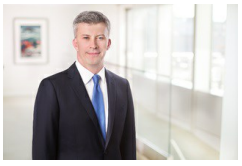
Key Contacts

Steve Bunnell
Washington, DC
D: +1-202-383-5399

Lisa Monaco
Washington, DC
D: +1-202-383-5413

Scott W. Pink
Silicon Valley
D: +1-650-473-2629



John Dermody
Washington, DC
D: +1-202-383-5306

Scott Harman-Heath
Washington, DC
D: +1-202-383-5214

PDF

EDPB Finalizes Guidance on GDPR Applicability Outside EU

December 11, 2019

The European Data Protection Board ("Board") recently published final guidance regarding the scope of GDPR's application outside the European Union. The final guidance is a culmination of a yearlong process, during which the Board solicited public input on draft guidance it released in November 2018. The final guidance updates several provisions of the draft guidance. The final guidance suggests that companies that hold or process data obtained from individuals in the EU will be subject to GDPR. This can include, among others, cloud storage providers, startups that facilitate or intend an application to be used in the EU, and even third-party contractors that process data on behalf of another company. Having promulgated its final guidance, the Board stated that entities whose conduct is within GDPR's scope are expected to be in compliance with "all provisions" of the Regulation.

The final guidance reiterates that parties must evaluate both whether they are "established" within the Union and whether any of their activities "target" individuals in the Union. Under the final guidance, a wide range of conduct can potentially trigger application of GDPR. Accordingly, parties who process or manage data that relates to EU residents or activities in the EU must continue to evaluate carefully whether their practices are compliant.

Under Article 3(1), GDPR applies to processing of personal data by parties that are "established" in the EU. The Board explained that per Article 3, when a controller or processor[1] takes steps that imply a "stable relationship" in the Union, any processing they control or undertake must comply with GDPR. The legal form of such arrangements, whether through

Related Practices

Data Security & Privacy

a branch or a subsidiary with a legal personality, is not determinative. For example, if a company establishes a branch office in the EU that oversees the company's European operations, the branch office is "established" in the Union. Similarly, if a company uses a branch office in the EU to facilitate and implement data processing activities in the EU, the branch's presence in the union is likely "established." If an entity is "established," GDPR applies to any controlling or processing of data carried out "in the context of the activities of the relevant establishment." This inquiry, according to the Board, is highly fact-specific.

While the threshold for establishment is low, the final guidance offered assurances that a non EU entity's actions do not necessarily become subject to GDPR the moment an employee is present in the Union. The Board explained that if a controller or processor's handling of data is unrelated to an employee's presence in the EU, GDPR likely does not apply.

However, the Board noted for the first time that when a controller delegates processing activities, which would otherwise be subject to GDPR, the controller has a responsibility to ensure the processor complies with GDPR. This applies regardless of whether the processor has established itself in the EU. For example, a Finnish controller cannot evade GDPR regulation by delegating processing responsibilities to a Canadian processor. In this hypothetical, the Finnish controller is obliged to take steps to ensure the Canadian processor complies with GDPR requirements.

Even if an entity is not "established" in the EU under Article 3(1), its conduct is subject to GDPR if the conduct "targets" individuals in the Union. The Board clarified that Article 3 encompasses only targeting activities that are "intentional" as opposed to "inadvertent or incidental." The Board explained that activities as minor as processing location data to offer targeted advertisements constitute "targeting" under Article 3(2) and brings conduct within the scope of GDPR.

The Board offered the following example of an entity whose conduct "targets" individuals in the Union: a US-based startup, with no business presence or establishment in the EU, provides a city-mapping application. As part of its routine functioning, the application processes users' personal data related to their location and offers targeted advertisement for places, restaurants, bars, and hotels to visit. The application is not available in all cities but does offer services for Paris and Rome. By specifically targeting individuals in Paris and Rome, the startup is "targeting" individuals in the Union and the processing of associated data must therefore comply with GDPR.

The Board clarified that an entity need not comply with GDPR simply because users interact with the entity while the user is in the EU. For example, an entity is not subject to GDPR if it clearly does not intend to target its application to the EU market. A provider that directs its application exclusively to the US market does not become subject to GDPR if a non-EU

resident uses the entity's mobile application while she vacations in or is otherwise visiting the EU. The Board confirmed that an application's use of exclusively foreign currency (*i.e.*, US Dollar) is evidence that a controller does not intend for the application to target the EU market.

Further, the Board reiterated that a processor, who is not established in the EU, may still have some activities subject to GDPR under Article 3(2) if its activities are "related" to the targeting activities of a controller. For example, by processing previously collected data to facilitate targeting of EU data subjects, a processor's activities become subject to GDPR. Importantly, the final guidance states for the first time that this includes cloud storage providers that process data on behalf of a controller that is targeting subjects in the EU.

Finally, a non-EU entity does not invite GDPR regulation by associating itself with an EU-based processor. For example, a Mexican retail company that offers its services only to the Mexican market is not subject to GDPR if it contracts with a Spanish data processor. The Mexican company is neither established nor targeting individuals in the Union and is therefore not within GDPR's scope. The Spanish processor, however, will be required to comply with GDPR in its processing of the Mexican company's data.

Once conduct is within the scope of GDPR, a party is obliged to comply with GDPR's requirements. The final guidance provided additional detail on the two responsibilities, in particular. First, a party that is not established in the Union must designate a data representative that is based in the Union. The final guidance clarified that parties are required only to appoint a single representative. Parties are not required to appoint multiple representatives for multiple activities within the scope of GDPR. Further, the final guidance confirmed that a party cannot designate its Data Protection Officer ("DPO") as its data representative in the Union. DPOs are responsible for monitoring compliance with GDPR. Because the DPO and representative's obligations will sometimes be in tension, the board explained that designating a single person to serve as DPO and representative would create a conflict of interest.

Second, Article 30 requires controllers and processors, established and unestablished alike, to maintain records of all covered processing activities. According to the final guidance, Article 30 imposes a joint responsibility on the controller, processor, and data representative. The final guidance went above the draft guidance's original proposal and added that the representative, in accordance with Article 27, must be able to provide relevant records to interested parties (*i.e.*, a supervisory authority).

The Board's final guidance raises particularly important compliance concerns for cloud storage providers and startups that facilitate or encourage users' accessing their services in the EU. More broadly, the final guidance reaffirms that GDPR raises difficult questions about compliance for any company whose business touches the EU. With the final guidance now adopted, companies must seriously evaluate all controlling or

processing activities to determine whether they are subject to GDPR and, if so, that they are fully GDPR compliant.

---

[1] Article 4 of GDPR states that a controller is a natural person or entity that determines the purposes and means of processing personal data. Conversely, a processor is a natural person or entity that processes personal data on behalf of a controller

---

This memorandum is a summary for general information and discussion only and may be considered an advertisement for certain purposes. It is not a full analysis of the matters presented, may not be relied upon as legal advice, and does not purport to represent the views of our clients or the Firm. Steve Bunnell, an O'Melveny partner licensed to practice law in the District of Columbia, Lisa Monaco, an O'Melveny partner licensed to practice law in New York, Scott W. Pink, an O'Melveny special counsel licensed to practice law in California and Illinois, John Dermody, an O'Melveny counsel licensed to practice law in California, and Scott Harman-Heath, an O'Melveny law clerk, contributed to the content of this newsletter. The views expressed in this newsletter are the views of the authors except as otherwise noted.

© 2019 O'Melveny & Myers LLP. All Rights Reserved. Portions of this communication may contain attorney advertising. Prior results do not guarantee a similar outcome. Please direct all inquiries regarding New York's Rules of Professional Conduct to O'Melveny & Myers LLP, Times Square Tower, 7 Times Square, New York, NY, 10036, T: +1 212 326 2000.

Attorney Advertising © 2020 O'Melveny & Myers LLP. All Rights Reserved.