Re-Examining the GDPR’s Territorial Scope

By Andreas T. Kaltsounis

In November 2019, the European Data Protection Board (“EDPB”) issued its final guidance on territorial scope of the General Data Protection Regulation (“GDPR”), following release of the draft guidelines in November 2018 and a lengthy public consultation period.

Comparing the final and draft versions provides critical insight into the EDPB’s current stance on territorial scope, and how its position has changed over the past year. In most cases, the final guidelines clarify a more measured approach to territorial scope, which suggests the EDPB has accepted certain legal and practical limits to the GDPR’s extraterritorial scope.

But in some cases, such as how the targeting prong pulls processors not established in the European Union into the GDPR’s scope, the guidelines take a more expansive view of the GDPR’s territorial reach.

This article explores key takeaways and recommendations from the final guidance.

The GDPR Applies to Processing Activities, Not Organizations

Perhaps the most important general takeaway is the EDPB’s restatement that the GDPR applies to processing activities, not organizations. As the EDPB emphasizes in new language added to the final guidance, this means “certain processing of personal data by a controller or processor might fall within the scope of the Regulation, while other processing of personal data by that same controller or processor might not, depending on the processing activity.” And in new language discussing the scope of the targeting prong, the EDPB stresses “that a controller or processor may be subject to the GDPR in relation to some of its processing activities but not subject to the GDPR in relation to other processing activities.” In determining the GDPR’s application, therefore, we should not analyze whether an organization is subject to the GDPR, but instead whether a particular processing activity in question falls within its scope under Article 3.

The guidance also establishes important limits to Article 3’s “establishment” and “targeting” prongs that help ensure scope is considered in relation to discrete processing activities, not in relation to an organization as a whole. Take the simple example of a U.S.-based organization with no establishment in the EU that
The GDPR

intentionally offers goods to EU data subjects through an e-commerce site (i.e., it “targets” EU data subjects). Although the data processed by the organization in relation to its targeting activity is within the GDPR’s territorial scope (pursuant to Article 3(2)), personal data processed by the organization in any other context, even if it is personal data of EU data subjects, must be separately evaluated to determine whether it is within the GDPR’s scope.

Important considerations for the establishment and targeting prongs are addressed below.

The Establishment Prong

The final guidance retains the EDPB’s generally expansive view of the GDPR’s reach with respect to processing activities by controllers or processors established in the EU. But this reach is not without limits, and the final guidelines emphasize several important limitations on application of the establishment prong under Article 3(1).

- Where a processing activity is carried out by a controller or processor in the context of the activities of an establishment of that controller or processor in the EU, the EDPB retains an expansive view of the GDPR’s reach. In this scenario, the processing activity is in scope regardless of the actual place of the processing. This means that personal data of non-EU data subjects being processed in a non-EU country may be within the GDPR’s territorial scope under Article 3(1), if the personal data is processed in the context of the activities of an established controller or processor. Many continue to mistakenly believe that a GDPR scoping analysis is tied to a data subject’s EU residency or citizenship. It has nothing to do with either. Where personal data is being processed in the context of the activities of an established controller or processor, the GDPR’s protections apply to personal data of all data subjects whose data is processed, regardless of where those data subjects are located or where the data is processed, and regardless of whether the data subjects have ever set foot in the EU. This follows from the European treatment of data protection as a fundamental right and is a departure from most U.S. state-based data protection and breach notification laws.

- But an establishment in the EU does not bring every processing activity by an organization within the GDPR’s scope. Processing related to activities of the controller outside the EU remains outside the GDPR’s scope. As the EDPB clarifies in new language, “when an employee is based in the EU but the processing is not being carried out in the context of the activities of the EU-based employee in the Union (i.e. the processing relates to activities of the controller outside the EU), the mere presence of an employee in the EU will not result in that processing falling within the scope of the GDPR.” Therefore, although the bar to determine establishment may be quite low, this does not end the inquiry. To determine whether processing is being carried out in the context of an organization’s establishment in the EU, the guidelines instruct organizations to consider two factors: (1) whether the processing activities of the controller or processor outside the EU are “inextricably linked to the activities of a local establishment in a Member State,” and (2) whether “revenue raising” in the EU by the local establishment is “inextricably linked” to the processing of personal data taking place outside the EU and of individuals in the EU.

- A controller that uses a processor established in the EU is not considered established in the EU solely because it uses a processor established in the EU.

- Controllers and processors have separate obligations under the GDPR, and scope is considered separately for each entity. For example, a processor established in the EU may be subject to the GDPR’s provisions applicable to processors even though the processing activities of the controller it is working for fall outside the GDPR’s scope.

The Targeting Prong

The EDPB’s final guidance with respect to the targeting prong under Article 3(2) is mixed. It first limits the GDPR’s reach by emphasizing the intentionality required to trigger Article 3(2). But once that prong is triggered, the guidance expands the GDPR’s reach to any non-EU processor whose processing activity is “related to” targeting activity by a controller.

- Although the GDPR protects all natural persons in the EU, not just EU citizens, there are limits. With respect to offers of services, the targeting prong captures processing activities only for offers that “intentionally, rather than inadvertently or incidentally, target individuals in the EU.” Likewise, with respect to the offering of both goods and services, the EDPB added new language to emphasize that “when goods or services are inadvertently or incidentally provided to a person on the territory of
the Union, the related processing of personal data would not fall within the territorial scope of the GDPR.” Importantly, the guidelines now clarify that “if the processing relates to a service that is only offered to individuals outside the EU but the service is not withdrawn when such individuals enter the EU, the related processing will not be subject to the GDPR.”

But once an activity triggers the targeting prong, it can sweep both non-EU controllers and their non-EU processors into the GDPR’s scope. In an entirely new section to the final guidance, the EDPB has taken an expansive view of the GDPR’s scope with respect to processors not established in the EU. The EDPB clarifies that processing by a data processor not established in the EU may be subject to the GDPR under Article 3(2) if the processing activities “are related” to the targeting activities of the controller. That is, “where processing activities by a controller relates [sic] to the offering of goods or services or to the monitoring of individuals’ behavior in the Union (‘targeting’), any processor instructed to carry out that processing activity on behalf of the controller will fall within the scope of the GDPR by virtue of Art 3(2) in respect of that processing” (emphasis added). This is a critical clarification that may bring a non-EU processor within the GDPR’s territorial scope even though the processor is not established in the EU and is not the controller targeting individuals in the EU. The guidelines contain a new example (Example 20) in which a U.S.-based organization with a small satellite office in Ireland. Although the Irish office almost certainly satisfies the establishment prong under Article 3(1), only the personal data processed in the context of the Irish office’s activities falls within the GDPR’s territorial scope. The Irish establishment does not bring every processing activity carried out by the organization within the GDPR’s territorial scope, and other processing activities must be evaluated separately under Article 3’s two prongs. It is entirely possible, in this scenario, for the single organization to engage in at least three types of processing activities, each with a different scope:

1. A processing activity related to the context of the Irish office’s activities (e.g., a service offered in Ireland only and administered out of the Irish office), which is within the GDPR’s scope under Article 3(1), regardless of where the processing takes place.

2. A processing activity related to the targeting of EU data subjects (e.g., an app created by the U.S. office that has nothing to do with the Irish activity and targets EU data subjects generally), which is within the GDPR’s scope under Article 3(2).

3. A processing activity in the context of the organization’s activities outside the EU (e.g., an app created by the U.S. office that targets U.S. or other non-EU data subjects), which is not within the GDPR’s scope.

Interaction with GDPR Chapter V (Data Transfers)

Disappointingly, the EDPB failed to clarify the interaction between Article 3’s provisions on territorial scope and Chapter V’s provisions on international data transfers, despite public commentary requesting such clarification. This is unfortunate but perhaps expected given the uncertainties on international transfers raised by Brexit and the Schrems II litigation working its way through the Court of Justice of the European Union. In new language added to the final guidelines, the EDPB ducked the question, stating that “the EDPB will further assess the interplay between the application of the territorial scope of the GDPR, as per Article 3 and the provisions on international data transfers as per Chapter V. Additional guidance may be issued in this regard, should this be necessary.” Indeed, as noted by public commentary, it is necessary.

Types of Processing Activities

Considering the guidance in total clarifies that an organization — especially one not established in the EU — must examine each processing activity it undertakes in a separate analysis to determine whether the activity falls within the GDPR’s territorial scope. Consider a U.S.-based organization with a small satellite office in Ireland. Although the Irish office almost certainly satisfies the establishment prong under Article 3(1), only the personal data processed in the context of the Irish office’s activities falls within the GDPR’s territorial scope. The Irish establishment does not bring every processing activity carried out by the organization within the GDPR’s territorial scope, and other processing activities must be evaluated separately under Article 3’s two prongs. It is entirely possible, in this scenario, for the single organization to engage in at least three types of processing activities, each with a different scope:
In the meantime, controllers and processors should continue to use standard contractual clauses; Privacy Shield, where appropriate; and binding corporate rules, where available to corporate groups. Controllers and processors may also rely on guidance issued by the U.K. Information Commissioner’s Office (“ICO”) regarding “restricted transfers,” which advises that an international transfer to an organization whose processing of the transferred data is also subject to the GDPR is not a restricted transfer and requires no additional safeguards. But note that this is the ICO’s guidance only; other supervisory authorities may disagree, and the U.K. will likely soon not be a member of the EU.

**Article 27 Representatives and Enforcement Against Non-EU Organizations**

One of the more interesting clarifications in the final guidelines comes buried in the last section, dealing with representatives of controllers or processors not established in the EU.

This section begins with the expected statement that data controllers or processors subject to the GDPR under Article 3(2) (the targeting prong) must designate a representative in the EU under Article 27, unless one of the limited exceptions in Article 27(2) applies.

The guidance then adds new language that significantly limits the role and potential liability of the representative, in two ways.

First, where the draft guidance described maintenance of the Article 30 record of processing activities as a “joint obligation” of the controller or processor and the representative, the final guidance strikes the word “joint” and clarifies that “the controller or processor not established in the Union is responsible for the primary content and update of the record.”

Second, and most important, the final guidance reverses the draft guidance’s suggestion that supervisory authorities may take enforcement action against a representative for a controller’s or processor’s GDPR violations.

Edits to the draft language clarify that (1) “[t]he GDPR does not establish a substitutive liability of the representative in place of the controller or processor it represents in the Union” and (2) the representative concept was introduced to “facilitate the liaison with” controllers and processors.

Additional edits replaced aggressive language allowing direct enforcement against representatives with more benign language clarifying that the representative is merely a liaison in the enforcement process: “[I]t was the intention to enable supervisory authorities to initiate enforcement action against a proceedings through the representative in designated by the same way as against controllers or processors not established in the Union. This includes the possibility to impose for supervisory authorities to address corrective measures or administrative fines and penalties, and to hold representatives liable imposed on the controller or processor not established in the Union to the representative, in accordance its articles 58(2) and 83 of the GDPR. The possibility to hold a representative directly liable is however limited to its direct obligations referred to in article 30 and article 58(1) of the GDPR.”

This apparent about-face on direct enforcement against an Article 27 representative has two important consequences.

First, eliminating the option for direct enforcement against an Article 27 representative begs the question of how, exactly, supervisory authorities intend to enforce the GDPR against controllers and processors not established in the EU. It seems the EDPB has not yet resolved this question, as the guidance notes in new language that it is currently “considering” the development of “further international cooperation mechanisms” to enforce the GDPR in relation to third countries and international organizations.

Second, because the Article 27 representative may no longer be an enforcement hook against a nonestablished controller or processor, organizations that once hesitated to appoint a representative for fear of exposing the organization to enforcement liability may wish to reconsider this decision and check this box in order to avoid noncompliance with Article 27’s requirements. But despite this new guidance, organizations should remain cautious about how an Article 27 representative will affect enforcement options against a nonestablished controller or process. Uncertainty remains about whether some supervisory authorities will attempt to impose fines directly on representatives, especially under certain member state laws that are in conflict with the EDPB’s guidance.

**Conclusion**

The EDPB’s final guidance on territorial scope contains important new clarifications and examples that constrain the GDPR’s reach in some cases and expand it in others. Controllers and processors should consider these key takeaways and actions in light of the final guidance:

- Applying Article 3’s provisions to a controller’s or processor’s activities requires a nuanced analysis focused on (1) specific processing activities, and (2) activities of controllers and processors in separate analyses. The correct analysis is important because it determines the controller’s and processor’s respective
obligations as well as the processing agreements and data transfer mechanisms that must be in place.

- A similar nuanced analysis is required in the case of a personal data breach to determine (1) whether the data in question is within the GDPR’s scope, and (2) the respective notice obligations of a controller and processor, and whether those obligations arise from contractual terms only or direct application of Article 33 (notice to supervisory authorities) and Article 34 (notice to individuals) to the controller or processor.

- Controllers and processors that have not revisited how the GDPR applies to their processing activities since 2018 should do so, taking this new guidance into account. This is especially important for controllers and processors based outside the EU.

- Processors based outside the EU whose activities are related to a controller’s targeting activity should reexamine how the GDPR may apply to their activities and ensure they are complying with all direct obligations imposed on a processor.

- Controllers and processors outside the EU that have not appointed an Article 27 representative should reexamine their decision in light of this new guidance and conflicting member state laws.

Notes
2. Stricken language deleted in the final guidelines; italicized language added.