CARLTON FIELDS

CF on Cyber: The GDPR's New Territorial Scope Guidelines

CYBERSECURITY AND PRIVACY | DECEMBER 6, 2018


John E. Clabby


Steven Blickensderfer


Michael L. Yaeger

The European Data Protection Board on November 16, 2018, released new guidelines to help describe how the GDPR will apply to data controllers and processors both within and outside the European Union. The Guidelines focus on the territorial application of the GDPR, including both the "establishment" and "targeting" criteria. In this podcast, attorneys Jack Clabby, Michael Yaeger, and Steven Blickensderfer discuss these new guidelines and how they affect businesses not only in the EU, but around the world.

Transcript:

Jack: So today we're going to talk about the new guidelines adopted on November 16th of 2018 from the European Data Protection Board. The goal today is not to go through this in long detail. They're pretty significant and that would take a long time. The goal today is to hit some of the highlights of these new guidelines, focusing on the impact of them for U.S.-based companies.

We have with us two Carlton Fields attorneys, Michael Jaeger, who's a shareholder in our New York office. Michael does a significant amount of cybersecurity work across industries with a particular experience in health care and financial services. We also have with us Stephen Blickensderfer who's a privacy attorney and a CIPP from our Miami office. So welcome, Michael and welcome, Steve.

Steve, let's get started with you. These guidelines are published by something called the European Data Protection Board. Can you give us a sense of what that is?

Steve: Hey Jack, thanks. So the European Data Protection Board or "the Board" for short, is an independent European body that promotes cooperation between e-regulators. It's comprised of the various Member State Data Protection Authority representatives and one of the main things they do is achieve this cooperation through guidelines, through issuing guidelines on the GDPR on big issues.

Just to provide some context on how important some of these guidelines are, back in March I went to the, you know, was at a big conference. The European regulators were there and one of the messages that they conveyed to us was that they believe that we have enough guidelines or that there are sufficient guidelines out there and that they, you know, put enough information out there where companies can start, you know, can be well on the road to GDPR compliance.

So, you know, we've been waiting for these guidelines on extraterritoriality of Article 3 for quite some time so it's, you know, one of those things that we shouldn't expect too many more guidelines. So when we do see guidelines from the Board, it's pretty important. We should all take notice.

So one of the other things I wanted to mention were the import—or the effect of these guidelines. Really, at the end of the day, they're persuasive authority. The GDPR is enforced by the Member State Data Protection Authorities and it's interpreted by European courts, not the Board. However, it's safe to say that these guidelines are pretty persuasive. Particularly where we see the Board aligning itself with European court case law, you know, the Google versus Spain case for instance. So, you know, I think it's safe to say that these guidelines in particular were pretty persuasive.

Jack: Alright, so Michael, we heard from Steve a bit about the Board that creates these guidelines, but this particular release in mid-November, you know, what is it aimed at?

Michael: Well, Jack, I'd say the purpose of these guidelines is to make clear the territorial scope of the GDPR. It's like the old cliché, the long arm of the wall. So, the guidelines are trying to tell you how long the arm is, how far it reaches. And the guidelines have to be reviewed kind of carefully because they're full of caveats and nuance, but they're still helpful. It's not all pain.

And I'd say there are two main ways that the arm of the GDPR can reach somebody, can reach a company. First, if you're an establishment in the EU, and second, if you're targeting data subjects in the EU. And that's how the guidelines are organized. They discuss what makes a controller or processor an establishment and they discuss what actions qualify as targeting.

Jack: So we've linked to these guidelines in the podcast prompt you can pull them up and take a look, but it really, they are organized around these two principles. You know, the first, of the establishment criteria and the second, the targeting criteria. Let's start with this establishment criterion. Stephen, what is this?

Steve: So Article 3(1) lays out the establishment criterion and it says that the GDPR applies to the processing of personal data in the context of the activities of an establishment of a controller or processor in the Union regardless of whether the processing takes place in the Union or not. So that's what we know from Article 3(1).

The recitals give us a little bit more background, and now these guidelines provide us even more information as to how to understand how the GDPR applies to a controller or processor with an establishment in the EU. So breaking this down, first, the guidelines actually remind us, which is always helpful to take a step back and ask and conduct this analysis by first asking are we talking about a controller or a processor. A company's GDPR responsibilities and this analysis of extraterritoriality hinges on whether or not the company is acting in the capacity of a controller or processor and that sometimes is a complicated question.

But addressing that first, the guidelines then instruct that we are to then address whether there is an establishment in the Union. And what does this mean? Well, Recital 22 talks about an establishment as being one that implies the effective and real exercise of activity through stable arrangements regardless of legal form. Well, what are stable arrangements? The guidelines further explain that this is a very fact-specific analysis. Both the degree of stability of the arrangement and the effective exercise of real activities in the state are to be taken into account. So, could one single employee or agent of a non-European Union entity be sufficient? Maybe. That's actually one of the examples that the guidelines gives us as this could be sufficient and it's not necessarily tied to any particular legal form.

So figuring out whether you have an establishment can be particularly tricky for internet businesses and, you know, and companies that sell services online. But one of the things that the guidelines does help us with it eliminates the idea that just because your website is accessible in the EU, that's not enough to create an establishment there. That's something that the guidelines definitely answer in the affirmative.

It's also important, and just before we move on to the next point, that there must be a connection. The guidelines talk about, in the context of the activities of an establishment. So in doing conducting the analysis under establishment, there must be a link between the processing and that establishment.

And then the guidelines then talk about the case law and this is where the EU case law kind of comes in and adds additional flair. In particular, the Google versus Spain case, and that that case is important as the guidelines instruct because the connection between the processing and the establishment can even exist if the local establishment is not taking a direct role in the data processing itself, which is pretty significant.

Jack: And I want to, Michael, I want to go back to this idea that Steve talked about where under certain circumstances a single employee would be enough to find an establishment. How do you think that's going to play out?

Michael: Yeah, sure. Yeah, it's important to think about it. I mean let's say you're an academic medical center or a hospital system. If you have just one employee residing in the EU who is promoting consults toward EU markets you might be making yourself an establishment. Oh hey European Union residents, we have really expert cancer docs here. You can get a consult

from them without coming and having to visit the U.S. If someone is established, if someone is in the U—EU promoting those consults, that could be enough.

Same goes for an investment advisor. If there's one person in the Union soliciting investors, even that by itself could be enough. The examples in the guidelines make this clear. In this case I think it's example two. But in general I, you know, frankly it's worth pausing a little bit to talk about the examples and the role they play in the guidelines. They seem, actually, quite important for cashing out what the guidelines mean. You can tell because they keep using this Latin term, in concreto. It's like five times in the document. Elegant? It's a little goofy, frankly. I mean, when I googled this I found it mostly popping up in Immanuel Kant's Critique of Pure Reason, so this is not exactly the kind of thing that you see in U.S. regulators guidance, but we're in Europe and it's there. And in concreto serves a purpose. It tells you that the analysis will be concrete, tied to verified facts, and crucially on a case-by-case basis.

So, a lot of this analysis is just not about bright-line rules. It's about context and the totality of the facts. Even where they say oh, this one factor by itself is not enough, they can still use that factor as part of their contextual analysis to say you are in fact an establishment.

Jack: Right so, you know, Steve, another aspect of this establishment prong is that if you are an establishment it doesn't matter if it's you, resident data or not. Can you unpack that a little bit?

Steve: Yeah. This is a big distinguishment between the establishment prong and the targeting prong which we'll get into in a second, but the establishment prong applies no matter where the data subject is and this is really illustrated in example four in the guidelines. This is the example of a French company that developed a car sharing application exclusively to customers in Morocco, Algeria, and Tunisia. And the service is only available in those three countries, but all the personal data is being processed and carried out by the data controller in France. At first, you would think, you know, there's no European residents involved no citizens so this can't possibly apply. Wrong. Under the establishment prong three—Article 3(1) this French company will be required to comply with the GDPR.

We also know from the guidelines that the place of processing is irrelevant. We already knew this, but what we didn't know for sure is whether an EU processor working with a U.S. controller is required to comply with the controller requirements too. And these guidelines clarify that that is not the case.

But note, if you're a, if you're a U.S. processor working with an EU controller, for example going back to example four, if you're a U.S. processor working with that French company that it has developed a car sharing application the GDPR technically does not apply to you. However, the guidelines say that some of the GDPR will indirectly apply through contractual arrangements under Article 28. While those may not already be in place we suspect that in light of these guidelines we'll see more of these in the future, these data processing addendums to contracts.

Jack: I think as we, sort of, wrap up the discussion of establishment there was one, I remember sitting at thinking, wow this is, this is a gift that the Board is giving to EU-based data processors. So the flip of the example you just gave, Steve, where you have a U.S. or Mexico or Canada-based controller, which otherwise does not have an establishment in the EU who wants to hire an EU-based data processor. Right? The act of hiring an EU-based data processor does not make the U.S.-based controller subject to the GDPR.

And I have to think that's simply the practical reality of, you know, the EU-based data processors are growing in size as a result of the GDPR and if you had made, I think there could be a good argument, right, that a U.S.-based controller that avails itself of an EU-based data processor and sends all it's, you know, PII over to have this done in France, you know, would be subject under the establishment provision. But this guideline clearly says it's not. I think that is the, example seven which uses a Mexican retail company that happens to use an EU-based processor is probably the clearest example of that in the guidelines.

Alright, so Michael, let's talk about the second of the two criteria the targeting criteria.

Michael: Sure. Well, even if a company is not an EU establishment it can still be subject to the GDPR if it is targeting people in the Union. So, the targeting criterion is about behavior of the company not always its location. There are two kinds of targets, offering and monitoring. So offering is about offering goods and services to people in the Union. Monitoring is about monitoring a person's behavior in the Union. That second term, I think seems a little odd on the first reading, but those who spend time with the GDPR are probably already aware of it and the guidelines clarify it. They give an example of a marketing company that analyzes customers' movements in a shopping center. Let's say those movements are collected through Wi-Fi tracking. So that is monitoring behavior and the company may be in the U.S., but the behavior that it's monitoring is happening in the Union.

In any case, whichever kind of targeting is going on here, targeting applies to any natural person in the EU, any flesh-and-blood human being. Doesn't matter if it's not an EU citizen or the person is not an EU resident. So, if there's a U.S. startup that has an app that's designed for U.S. residents to use when they're visiting Paris or Rome, then the U.S. startup is targeted in the way that the guidelines describe. Why? Because that company is intending to process data about the location of natural persons at a time when they are in the EU.

There's some good news here though. As you can see, the way I'm putting it there's a kind of intent, or purpose, or foreseeability analysis going on here. And that puts some limits on how far the arm of the GDPR can reach. You can see this

in example 9 of the guidelines. They explained that if a U.S. news app is exclusively directed at the U.S. market, it doesn't matter if a U.S. tourist checks the app on her European vacation. In that case the GDR—GDPR doesn't apply because the app isn't directed at the Union.

Jack: Stephen, in Michael's example about the app sales, you know, at the moment that the sale occurs it's clear that it's going to be used and only used, right, in an EU environment so there's a good, there's a good intent. But when does, when do these guidelines say that intent, or however you want to describe it, what, when is it triggered? When is it measured?

Steve: Yeah, Jack. The guidelines actually help us understand what is the triggering event for the analysis and they say that it's, that when you're, whether you're targeting depends on the moment of offering the goods and services.

So let's return to Michael's example. I believe it was example 8 in the guidelines. While the company, the U.S. company, could say it only intended to target U.S. residents while they were stateside, perhaps this is where they were going to download the app they were going to use abroad, the moment of offering goods and services actually happened while they were abroad and started using the app. That's when the data was starting to come in and processing started taking place.

I also want to, let's go into the website examples that are given in the guidelines which I thought were really helpful. So the first is example 12. We see a Turkish website that creates prints, photo albums, and sells them to various countries in the EU. So what did we know before in recital 23? We knew that there were certain factors that the GDPR looks at, that the regulators are gonna be looking at to determine the intent to target to offer goods and services and the EU. What are some of these examples? Making websites available in EU languages, accepting EU currency, indicating delivery in an EU country. The more countries you deliver, the more likely it's going to apply to you and that goes back to Michael's comment about being, this being an in concreto analysis.

So what does the, what do the guidelines add? Well, they dive again back into the EU case law and they help us understand that there are some other factors that may be at play.

One of those that really stuck out to me, that I thought was interesting, is where a website uses a search engine to optimize its ability to offer good services in an EU country. You wouldn't think that a regulator would be looking at something like that, but in fact, they are. And so it's very important to be looking at indirect touches and putting kind of everything on the table when talking about targeting, intent to offer goods and services in the EU.

So, you know, going back to my, that example 12, just having a website, accepting EU currency, and indicating delivery in the EU country was enough for the Board to say that the GDPR applies to that country. And I also wanted to note example 13 which was an interesting example. This is about the private company in Monaco processing personal data for employees for the purposes is just issuing salary, issuing checks, and a large number of those employees reside in Italy in France.

So, at first this was like, oh, naturally the GDP has to apply this country. But when you, when you disciplined—take the analysis one by one. Let's look at establishment. Well, this country is in Monaco. It's outside the EU and so, the GPR doesn't apply under the establishment prong.

Then let's go to the second prong, which is targeting, well, the guidelines now help us understand that offering goods and services doesn't include paying salary, which is a big deal for some companies that, you know, perhaps they have employees that also reside in the in Europe. So that's kind of another helpful guideline or another example in the guidelines.

Jack: I mean, there are, there are 20 examples in this, in the guidelines and you really could make them into flashcards where the factual light on the front of the card, right, you could put the factual prompt and on the back of the card the answer. I think I would have gotten maybe 18 out of 20 right but that was one of the ones I would have gotten wrong.

I would have thought that if a non-EU country had employees that were EU employees and they were tracking their data as employees, including pay stubs and whatnot, that they would have to be subjected to GDPR. But it's, when you break it down by the two criterion that the guidelines discuss it does become evident that they're not. Right?

Steve: Right. And it's al— it's important to note that the guide—the example is very clear. It was about processing for purposes of salary. Right? So you can imagine there's a number of examples where that company could maybe do something else with data of their own employees and then start offering goods and services within the scope of that prong.

Jack: And I think that next example, which is exhibit, example 14 talks about a Swiss company, actually a Swiss University, and again Switzerland, not in the EU, but because it's adjacent to the EU a lot of Swiss companies and entities are gonna have to deal with some tough questions.

And the example of the Swiss university is pretty important to our practice. We've been advising a fair number of private schools and colleges on the application of the GDPR. And it's tricky, but under the targeting prong the example gives, you know, if the Swiss university has a master's degree program, it has a website for it, it has it in the Swiss languages that, you know, just German and English, and it accepts payment only in Swiss currency it's not necessarily, probably not going to be found to be targeting. Right? Because it's just a passive, they're willing to take someone from the EU, but they're not targeting the EU.

But the example 14 gets tweaked a little bit at the end where the Swiss University starts offering summer courses and takes out ads or otherwise advertises in German and Austrian universities trying to solicit students within the EU directly. And in that case, it's gonna be found to have targeted and it would apply. You know, a third piece of this with the universities that

we've seen a fair amount is, you know, if universities in the U.S. or elsewhere not, outside the EU, keep admissions officers, you know, in satellite offices or on the road in EU trying to drum up applicants from the EU, you know, there's going to potentially, there's going to need to be an establishment analysis as well to see if, you know, those employees who are working on behalf of the non-EU universities in the EU, you know, end up subjecting those universities to GDPR.

Alright but what, so what happened, Michael, what happens here in that kind of a scenario where, let's say you're a university like you are in exhibit 13 where you're not established, you don't have an establishment, but you are doing targeting? What do you have to do?

Michael: Well, okay. So you're targeting, you're covered by Article 3(2), at a minimum, you've gotta designated representative in the EU. You know, there are some things that ease this up a little bit because an entity with an establishment can take advantage of the one-stop shop mechanism in the GDPR and doesn't need to separately designate an Article 27 rep, but here we're talking about companies that aren't establishments but they followed their targeting, they've gotta have a rep in the Union.

The good news is the guidelines do mention there isn't some weird catch-22, the act of having a representative doesn't actually convert you into an establishment. But you gotta have one. And the representative has to be different from your data protection officer. Your DPO can't be the same person and they're envisioning somebody who's more, a DPO has to be more independent than someone who is representing you.

Steve: You know, one of the other things that stood out to me and the guidelines is that the regulators are, or the Board, is telling us that when one of the requirements in the GDPR is that you identify your Article 27 representative that Michael was just talking about. And, you know, when we're doing these privacy policies for clients and, you know, one of the things that we need to, it's all about transparency and being transparent includes identifying ways in which you can contact representatives. So, the fact that the regulators are telling us, you know, make sure you also include this in the privacy policy, that's a reminder that the regulator's gonna be looking for that in reviewing privacy policies for companies.

And so, that's just a, you know, in the very beginning of the guidelines the Board says that once the GDPR applies, all of it applies and it's very—this is one of the sticking points is that Article 27 representative designation for those who fall under that targeting prong, it's a challenge but if at the end of the day you reach the conclusion that the GDPR applies under that, Article 27 comes with it under, you know, minus exceptions that that Article talks about, but for all intents and purposes Article 27's trigger.

Jack: But that's good. I mean that, when you go through the guidelines, I like to think, okay, what am I adding to checklists that I have in place for incident response guides. What am I adding to checklists that we have in place for privacy policies? And certainly listing your Article 27 representative is now gonna be added to everybody's checklist about your privacy policy. You gotta put it there because it, you know, with these guidelines it almost makes it seem like if you don't have it there to be in trouble and it's something that they couldn't have been more plain about.

Michael: Yeah, and it's an easy thing to cite people for. It's black and white.

Jack: Well, wanted to thank Michael Jaeger from our New York office, who's a shareholder does a lot of cybersecurity work, and we've got Steve Blickensderfer from our Miami office, who does quite a bit of privacy and GDPR counseling. Thank you, Michael and Steve. And I'm Jack Clabby, shareholder in our Tampa office, works on a number of data breach incident response matters. Thank you all for joining us.