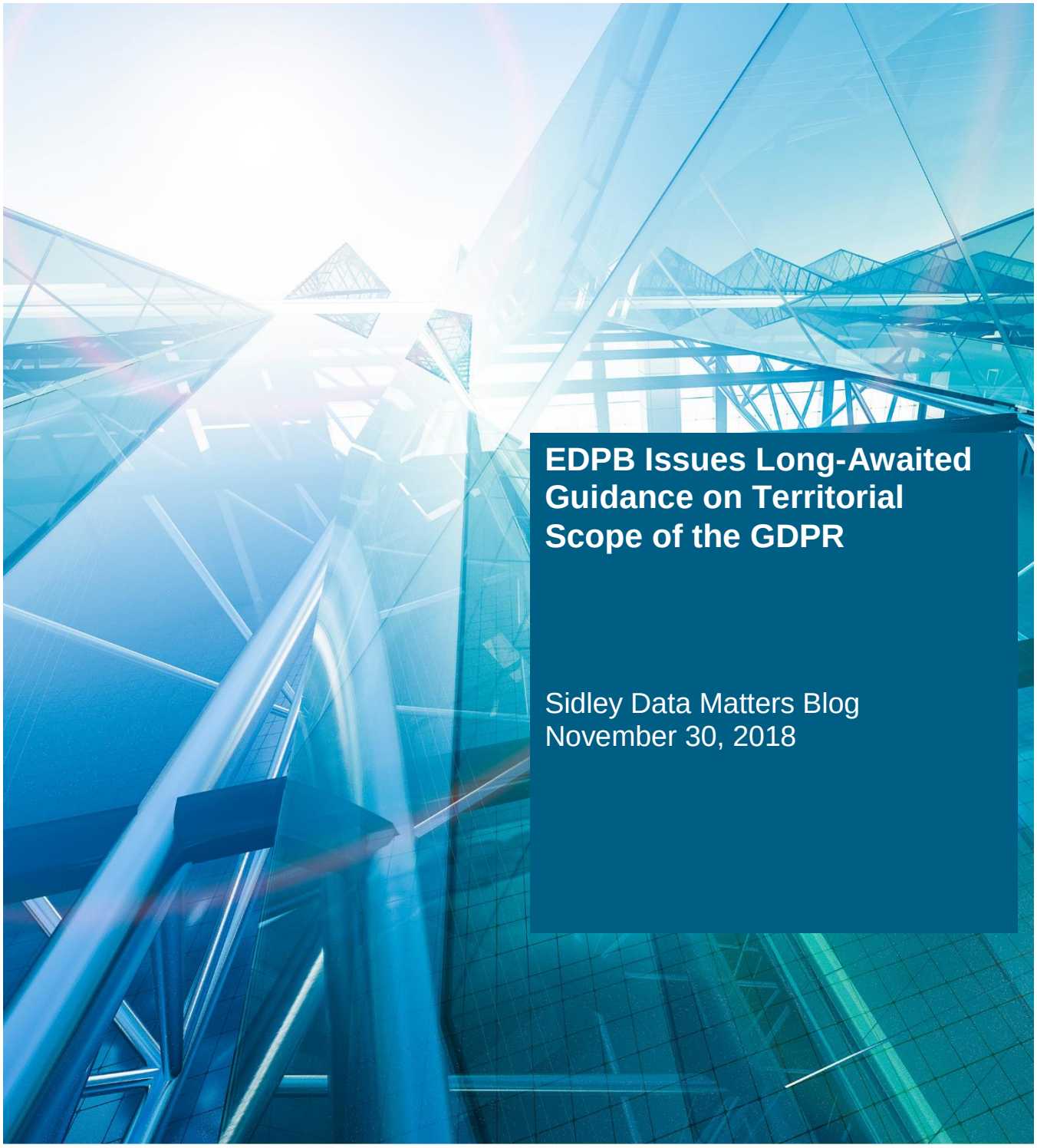

EDPB Issues Long-Awaited Guidance on Territorial Scope of the GDPR

Sidley Data Matters Blog
November 30, 2018

SIDLEY

TALENT. TEAMWORK. RESULTS.

EDPB ISSUES LONG-AWAITED GUIDANCE ON TERRITORIAL SCOPE OF THE GDPR

WIM NAUWELAERTS, WILLIAM RM LONG, CAMERON F. KERRY, COLLEEN THERESA BROWN, GERLADINE SCALI, LAUREN CUYVERS AND STEPHEN MCINERNY

November 30, 2018

On November 23, 2018, the European Data Protection Board ("EDPB") published draft guidelines seeking to clarify the territorial scope of the GDPR ("Guidelines"). The Guidelines have been eagerly awaited, particularly by controllers and processors outside of the EU looking for confirmation as to whether or not the EU data protection rules apply to them. The Guidelines largely reaffirm prior interpretations of the GDPR's territorial application under Article (3)(1), and offer essential guidance with respect to the GDPR's – heavily debated – extraterritorial application under Article (3)(2). The GDPR applies to companies established in the EU as well as companies outside of the EU that are "targeting" individuals in the EU (by offering them products or services) or monitoring their behavior (as far as that behavior takes place in the EU).

The proposed Guidelines are open for public consultation until January 18, 2019. It remains to be seen whether and how any outstanding issues will have been addressed upon conclusion of the consultation.

Some key takeaways include:

- **Not all companies that process personal data relating to individuals in the EU are necessarily subject to the GDPR.** Where, for example, a controller in the EU designates a processor located outside the EU to perform processing activities, the processor will not be subject to the GDPR merely because it is exposed to personal data that originates from the EU. However, the processor will have to comply with certain contractual obligations that the controller is required to impose on the processor pursuant to Article 28 Similarly, a controller outside of the EU which processes personal data relating to individuals in the EU may fall outside the ambit of the GDPR if it does not "target" or monitor individuals in the EU.

- **Companies outside the EU processing personal data relating to individuals in the EU may be subject to the GDPR** when they have an establishment in the EU and their processing activities outside of the EU can be considered "inextricably linked" to the (business) activities of that EU establishment.

- **The application of the GDPR to processing activities must be assessed per controller/processor**. For instance, the designation of a processor in the EU by a controller outside of the EU for certain processing activities does not automatically bring both the controller and the processor in scope of the processor is not considered an establishment of the controller for purposes of GDPR application. As such, the mere fact that the GDPR applies to, for example, a French subsidiary of a U.S.-based company acting as processor does not necessarily trigger application of the GDPR to the parent/controller in the U.S. In that case, the French processor will be subject to the GDPR's processor obligations only.

- **Minor commercial presence on EU territory may suffice as an "establishment" for GDPR purposes.** One single sales agent or employee, operating through stable arrangements in the EU, may trigger application of the GDPR if the processing of EU-originating personal data is in the context of the activities of that establishment.

- **The GDPR's extraterritorial reach only extends to the "targeting" or monitoring of individuals who are in the EU**. EU citizenship, residency or other type of legal status is therefore irrelevant to determine the scope of application of the GDPR. This would in theory also capture non-EU citizens whose behavior is monitored by an app while traveling in the EU.

- **Indications that contribute to the targeting intention of service offerings to the EU market** are the launching of marketing campaigns directed at an EU audience, the inclusion of addresses or phone numbers in EU Member States, the use of a top-level domain name specific to an EU Member State, the inclusion of travel instructions to a country in the EU, but also the mere international nature of the commercial activity itself in some instances (e.g. certain tourist activities).

- **"Monitoring" appears broader than foreseen in the GDPR's recitals**. According to the Guidelines, "monitoring" not only potentially covers online activity tracking via cookies, but could also include CCTV, Wi-Fi tracking and geo-localization activities. A case-by-case assessment needs to be performed in order to establish whether "monitoring" is performed.

- **Controllers and processors in scope of the GDPR by virtue of Article 3(2) must appoint an EU representative via a written mandate**, such as a service agreement, and the EU representative can be a law firm, consultancy firm or an individual. In the opinion of the EDPB, EU representatives should not take on the role of Data Protection Officer for the same controller/processor. Data controllers should inform individuals about the identity of their EU representative at the time of data collection, e.g. in the privacy notice.

- **The guidance leaves legal uncertainty for controllers and processor outside the EU on how to deal with the GDPR's data transfer restrictions (Chapter V)**. Controllers and processors outside the EU that find themselves subject to the GDPR are required to implement a GDPR compliance program, through which they offer an adequate level of protection to the personal data that are "imported" from the EU. Hence there are arguably no restricted data transfers in that case. Unlike recent UK ICO guidance, the Guidelines do not explicitly confirm that in such a case data transfer mechanisms are no longer required, and the EDPB did not address this question, leaving room for legal uncertainty. Hopefully this void will be addressed during the consultation round.