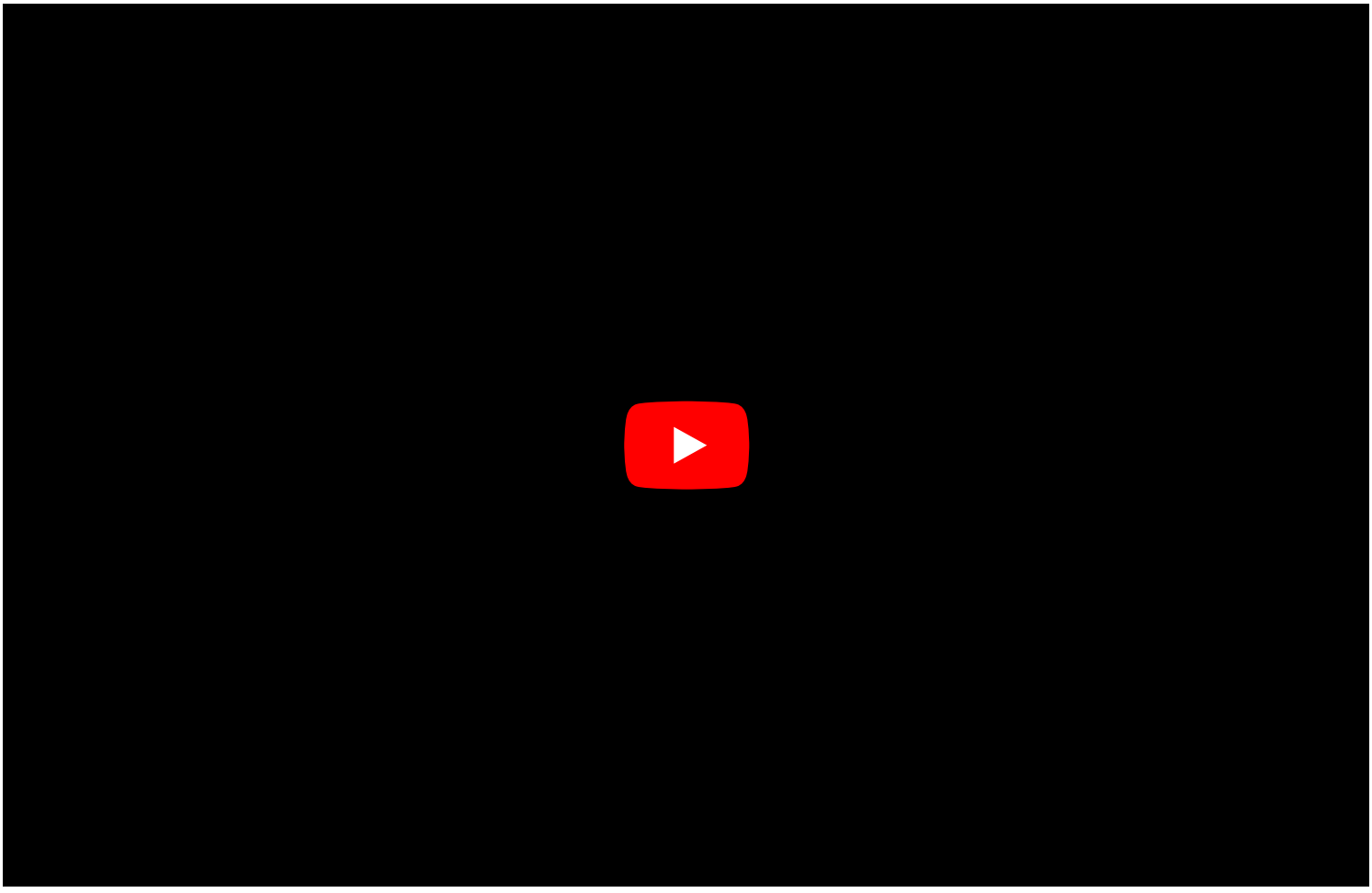
CARLTON FIELDS

CF on Cyber: GDPR Regulator Takes Narrow View of "Contract" Basis for Processing Data

April 26, 2019



Under the GDPR, businesses need to specify their basis for processing personal data, and the European Data Protection Board has recently released guidelines (2/2019) that take a narrow view of the "contract" basis for processing under Article 6(1)(b). Join Mike Yaeger and Steve Blickensderfer

as they discuss these guidelines and how they affect compliance for US-based businesses.

Transcript:

Steve: Hello, and welcome to another episode of CF on Cyber. My name is Steven Blickensderfer. I'm an associate at the firm's Miami office in its Data Privacy and Cybersecurity practice group. I am joined today by Mike Yaeger, shareholder in our New York office. Mike, why don't you introduce yourself?

Mike: Thanks, Steve. Well, I help companies and individuals with sensitive problems with the government and private parties. I focus on cybersecurity and white collar matters, and have ever since I left the federal government where I was a prosecutor.

Steve: Excellent. Thank you, Mike. So, we're going to be talking today about guidelines that were recently issued by the GDPR's lead enforcer, and that is the European Data Protection Board. We've talked about their guidelines before in a past episode. We talked about the extraterritorial reach of the GDPR that was a very important one for US-based businesses.

This is an equally important one in our eyes, because it talks about the justifications for processing. And to recap, under the GDPR there are six reasons, six bases, for processing data. It's found under Article 6. You have consent, contract, legal obligation (like you're complying with the law), vital interests (where it's necessary to protect vital interests), public interests, and the legitimate interests of the controller, where you have to balance it against the rights of those subjects. So, we're specifically talking about the second of those bases, the contract basis, and so under Article 6(1)(b), you can justify processing personal data where you need it to perform a contract or set up the contract at the request of the subject.

Another little nuance here: we're talking about this basis in the context of an online services contract. Think buying goods on Amazon.com, for example. And that is important for US-based businesses because there are a lot of companies here that operate online and that collect data from the European Economic Area. And so that's why these guidelines in particular impact businesses all over the globe and particularly in the United States.

So, we're going to shift gears now and get into the nitty-gritty. Mike, why don't you start us off?

Mike: Absolutely. So, necessity is the key inquiry under the contract basis. We're talking about the basis for collecting or processing information, personal information from a data subject. And the contract basis says that processing is acceptable when it's necessary for the performance of a contract, or for setting up the contract. For both, there's the necessity requirement.

I guess I should just give you an example of what it means to set up a contract.

Steve: I was just going to ask. What kind of contract we talking about? An online contract, like when you purchase a good online, you're a consumer, you go on Amazon, and you purchase something?

Mike: Absolutely, and the weirder thing is the setting up. I mean, the example they give in this guidance is someone entering her postal code on a company's website to see if a service is offered in the area. That's an example of something that's pre-contractual that would fit under the contract exception.

But the more important piece for most people, most companies, is about collection that actually furthers performance under a contract. And the key thing here is they're taking a pretty restrictive view of necessity, because the guidance says that a processor is supposed to process as little data as possible in order to achieve the purpose, and the purpose is the specific performance under the contract.

They also say if performance is possible and realistic without collecting the data, if there are less-intrusive alternatives, then you haven't demonstrated necessity. The processing is not necessary and you don't get the contractual exception.

Steve: Now, we see this processing, this purpose limitation throughout these guidelines, and I think that's because of one of the fundamental elements to the GDPR—that you are supposed to limit the purposes by which you are processing data. If you don't have a good reason to process it, then you shouldn't be processing the data or you should find a good reason, if one exists.

Mike: Right. This is an interesting limitation because enormous amounts of what are going to be relevant here are contracts, economic activity, and so one might be tempted to think that this would handle almost all collection issues. But as they narrow it, you see that it can't.

One example is the guidance also makes clear that a company would not have a lawful basis simply because advertising indirectly funds the provision of the service. So, if you're collecting information in order to do behavioral advertising, to advertise to people based on, say, past online purchases, that would not be activity that would fall under the contractual exception. They don't care if a company's business model is based on advertising.

Steve: And what is the reason they give for that?

Mike: Well, essentially they want this to be governed by the particular contract with the particular individual. They don't want this to be a justification on the level of a business model. These are

contracts that people just click though and come online, and there seems to be a sort of suspicion of, frankly, click-through agreements and the sorts of things that we see and don't read.

Steve: Yeah, and that's getting to a point that I wanted to raise, which is why the focus on online contracts? And I think that's because, and we kind of get the hint in the recitals and the background section is that online contracts, when you're dealing with an online website, for instance, it's a faceless company and they recognize that you don't have the opportunity as you, the consumer, to negotiate the terms of this contract with the faceless company. And so you might not realize the data that you're giving up, and the contractual basis centers on the reasonable expectations of the subject.

So often, representing the controller, that is the entity that's collecting and saying how to use data, you focus so much on your point of view. This is justified under the contractual basis because I said it is. It relates tangentially to the contract, and so that's gonna be my justification. Well, these guidelines are important because these particular examples and what we're talking about really shuts that down when the regulator is saying we will not accept that, in the context of an online services contract.

And again, as we talked about in the last podcast we had on the GDPR guidelines, these are fact-specific circumstances. So, the guidelines are just that. They're guidelines and rules of thumb for general instances. So the behavioral advertising may not work most of the time, but there could be an instance where it does work. Right, Mike?

Mike: Yeah, you're gonna have to drill down to the purpose of the particular contract. What is the bargained-for performance? And so that's different from saying why the company does this. Well, maybe the company does this because, frankly, it wants to make money off of advertising. But that's not what the data subject, the flesh-and-blood human being, is coming to the website for. And that's what they mean by looking at it from the data subject's point of view.

Steve: Right. One of the examples I love, because it really hits this point between what's reasonable necessary and what's, you know, not necessarily expected. It's actually in the first example. It's when you're shopping on Amazon and you put in your name and your address and your credit card, you need that information to process and ship the information. What if you go on website where you could go and pick up the item in store? Then the collection of your home information, to the extent it's not necessary for your credit card processing, is not necessary, and so you cannot rely on the contractual basis, basis to process that data. You would have to find another basis on which to justify the processing of the data. So, very interesting examples there.

Mike: And this also applies, this applies also to bundled services as well.

Steve: Right.

Mike: That you would need to examine each service separately.

Steve: Right.

Mike: You have to look at, okay, this service is being contracted for this reason, that's the performance under this particular one. And overall, we're just seeing that this vision of necessity, this definition of necessity, is far narrower than what you will see in other places of America Law. I mean, this is not the Necessary and Proper Clause in the Constitution. This is not John Marshall giving a broad, expansive interpretation that gives the government a lot of room to run. This is a much narrower code of conduct that they are putting on companies that operate in this space.

Steve: This is a European version of necessary.

Mike: Yes, it is not the Constitution we are interpreting here.

Steve: But it's important to realize that it is objective, and you have to consider, not only your perspective if you're the controller, but also the subject, the subject's perspective. What could they reasonably expect you would do with their data, if they either are, you enter into this contract to preform it or the steps, what you need to take to get into this contract that they request.

Mike: Absolutely, and not just what you need to get into the contract, but also what you need to get out of it. There is some guidance here also on contract termination, because the GDPR requires deletion of data that's no longer necessary for the purpose for which it was collected. So, you just have to keep track of this more. When the original legal basis is gone, the data's gotta be deleted. Now, if at the outset of the contract the user has also given consent, the data subject has given consent for the controller to use the data even after the contract terminates, well then the controller can use it.

But if your business model is going to be about the data subject's data, if it's going to be monetizing that long-term, you're going to have to think of these things at the outset of the contract. You can't simply try to backfill it at the end or come back to them for consent.

Steve: Well, you also raise another point in that these guidelines talk about the relationship between the contractual basis and the other bases. Okay, because there are five other legal bases by which to justify processing data.

So, in your example of a termination of a contract, which comes out in example three in the guidelines, that makes clear you could couple it with consent and then processing after the

termination of a contract, your legal basis is consent, assuming it meets the threshold, the heightened threshold for consent and the GDPR.

So, what we're finding in these guidelines is that contractual necessity is a tougher basis to justify processing, because if you don't meet its limited criteria, you should have, if you want to continue to process that data, another basis. And if anything, you should be, unless it's clear, like giving your shipping address to ship a product you buy online, you should double check and ask, are there other bases on which to justify this data?

And so example five really hits on that. That's when the bank asks you to confirm your identity before, either leading up to the contract, or performance of the contract, because it has a legal obligation to do that. Well, it would make more sense to justify that processing on with the legal obligation prong of Article 6, and...

Mike: Right. Then in that case...

Steve: ...the guidelines actually advised it's better to justify it on that basis than the contractual, which is very interesting.

Mike: Absolutely, and in that case, that won't sneak up on a financial institution. They're aware that they have KYC, "know your customer" obligations; they know about it.

Some of these other things make it trickier when they're not proscribed by law. I mean, a lot of the time people will want to rely on consent. The thing to remember is that the GDPR requires a fairly robust version of consent. Some of the things that passed muster in the U.S. would not pass muster under the GDPR, and as you're saying, I think this is basically the Data Protection Board's attempt to close off other escape hatches. So that, really, you can't take too much comfort from the contract exception, which otherwise might look like it would allow you to get around the more specific requirements for consent.

Steve: That's right. The regulators are smart. Let's dial the clocks back before the GDPR, we are under the Directive. And then the Directive, one of the bases that was most often used was the legitimate interests of the controller. Okay.

Mike: Right.

Steve: And in the Directive, the burden shift was not on the controller like it is now. It was, if you have a problem with it, than you have to show how the controller doesn't have that legitimate interest. But here under the GDPR, they looked at it and said, "No, no, no, this became a catch-all." And you know, the exception kind of swallowed the rule, kind of thing.

Where they now, you have to, if you're the controller, you have the burden of showing that your legitimate interests in the data override fundamental rights of privacy, and so that's a very high bar. And so by shifting that, that made parties look at it and say, okay, what are the other bases, oh you know, this probably falls under contract, because it's related to a contract. Well, no, no, no, the language of the GDPR includes the word necessary which, you know, Mike, you talked about just a moment ago.

That makes, by issuing these guidelines and talking about this, they're basically putting their thumb on this and showing that in the context of online services, in particular, because that's an area of concern, this basis is going to be looked with heightened scrutiny...

Mike: Yes.

Steve: ...along these lines in a fact-based context. So, one of the other things that the guidelines do is, I love the examples. I think the examples are great, it really brings home some of the stuff that they're talking about in these very dense guidelines. So, they talk about specific situations and they give examples for each.

So Mike, let's go through some of those. And you brought it up earlier, but let's talk a little about behavioral advertising, because there's some interesting stuff in here about that.

Mike: Yeah, I mean, I think example six talks about an online news site where it's offering a service of news aggregation, and it might require a user to create a profile of interests and personalize it so that they can get particular content.

Steve: Right, I've done that before and I'm sure you have, too, when you sign up for something and you want to get particular data...

Mike: Absolutely.

Steve: ...filtered through that way.

Mike: Absolutely, and everyone can see why that would be especially useful. I mean, perhaps the paradigmatic example would be some of these old-style dating services. Old-style meaning not Tinder swiping, but when people are putting in every possible aspect of their own personality and trying to match some completely identical mate or something. Well, personalization really is what part of what people are bargaining for in that context. So, that seems like an easier example.

Steve: Right, where the processing is objectively reasonable.

Mike: Right.

Steve: But then you go to the next example, which is example seven. You have the online hotel search engine, and it monitors your past bookings to create a profile and recommend particular hotels in your next booking experience. The guidelines actually point that out as a profiling of past behavior that is not objectively necessary under the contract basis. So, you'd have to find another basis, if you can, in order to justify that processing, one of those low-hanging fruits being consent. That makes a lot of sense.

Mike: And that's another one worth dwelling on because this is so obviously part of the business model of an online hotel search engine that is not charging you a fee to use it. How else are they making money? They are advertising and personalizing ads towards you and perhaps selling your data. And this would seem to be clear, it's certainly part of the business model, but this just shows that a business model is really not the same thing as the specific individual contract at issue.

Steve: Right.

Mike: And you cannot, a company cannot justify this entire form of operation just by pointing out that this would be obvious or implicit in their business model.

Steve: That's right, and so let's just wrap it up with some big-picture thoughts here. And one of those that comes to mind is just as you're saying, you can't just default to the contract basis as being the justification for processing data. There appears to be a push to consent, among others. But consent is probably the "chosen one" of them all because that is the one that allows, it has to be informed, it has to be specific, it has to be contemporaneous, to the time. So, if you can meet all those things, then it kind of creates this, you are allowed to do with the data what you want because at that point the individual knows exactly what you're going to do, and all is well. So, there seems to be a move towards that.

Mike: I agree, and I think that these guidelines are also showing that what a lot of us were worried about with the GDPR is slowly, inexorably coming to pass. There are ways in which this, the underlying theories behind the GDPR are going to impose costs upon the online marketplace and on the margins may push some services to charge fees as opposed to subsisting on an advertising model. Clearly, you can obtain consent, you can do this, but it is a real cost for businesses and a change in the way they have to operate.

I'd also say that because there are many businesses that have already built large networks before these rules were in place, this may have the effect of entrenching incumbents in the market place in different sectors, people who already have those networks. It may also lend some benefit to people who build networks outside of the EU before they venture in.

Clearly, there are downsides to avoiding a region of the world for a while, but it just shows that if the EU remains different from the rest of the world in this respect, it will have some interesting effects on where people want to start businesses.

Steve: That's right, because as we're seeing global data privacy laws take hold in other countries, Brazil comes to mind. They recently came out with their Brazilian data protection statute that covers all industries in Brazil and extends beyond Brazil's borders. One of the differences, notable differences, between the Brazil statute and the GDPR, is that it has different bases. Some are the same, but some additional bases for processing.

And that's a subtle little difference that can make a profound change, because if you can have a justification for processing data in one country, but you can't have a justification for processing in another country, then you might shift to that other country, depending on your business or whatever, there are lots of variables. But in a very basic sense, you would go where there is less regulation, and you know, we're having those here in the United States. The California statute is obviously the top of mind for lots of folks...

Mike: Absolutely.

Steve: ...and that doesn't necessarily have this same style of legal bases for processing, but there are impediments to doing what you want with data because now consumers have rights, because California consumers in particular where they didn't have them before.

So, it's a fast-changing world, particularly in the data privacy space, so state tuned for more. This is obviously a signal from EU regulators about this kind of processing. The justifications for processing, you have to be very particular and very careful and align yourself with folks, your team internally or externally, your legal, your consultants to the extent that you have them, they need to look at these guidelines because they are very persuasive when it comes to interpreting the GDPR.

Mike: Yes. I mean, if we're going to do privacy by design, we need the technical people to be aware of this as they're designing. And the business people, because as you were just outlining, there are choices of market that you might make. Just elementary basic business decisions that are going to be driven by these kinds of considerations.

Steve: Well, that's all we have today. Thank you so much for joining us. Thanks, Mike, for taking the time and everyone for listening. We hope you'll join us again soon.

Presented By

Michael L. Yaeger

Related Practices

Cybersecurity and Privacy
Technology

Related Industries

Technology

©2024 Carlton Fields, P.A. Carlton Fields practices law in California through Carlton Fields, LLP. Carlton Fields publications should not be construed as legal advice on any specific facts or circumstances. The contents are intended for general information and educational purposes only, and should not be relied on as if it were advice about a particular fact situation. The distribution of this publication is not intended to create, and receipt of it does not constitute, an attorney-client relationship with Carlton Fields. This publication may not be quoted or referred to in any other publication or proceeding without the prior written consent of the firm, to be given or withheld at our discretion. To request reprint permission for any of our publications, please use our Contact Us form via the link below. The views set forth herein are the personal views of the author and do not necessarily reflect those of the firm. This site may contain hypertext links to information created and maintained by other entities. Carlton Fields does not control or guarantee the accuracy or completeness of this outside information, nor is the inclusion of a link to be intended as an endorsement of those outside sites.