EP 38 - GDPR Minitraining

info@awbfirm.com

[music]

00:06 Autumn Boyd: Welcome to the Legal Roadmap podcast for online and ecommerce entrepreneurs. I'm your host, lawyer Autumn Witt Boyd. I'm an experienced copyright and trademark lawyer. With my team at the AWB firm, I leverage, grow and protect multimillion dollar online businesses. My goal in every episode is to teach you about the sophisticated legal and business strategies to build your own seven or eight figure business. If you're a new business owner, go back and listen to episodes 1-12. You'll learn the basics to set up a strong legal foundation. The Legal Roadmap podcast is sponsored by the AWB firm. You can find show notes for every episode, and learn more about how we help our clients achieve their next level goals at awbfirm.com.

[music]

00:52 AB: I'm excited to be here today to chat with everyone about GDPR. You have probably gotten a number of emails in your inbox about this. It's the EU regulation, the General Data Protection Regulation, but a lot of your service providers if you're using apps or other cloud-based tools in your business, you probably have heard about this, because it is causing a lot of changes not just in the EU, but also for US companies. So we are going to start today with a mini training on the GDPR and I'm going to do a series of four of these, so this is the first one. And today, we're just going to go over what the heck is the GDPR and who needs to worry about it, who needs to think about whether they need to comply. We are not going to get into the nitty gritty of what you actually have to do to comply.

01:39 AB: I'm just going to give a very high level overview of what the regulation is, who it affects, kind of some of the principles behind it. And then in the following weeks, we will go into the more nitty gritty of how US businesses might actually need to change their websites or change their marketing or other business practices to comply. There are two major areas where most US businesses, especially online businesses, ecommerce, the kinds of businesses that I love working with in my law firm, those businesses are going to have to make some major changes on their websites and in their marketing campaigns. So we will talk about that more next week and I'll give a little brief overview of that in a minute.

02:17 AB: But in case you are new here. Hi, my name's Autumn. I am a lawyer, I'm licensed to practice law in Tennessee. So, everything I'm talking about today is based on US law, my interpretation of this EU regulation on US companies. So I'm licensed to practice in the United States, in Tennessee. I am not an EU or UK lawyer. So, if you need that kind of... If your business is in one of those places, you may need to go somewhere else for more information. But my standard disclaimer, this is information, this is not legal advice, and this law is really complicated as you'll see when I start talking about it. So for your business, especially if you have a larger business or you deal with a lot of data that is your customers or your users, you may need to consult with your own lawyer and make sure that you are taking the right steps, get some custom advice for your business. As you'll hear, there are some pretty major penalties with this law, if you are doing things the wrong way. So we want to be really, really careful and we want to make sure we're doing the

right thing.

03:13 AB: So again, this video series, this podcast is information, not legal advice. Please consult your own lawyer, whether it's me or someone else, if you need specific advice for your situation. I'm going to just give a little background about me and my law firm since we have a lot of new faces here today. So I have been a lawyer for almost 14 years, I graduated at the top of my class from Vanderbilt University Law School. I worked for a judge, I worked for a big law firm, I worked for a small law firm. My last law firm job before I started my own law firm was with a virtual law firm, so that's what kind of opened my eyes to this world of online and virtual business. My background is both business and copyright and trademark work and my law firm, the law office of Autumn Witt Boyd, we work with primarily ecommerce and online companies, we help them with intellectual property, so copyright and trademark. We also help them with business issues. So we work on a lot of contracts, we help with negotiation, we help buy and sell businesses, we set up licensing programs, we do all kinds of things.

04:12 AB: So we try to be full service for those kinds of businesses that we really enjoy working with. So the first thing I want to mention is that the background for all of this, what I do as a lawyer is, my job is to outline what is the law, what are the rules, what do you need to know. And then I help my clients look at the pros and cons and figure out what they actually need to do. But every business is different, every business is doing different things and every business has a different level of risk tolerance. So there are some decisions that you will have to make in how your business deals with GDPR that are going to be different maybe for you than for your neighbor, or your friend, or your colleague. It really is a matter of what protections do you want to comply with and what level of risk are you willing to take if you don't comply?

04:58 AB: So it's like any other law, there are lots of regulations that people don't comply with. It is at the end of the day, your choice. So what is the EU's General Data Protection Regulation? It's complicated is the first thing it is. So this is a... It's a long document. The regulation itself is about 50 pages. The documents explaining it are another hundred pages, so this is a big, big fish to get your arms around, and we are not going to cover everything today. I may give you a high level overview of the things that I think are the most important to online and creative business owners, but there may be things that I leave out. So please don't rely on this as your 100% everything about the GDPR.

05:38 AB: Some background about why the EU put the GDPR in place. So, there were three main goals: The first was to ensure the protection of privacy rights of EU residents. So the background is really, they want to give EU residents more control over their own data and how it's used by other companies, other people. So some of the goals were security, confidentiality, notice about how it's going to be used, having a choice about how your data is used, having the right to access your data even if it's held by a third party, how to change it or have it deleted if you don't want anyone to hold it. There's more than that, but that is a good background for you to think about as we're talking about GDPR.

06:16 AB: They also wanted to update the privacy laws because they were just out of date. Over the last 20 years since the prior biggest change, a lot of technology had changed. So they are wanting to update the privacy laws so they keep pace with technology. And then the third one was just

standardization. Right now, there are 28 different privacy laws in the EU. So this is kind of going to make everybody have an equal playing field, it's going to make it much easier for people to do business in the EU. These were actually passed two years ago, so everybody's had two years to get up to speed. But a lot of the guidance has come out more recently, and I think businesses everywhere have been kind of scrambling a little bit to figure out how to comply with GDPR, do they need to comply with the GDPR, especially if they're outside the EU. So, if you are feeling overwhelmed, you are certainly not alone. Even in the EU and the UK, and I should be clear, this does apply in the UK, even though they are in the middle of exiting the EU, a lot of those companies in those places are scrambling a little bit too.

07:13 AB: So here is what I really want to spend some time on today. Who has to comply with GDPR? Again, there is no one answer that is right for every company. But in my reading of the law, I think this applies to virtually all US businesses who have a website. The GDPR says that it applies to any business anywhere that processes, so processing is the keyword, processes any personally identifiable data that is related in certain ways to EU residents. So processes is much broader than you might think. So it includes collecting data, using data, storing data, or receiving data. So even if maybe you didn't get data directly from the person in the EU, if one of your vendors did... And I'll give this example that we thought of. Let's say you're a restaurant and you're using OpenTable to collect reservations for your restaurant. So you're not directly collecting the information on that reservation which usually will include a name, a phone number, maybe an email address. OpenTable is actually doing the collecting, but they transmit that to your restaurant so that you can know who's coming to dinner. So you're receiving that information from a third party but you still have to comply with the GDPR, with any data that you are now holding, that came from an EU resident.

08:32 AB: And the important thing here is it's going to apply to data that came from someone who's sitting in the EU. So it's not necessarily are they a citizen of the EU or do they even live there all the time, but it is were they sitting in the EU when they transmitted the data? So I hope that you're starting to see that this law is really, really broad in how it applies and it has lots of tentacles that are going to reach lots of different businesses. So we've talked about processing. That was the first thing. What does it mean to process data. The next thing I want to talk about is personally identifiable data. So that is what is an issue. So the examples here are things that I might not think of as necessarily personally identifiable data, it's also very broad. So it could include a name, a photo, an email address, your bank details, but also your posts on social networking websites. Your medical information is obviously very private and personal, but it's also going to include things from which your identity can be derived. So your IP address, which if I look at it, it's just a string of numbers that means nothing. But you can use that to eventually get to someone's identity.

09:39 AB: So even an IP address, if that is something that your business is receiving from someone who's sitting in the EU, so that means they were coming to your website, you now have to comply with the GDPR in how you handle that data. So my understanding after looking at this is nearly every US business is going to need to comply in some way. Now, the good news is, it's not that hard for most small businesses. I think there's a lot of anxiety, and a lot of, "Oh, GDPR is coming, I'm not ready." You're not alone. But also, there's some steps you have to take if you want to comply, if you decide to comply, but they're not that big a deal for most small online ecommerce businesses. Now, if you're a larger business, if you are running an app or if you have a SaaS, Software as a

Service company, if you are a social media company, if you're doing much larger processing and holding of information, especially really sensitive private medical information, you are going to need to take a closer look at this. What I'm talking about today is most of my people who are selling services and products online or maybe in a shop on a pretty small scale. So all of my recommendations are directed to that kind of business.

10:52 AB: So for that kind of business there are some things, some steps you need to take and some changes you need to make, but they're not quite as dire as I think a lot of people have been talking about. So looking at this, when we are talking about any business that processes personally identifiable data from EU residents, I think there are two categories that we can think about of who needs to comply. So the first category is, are you selling goods and services directly to EU customers? And that can include giving them free things.

11:21 AB: So a lot of my online business friends have what we call an opt-in on our websites. I have one on mine. If you go to awbfirm.com you can see it there on the front page. This is where we offer something of value in return for people giving us their email address, and then we put them on our email list. So, they now get newsletters or they get marketing materials, they get offers from us. This has kind of been standard operating procedure for many years in the online world. Again, this is something called an opt-in, some people call it a freebie, or a downloadable. There's lots of different things that these are called, but no matter what you call it, [chuckle] this idea of you give me my email and I will give you something of value. And it often is a workbook, or a PDF, a worksheet, it might be a short course, so you might send them a series of emails, or you might invite them to a private Facebook group. There can be all kinds of things that you're exchanging in exchange for their email address.

12:16 AB: Under GDPR, if you are offering that to people who are in the EU, even if it's for free, so you're not taking their money, there's no monetary transaction going back and forth, but you're giving them something of value, they're giving you their email address, you now fall under the GDPR, because you are offering goods and services directly to EU customers and they are providing you their personally identifiable data. So if you have even one EU person who is sitting in the EU and giving you their data, if you have even one person who has done that on your email list, you now fall under the GDPR. So I think most of us likely are going to fall under GDPR. That's the first category. Pretty clear. If you have one person on your list, if you have shipped one product to someone in the EU, if you have provided services, if you have a client... I have clients in the EU. [chuckle] Even though I'm a US lawyer they've hired me to help them with US legal issues. So it is very broad in its application, and I think a lot of us who are doing business online, unless we have been turning away EU residents, we likely are in this first category where we very clearly have to comply with GDPR.

13:29 AB: The second category of people is a little more gray. So this is, you are located outside the EU, so you're a US business or you're headquartered in the US, you're not targeting EU customers, you maybe don't have anyone from the EU on your email list, you haven't had any transactions with them whether they're free or paid, but you may be interacting with EU data. And this is much less clear. You'll see me, I've got some notes on this because this is a really tricky issue.

13:56 AB: The thing to think about here is, a lot of us when we're trying to figure out have we interacted with someone in the EU is we might rely on their IP address. You can do what's called geolocating based on an IP address. The problem with that is that it's not going to be 100% accurate. I think if you dig into this at all, you'll know that lots of people spoof IP addresses. So they're bouncing it around, their IP address is not accurate for where they're actually physically sitting. So we've got a problem with using that kind of data to figure out do I need to comply with GDPR. It's probably not going to be accurate. The second thing to think about is the GDPR actually contains a special rule saying that you cannot profile people based on where they're located. So this means you cannot set up your website so that you are blocking everyone from the EU, which I think is a common immediate reaction that people have had. They'll just say, "Well, I don't want to comply with GDPR, so I am just going to make my website so that it doesn't interact with anyone from the EU." That blocking of EU visitors based on their IP address, this is profiling, that in itself is going to violate the GDPR. So we're kind of in a vicious circle with that one.

15:12 AB: The other issue is that you really don't have a way of knowing where someone is physically located when they're interacting with your website or sending you data. So I could be on a business trip to Paris, which I hope to do before too long. I mean, right? Wouldn't that be amazing? And I could be catching up on some work there, I could go to a US website as part of the work that I'm doing and I could enter some data. I'm sitting in Paris, but if they ask me... Another option that a lot of people have said is, "Oh, well, I'll just have a check box and ask, are you located in the EU? And I'll treat them differently." Well... Or, "Are you a resident of the EU?" I would click "No" to that. I'm not an EU resident. But if my computer is physically sitting in the EU when I'm transmitting that data, now I'm under the GDPR. So that is not going to work. You can't necessarily trust someone when you're asking these questions, and you might be asking the wrong question.

16:04 AB: The other thing to think about is, we have this issue of data that is anchored in the EU and this is a really open question, it is unclear at this time since GDPR has not even gone into effect, it goes into effect May 25th. I'm recording this on May 9th. So we haven't actually started yet. It's unclear to me and the guidance is very unclear at this point about data that's anchored to the EU, but that may be used elsewhere. And I'll give an example about this. So, how many of us have had the same cellphone number that we had in college, or that we had in the city where we first lived when we had our first real job? But we've moved states maybe three times but we've still got that cellphone number with that area code that would seem to indicate we live somewhere else. So think about that as like data being anchored in another state. The same thing could happen in the EU. So we could have a phone number or an email that was started in one place in the EU and now maybe the person lives outside the EU. But there's a question about whether that data is still anchored to the EU.

17:02 AB: Another example that I'll give. I live in Chattanooga, Tennessee, beautiful city. We have a lot of large manufacturers here that are headquartered in the EU. So we have a big Volkswagen plant, we had a big Volkert plant. Their headquarters are in another country, in the EU. There's, I think, a fair question about whether data that is being processed, like let's say an employee is using their employer's email address to transmit data. Is that data tied to the EU? These are all open questions. So when we've got a really gray area like this, I think that the best thing to do is just to presume that if you are interacting with anyone online, there is a pretty darn good chance that you are interacting with someone in the EU, and you just go ahead and assume that you have to comply

with GDPR. I think if you're trying to split hairs and segment and treat some people this way, and some people a different way and, "Oh, I'm going to treat US people this way, but I'm going to segment out the EU people and only do the higher levels that are required with them," I think that that is really risky.

18:05 AB: Again, you get to decide for your own business how much risk you're comfortable taking. But I want to move on to my next segment, which is on the penalties. Because as you are figuring out what kinds of risk you're willing to take, I think it's important to know what is the potential downside. So, with this, we've got some pretty big potential downsides. So the damages are up to 20 million euros, 20 million euros, or 4% of a business's gross annual worldwide income, whichever is higher. So I've heard a lot of people say, "Well, 4% of my income is not that much. I'm totally willing to take that risk." No, no. 20 million euros or the 4% of your income, whichever is higher. And I think what we'll see in the way the law is written, there will, of course, be a range. I mean, if I violate GDPR, the chances that they are going to fine me 20 million euros are very, very small. It's going to depend on what was the consequence of me failing to comply. Was very personal information disclosed? Was anyone damaged? There's going to be a range of different things that can happen that are going to affect what kind of a fine is issued, or penalty. But you should just know, that's a lot of money. And so, as you're thinking about, "Should I comply? Should I not?" I think that that is really important to consider, that these are some pretty darn big damages, and I want you to know about that.

19:28 AB: The second thing I want you to know about the penalties. I've heard a lot of people say, "Well, there's no way that Germany is going to take the time and energy to come after my teeny-tiny business." And that may be true. We don't know it yet. But this law has a private cause of action. So what that means for those of you are not lawyers, is that an individual can sue you. It's not just that a country or a regulatory agency or some kind of governmental entity could sue you or come after you for penalties. An individual can sue you.

19:58 AB: So, the scenario that I think would most likely happen where a US company could get sued for violating GDPR would be a big data breach. So let's say someone has submitted their information to you, your systems are not secure or one of your vendor's systems are not secure and their personal information is all of a sudden disclosed and maybe they suffer some damage, maybe their identity is stolen and they've got tons of debt racked up against them, or, you know. Who knows? All kinds of terrible things can happen when you have a data breach. So I think that that is likely what's going to happen. There's going to be a data breach and then the people who were damaged are going to follow the rabbit hole and try and see, "Well, how was my data involved in that data breach?" And they're going to end up with you if you're the person that they submitted the data to and the data breach flowed out of you either not having secure systems, or one of your vendors not having a secure system. So this could be somebody like your email provider, or your credit card processor.

20:51 AB: Just start to think about how all of these tentacles are starting to go. I think that is what would likely happen. That an individual will be damaged and then they would sue everyone who touched their data. And it's going to start with you if you were involved. So how likely is it that you will be sued? I don't know, we don't know yet, we probably won't know for the next five, 10, 15 years. But what I will tell you, and what I've told my clients is, I don't want you to be the test case.

You know, I've gotten lots of questions about, "Well, how are they... Legally, how are they going to come after me in the US if they're located in the EU?" I don't know, it's very unclear. I've done some research, we don't know yet. But I will tell you they are going to try because on the EU GDPR website, it specifically says the GDPR not only applies to organizations located within the EU, but it will also apply to organizations located outside of the EU if they offer goods and services to monitor the behavior of EU data subjects.

21:49 AB: So they're being very clear, they're saying, "We are going to go outside of the EU to go after people for this." Like, "You are on notice." They go on to say it applies to all companies processing and holding the personal data of subjects residing in the European Union regardless of the company's location. So this is very important. They are wanting to stretch outside of the EU. So this penalty could come and get you. Again, this is a matter of risk tolerance. How much risk are you willing to take? I think it's pretty serious.

22:20 AB: So I'm going to just quickly wrap up, 'cause we've gone on for a little bit, with just a brief overview of the changes that the GDPR is going to bring into effect for all businesses. Now, some of these may apply to you or may not, but this is just a general overview. So the first thing is that getting someone's consent to use their data, or hold their data, or process their data, or give their data to someone else, anything you're going to do with their data, consent now requires affirmative action. So if you are gathering emails through an opt-in, like we talked about at the beginning, you now have to ask them to agree to be on your newsletter list, if that's what you're going to do. If you're really just going to send them the thing that you promised them in order to get them to enter their email address, the free workbook, or the training, or whatever, then you don't need affirmative consent.

23:10 AB: But if you're going to do anything else with their data after that point, if you're going to market to them, if you're going to put them on your newsletter list, you must get their affirmative consent. This consent has to be freely given, specific, informed and unambiguous. So we're going to talk about that more probably next week when we go into some of our case studies and examples of what you need to do if you decide to comply with GDPR. But the key here is you have to tell people all the ways you're going to use their data, you have to get their affirmative consent. So a pre-checked box is no longer okay saying in your terms of conditions that so long as you use my website you agree to all these things. That's no longer okay. And where you're doing more than one thing with their data, you have to tell them all of it, upfront.

23:51 AB: The second thing, second big change, is that if you use cookies in your business and if you are not techie like me, you might not know what a cookie is. I found out recently when I was doing all this research that a cookie includes the Facebook pixel and includes Google Analytics. So it's anything, a little piece of code on your website that then tracks visitors to your website. It puts something on their browser that then tracks when they move around after they visit your website. So if you're using cookies, now you have to get people's affirmative consent to do that. So that is brand new. You may have seen these new cookie notices, banners, or pop-ups on websites. That is what that is. We're going to have to make some changes there if you're using cookies.

24:33 AB: The third one is, you have to tell how you're going to use the information in the place where you collect it. So you're now going to have to link to your privacy policy... Well, first of all,

you're going to have to have a privacy policy. Hopefully, you all already have privacy policies 'cause it's already required by California law. But you're going to have to link to that privacy policy. It's going to have to be a lot more visible than just hidden in your footer where most of us have had it. And you've got to have some very specific things now in that privacy policy to comply with GDPR. And yes, if you're wondering, we do have a privacy policy template that is GDPR compliant. If you go awbfirm.com/GDPR, you can link right to it. So that is available. But that privacy policy is now going to have to be linked on all of your opt-in forms, if you have a Contact Us form, if you are providing products or services and you have a check out screen that's going to have to be linked there, it's going to have to go in a lot of places.

25:21 AB: The fourth thing, you have to keep all the data you collect secure. It can be proportional to how private the data is and what potential issues. So I don't have to, with my law firm. Well, I'm a bad example because my data is pretty personal and private. But let's say, a life coach doesn't necessarily have to keep everything quite as secure as Facebook does, or as a bank does. So, it is proportional to what you're doing. But you do now have an affirmative responsibility to handle data securely. And you have to limit the access to it to those who really need it for a business purpose. If you do have a data breach, you have to notify the Data Protection Authority within 72 hours and inform all affected parties. So that's a new thing. There are a lot of new rights for EU residents. Now they can request their data from you, you have to provide it. They can ask you to erase their data, they can ask you to correct their data if it changes or if they think you have it incorrect. And there is a new right to withdraw their consent for you to store or use their data. So it has to be really easy for people to tell you, "I don't want you to hold my data anymore."

26:26 AB: The next one is privacy policy. I touched on this before, again, just going to give another plug, awbfirm.com/GDPR, and you can find our GDPR compliant privacy policy right there. There's some new required information in your privacy policy. So you're definitely going to need to update that and link it in lots more places. These last two are really going to apply to bigger companies. So if your company is really data-centric, if what you do is collect and process and gather other people's data, so I'm going to give Facebook as another example. All they do is help people... They say they help connect people but what they really do is process people's data, hold it, organize it, let people use it to communicate. They have to appoint what's called a data protection officer and there are a lot of requirements with that. And again, for data processors, and there's a specific definition of that. Most of you guys are probably not this, but I just want to let you know, you also are going to have new obligations.

27:18 AB: The last thing I want to just hit on is that the other thing that's really important here is that your business could be sued, could have to pay damages, could have penalties if your vendors or your providers that are handling data that your customers give you, if they are not compliant. So let's say you are using an email provider. I use ConvertKit. A lot of people use MailChimp or Mailerlite. There's lots of different providers. If they are not GDPR compliant and there's a breach and something goes wrong, or if they're just being annoying and they're not following the rules, they're sending emails that they shouldn't be. That could come back on you. So that is a big problem and you are going to have to be a lot more careful now vetting your vendors. And if you're a bigger company where you actually have some negotiating power and you're negotiating contracts with your vendors, this is definitely going to be an area where you're going to want to negotiate liability and indemnification protection. That's something that I do with my larger clients, where they have

some negotiating power with their vendors, we want to make sure that they are responsible for their own compliance. Because it could come back to me. I don't want that to happen.

28:20 AB: Okay, I have given you a lot to chew on, hopefully, and if you have more questions after you listen to this podcast, or watch my Facebook live, please, please, please leave them in the comments or shoot them over to us at awbfirm.com, you can use the contact form to get in touch with us there. And you may notice, depending on when you are going to our website, not all of our website is GDPR compliant but we are in the process, we will be compliant before May 25th, and I'm going to do these trainings on Facebook all week. We're also hosting a live GDPR training on Tuesday, May 15th at 12:00 PM Eastern Standard Time. So if you're listening before that, you can go sign up at www.awbfirm.com/GDPRtraining. All one word. Thank you so much for joining me today, I look forward to speaking with you next time with more helpful GDPR tips. Thanks, guys.

[music]

29:20 AB: Did you know that you could be making more money from your copyrights and trademarks? Intellectual property is probably the most valuable asset in your creative business, but most entrepreneurs don't know how to identify it. And you can't monetize what you can't find. Download my free five-minute IP audit worksheet at awbfirm.com/podcast. You'll find out what parts of your brand, logo, images, website, courses, digital downloads, or other content could be protected by intellectual property laws. And you'll create an inventory of your most valuable trademarks, copyrights, patents or trade secrets, so you'll know what's worth protecting as you build a more profitable and sustainable business. Get your five-minute IP audit worksheet now at awbfirm.com/podcast.

[music]