLP All Rights Reserved.

Source URL: https://www.natlawreview.com/article/google-s-move-to-avoid-data-uncertainty-unfairly-criticized-gdpr-evasion