

EP 39 - GDPR Minitraining 2 Email marketing

info@awbfirm.com

scribie

Audio Transcription, Perfected

<https://scribie.com/files/57f6c10230714e2794b3500c07f599c1b96e31ba>

[music]

00:06 Autumn Witt Boyd: Welcome to the Legal Road Map 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 through 12. You'll learn the basics to set up a strong legal foundation. The Legal Road Map 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: Glad to see you guys here. So, I am not going to go back and cover everything that I did last week in the GDPR Minitraining number one. So if you want to know more about what it is and who needs to comply, definitely go back and listen to that. It is in my Facebook page at facebook.com/autumnwittboyd. You can also find those on our website at awbfirm.com and their podcast, that's Episode 38. So, go check out Legal Road Map podcast 38 if you want all of that juicy info. I'm gonna give just a really quick overview so that if you don't have any idea what I'm talking about, this will at least make sense. And then we're gonna dive into what is affirmative consent under GDPR and how that means some of us are going to need to change, what kind of opt-in forms, or contact forms, checkout forms that we're using. Any time you're gathering information on your website, how does the GDPR affect that?

01:44 AB: So let's dive in. Alright. Minitraining number two on GDPR. So, what is GDPR? Going back just briefly, this is the EU General Data Protection Regulation. It applies throughout the EU starting on May 25, 2018, and it also is going to affect a lot of US businesses. So if you are interacting with any EU residents or even with United States residents who may be sitting in the EU while they're transferring data to you, you likely are going to need to comply with the GDPR. Go back and listen to podcast Episode 38 or my first minitraining on Facebook Live if you wanna know more about who needs to comply and why that's important.

02:25 AB: As I mentioned in the first minitraining, trying to opt-out of compliance for US companies with technology is not a perfect solution. You are still gonna have some risks there, even if you try to say, "I'm not going to interact with EU companies or people, or trying to treat EU data differently, trying to use IP addresses or other ways to geolocate and block people from your site." Those are all risky choices. They are actually prohibited by GDPR, and there are pretty stiff penalties. So, if you are not complying with GDPR, you risk a €20 million fine. That is huge. Or 4% of your business's gross annual worldwide income, whichever is higher. I know 4% doesn't sound like much, but it could go up to €20 million, whichever is higher. It's pretty stiff penalty. So I think this is something we should all be taking seriously and paying attention to because the risk is pretty darn great.

03:16 AB: Now, I went over all of the major changes that GDPR is going to bring into effect. But again, I just wanna give some background of why this matters 'cause I think this helps us focus our conversation and when we're thinking about the changes we need to make. So, there were three main goals with GDPR, the first one was really giving people control over their own data. So fundamental privacy rights are now a thing in the EU ensuring the security and confidentiality of your own data, ensuring that you get noticed, you have a choice of how it's gonna be used, you have the right to access your data, you have the right to correct it or to erase it, among other new fundamental rights. Another goal, which is to update the privacy laws, they had not been updated and obviously, technology has changed drastically in the last five, 10, 15, 20 years. And another goal was to really standardize the data regulations across the EU because right now there are 28 different ones, so it is very difficult if you are operating throughout the EU to figure out how you need to comply.

04:17 AB: But today what I really wanna talk about is one major change, which is now if you are collecting someone's data, you have to get their affirmative consent for any way that you're gonna use that data. So, how we see this play out with the online businesses and ecommerce businesses that I'm working with a lot is when we're building our email lists. And if you want more information about this, I'll mention this too. I did a full training on GDPR and I shared my screen so you can see some slides with some examples and sometimes visuals really help for something like this. So, go to my website, check that out if you are interested, awbfirm.com/gdpr, made it really easy. You can see all the screenshots there.

04:57 AB: But the important thing to think about when we're thinking about consent now is that we have to have affirmative action. In the past, what a lot of us were doing, and I was doing this too because it was allowed, was we might have what we might call a lead magnet or a freebie, a download, some sort of incentive to get people to give us their email address and their name, and then once we had that, they had to provide it to get the thing that we were providing, something of value, something hopefully that they wanted, then we would put it on our email list and we would start sending them marketing emails, maybe we'd send them information or a newsletter also but I think we all knew that the real goal here is to get their information so that we can sell to them. And that is no longer going to fly. We now have to have affirmative consent to use someone's email for a marketing purpose, or to sell to them, or even just to send them helpful information. They have to take some action to say, "Yes, I want you to contact me for X, Y, Z purpose."

05:53 AB: So under GDPR, the way we're thinking about it is consent has to be freely given, it has to be specific, it has to be informed, and it has to be unambiguous. So this is a pretty high standard for affirmative consent. So you have to tell people exactly what you're gonna do with their data. If you are gonna use it for several different things, you have to tell them all of those things and you have to give them the choice to opt-in to each of those. Now, you cannot just have an opt-out, what we sometimes used to call a soft opt-in, which used to be okay, where you send them the first email, and then they can always unsubscribe. That is not okay anymore. You have to get their affirmative consent before you send them the thing. And again, if you are using their data for multiple purposes, they have to grant you the consent for all of that at the time you get their information.

06:39 AB: So this is what we call unbundling. You cannot have a single checkbox for, "Yes, please

send me marketing emails and sell my data to a third party and use it for all of these other things." You have to split out that consent for all the different things that you're going to do. And you can't precondition giving services on getting consent. So they are really wanting this to be set up so that we are changing what we've all been doing for a long time, which is providing services in exchange for getting people's data. And that has been the foundation of a lot of technology, a lot of apps, a lot of services have really... They're free, but the flip side of that is, you're giving your data and so that's why they're able to... They monetize it in some other way. They're making money on advertising, or they're making money selling it to somebody else. The service is free but you are giving them something and that is your data.

07:32 AB: So the goal of GDPR is that is no longer gonna fly unless you give consent for that to happen and you know what kind of uses are gonna be made of your data after you give it to them. And you are now required to list any third parties who are going to receive that data. And you have to be specific, you cannot just say categories like trusted third parties. Yeah, I think we've all seen the little statement at the bottom of websites or the bottom of forms saying, "We may share your information with trusted third parties to serve you better." That is not gonna cut it. You are gonna have to be specific. Is it your email provider? Is it your credit card processor? Is it a sister company? Is it someone totally unrelated but who just wants your data and you figured out you can make a lot of money by selling your data to them? You are now going to have to say that and give people the choice of whether they want their data shared with each of those individual companies or people.

08:21 AB: So it's very granular, you have to be very specific, these are all the requirements. And again, go back and listen to my minitraining one if you're trying to figure out how you need to comply with this. If you are not having that much interaction with EU citizens, some of these may not be as burdensome as they sound for you, but you are gonna have to look at your own business and figure out how you are interacting with people and their data to figure out what parts of these you need to comply with. But it's really clear that inactivity is not gonna cut it and a prechecked box. So let's say, you're gathering someone's information at checkout and you have something that says, "Yes, I want to receive your newsletter. Yes, I want to receive marketing emails," and you already have a checkbox in it, that is not allowed. They have to take some sort of affirmative action to be included in your data processing however that looks, or sending it to third parties.

09:13 AB: So, when we look at this with email marketing, I think you can imagine all of your opt-in forms are probably going to need to change. If it's a classic bait and switch where you say, "Enter your email to get my free checklist," which is what mine used to say, that is not gonna fly. Now, there's a couple ways around that and I have three suggestions that I'm gonna go over today. But in general, if that's what you've been doing, you're probably gonna need to make some changes.

09:37 AB: As I mentioned, a soft opt-in is not okay. That's where you don't get their consent but then later they have the opportunity to opt-out or unsubscribe, that's not okay. And then, using prechecked boxes is not going to be okay. So if you're using any of those now, you're gonna need to make some changes. So here are my three, but I think are three great options. These are not the only options, and there are other ways other than consent that you may be able to interact with someone's data. I'm not gonna go over those in detail today. This is a high level view. If you're interacting with people who have already bought something from you, there may be some different rules called

legitimate interest. You may hear that tossed around, but that is a complex analysis that I'm not gonna go over today. If you have questions about that, feel free to pop in to my Facebook group, the Legal Road Map Facebook group, and post those there. I'm happy to talk about them more, but it is just a rabbit hole that I don't have time to go down in this one video today.

10:29 AB: So here are three suggestions. I forgot to give my disclaimer. Here's my standard disclaimer, that I am a lawyer, I'm licensed in Tennessee, I am not your lawyer, this is all information, this is just something to get your wheels turning. If you have specific questions for your business, please consult your own lawyer, whether it's me or someone else, who can look at your individual business and give you custom-tailored advice to your questions. So here's three options that you might wanna think about. The first one is, tell people that they're signing up for a newsletter. You just make it really clear, you say, "Sign up here for my free newsletter." And then if you wanna give them some incentive or something, you can do that, you can say, "Sign up for my free newsletter and get a free checklist," or something like that. But it needs to be clear that what they're really doing is not getting the checklist, what they're really doing is signing up for your newsletter.

11:15 AB: And I think this is going to change the way a lot of us market our newsletters or our weekly updates or monthly or however often you do it. I think we're gonna really have to start selling them, that they are valuable and that people should want to be on our email list because they get a lot of value, not because we spam them with a ton of marketing offers. Nobody is really excited to just know what you're selling. People either want a coupon, a discount, something of value, information, something they can use in their business, or they wanna know about new products, they wanna have some insider information, or they wanna find out things earlier than other people. I think we're really gonna have to get better at telling people what are the benefits of being on our newsletter list, and I think we're gonna have to be more creative about providing good benefits. And then I think people will still opt-in to our lists.

12:02 AB: I think that our joining rates are going to go down, but I think hopefully, we'll have people who are more engaged and more excited to get our emails and hopefully will actually open them and maybe even click on things and buy from us. That's really the goal. The goal is not just to send people emails, the goal is obviously to engage with people and eventually they become our customers or they become our friends or colleagues or other connections. So, option number one is just tell them that they're signing up for an email list, and if you're clear, it's very obvious what they're getting, that is okay under GDPR. The second choice is when they sign up for a freebie or a download, you can have a separate checkbox underneath or wherever, beside, there's no rule about where exactly it has to go, saying, "Yes, I want to receive marketing emails." Or, "Yes, please send me more information about..." so for me, it might be about online digital marketing rules or something like that.

12:57 AB: And again, if you have separate email lists for marketing and newsletters or information, you do need to split that out. Now, a lot of us are really combining our weekly newsletter lists, also maybe contain some offers. If you've got a double purpose, you gotta tell people, "Please sign up," or "Click Yes to receive legal updates and special offers." You can tell people that they're getting two things as long as you're not separating those things. If you can separate it out, you need to have separate checkboxes.

13:28 AB: And one suggestion that I read, and I thought this was really interesting, was instead of just having a yes that someone has to click, which is obviously a barrier, they have to take that action and that's the goal. But you might consider a yes/no option. So both boxes are blank and they have to pick one to go forward. They either have to click yes or they have to click no. And I think having that choice and seeing what benefit they're gonna get from clicking yes, you may see a higher conversion right there. So, just something to think about. So that's your second option is a checkbox, something affirmative, saying yes in addition to getting this incentive, download PDF, free course, whatever you're sending them, I want to receive marketing emails.

14:08 AB: That would be the same if you're selling a physical product or a digital product and you have this as part of your checkout process. You have to get their information to be able to send them the thing, but you can't use that information to market to them unless they click that box. Again, there may be some legitimate interest tests there. I'm not gonna get into that today, that is out there if you wanna read more about it and we can chat about that in the Facebook group.

14:30 AB: So our third option is to use what we call a double opt-in. What this means is, someone provides you their email, you send them the thing, you cannot not send them the thing. So you send them the thing, whatever it was that you promised when you said. For me, with this GDPR issue, I've got a free checklist of how you might comply with GDPR. Mine says something like, "Get your free GDPR compliance checklist in your email." I send them the thing and then after I send them thing, I don't send them other marketing emails, I send them one more separate email that says, "If you would like to receive legal updates, special information, special offers. If you wanna be the first to know about trainings that we offer like this one," I go really deeply into all of the benefits that people who are on my email list get and I say, "If you would like these, click here to subscribe." And it's very clear exactly what they're saying yes to, and that is in an email, they click that button and then they're automatically are now in my email system, which is, I use ConvertKit, but all of the big email systems should have a way to do this. I now have a record that they have given me their affirmative consent, that yes, they do want to receive information, further emails from me.

15:39 AB: So that is the double opt-in choice where you're having a confirmation email. Now, the downside to this is some people will not even read that email and a lot of people will not click on that email. I think there are some benefits to going ahead and gathering that affirmative consent right at the place before they've gotten the thing you promised with a checkbox or with letting them know that they're signing up for your email list. But a double opt-in is certainly one way that you can look at complying with GDPR. And again, if you're doing the double opt-in and you have multiple things you wanna do with their data, you're gonna need to split those out. So you would either need separate links or you would need to send them separate emails asking for the specific consent for the thing that you wanna do with their data.

16:21 AB: The important thing to know with this also when we're talking about email forms with any of these options is we now, under GDPR, have to post a link to our privacy policy, pretty close to where we're asking for their information. So there's a new rule that you have to tell people in more detail what you're gonna do with their data right at the point where you're collecting it. And there are new rules for what has to be in your privacy policy under GDPR. Hopefully, you already have a privacy policy. If you're doing business across the US, it was already required under

California law. So, you should already have one, but your privacy policy probably needs an update because there are new requirements under GDPR that you're gonna need to comply with.

17:00 AB: So, we've got a couple steps. We need to update our privacy policy and we need to make sure that we have that link. And again, whatever you're using, either for landing pages or your email service provider, however you're doing your contact forms, they should be providing some resources to make this easy, or your web developer can do this. There's no rule on exactly where it needs to be, but it's clear that under GDPR, they are not wanting it to just be buried in the footer of your website, which is where a lot of us have our privacy policy posted. They want it to be more prominent, they want it to be close to the place where you're asking for the information so that it's really easy to just click on it if someone's curious about how you're gonna use their data, or who you share it with, how the processing works, they can just click on it right there. It needs to not be buried, it has to be somewhat prominent.

17:44 AB: So, that is the summary of these new affirmative consent rules. Something else before I move on is a couple more notes. In addition to the consent being affirmative, you have to document that consent, so that means you should have records and there's no rule about what exactly those records have to look like but you should have documentation of how you got someone's consent. So if you're getting it through a form, maybe your email provider is saving that data for you. This is some due diligence you might need to do into your own systems and how things work. Just, if it's not clear, this should be maybe a call to tech support or figuring out how exactly this is gonna work so that you can make sure if you ever did get audited or had an issue come up with a data breach, I think that's most of where we're gonna see problems happen is if there's a data breach and people's personal information is sent out into the universe and they're not happy about it, they're gonna come back and try and figure out how their data got either sent somewhere or how somebody got into your system, and you are gonna have to show that you had their affirmative consent to do whatever you were doing with their data. So, we've gotta document that consent. That could look different depending on the different apps or service providers that you're using to actually gather this information.

18:55 AB: Another thing to think about is, there are new rules about withdrawing consent. We've always had the general understanding that you have to make somebody... Make it easy for someone to unsubscribe. That's under US law. There was a federal law called CAN-SPAM. So we've already had these requirements, and most of... I hope all the email providers make that very easy for people to opt-out. But the thing is, now it has to be as easy to unsubscribe as it is to opt-in. What I find sometimes, and I don't know if anyone else has this experience, but I have somehow done something to get on somebody's email list and I get their email and I do not want it and I click subscribe, and then it asks me for a username and password, and I don't know the username or password, I can't find the username or password, I don't have time to go through this whole rigamarole of figuring out my username and password. I just want them not to email me anymore.

19:43 AB: And so, those kinds of things where you put steps in place to make it hard to unsubscribe, that is not gonna fly anymore. It has to be as easy to unsubscribe, so it should be one click or it should be putting in an email address and clicking a button. It should be as easy to unsubscribe as it is to give it. And again, we're gonna have to link to our privacy policy where the option is to unsubscribe.

20:04 AB: So the last thing I wanna touch on before I wrap up is, what to do with your current list. Because under GDPR, if you had someone's contact information before May 25th, before the new regulations go into effect, unless you were doing all of these things, which most of us weren't, we were not getting these kinds of affirmative consents. Unless you have GDPR-compliant consent, you are going to need to stop contacting people on your list that you can't show that you have that kind of consent, that you don't have documentation. So I think most of us are going to have to scrub our email list to some extent.

20:39 AB: Now, I think, and this is just one person's opinion, it's your choice as to whether you ask everyone on your list to re-subscribe, to make sure you now have their affirmative consent. We've talked about what's called a re-engagement campaign where you ask people to confirm that they want to be receiving the kinds of emails that you're sending. That would be GDPR compliant. I think there's an open question about whether that needs to be for your whole list or whether you can narrow that down to just people who are in the EU, since that's who we're really worried about. And I think with something like this where you're likely gonna lose a big portion of your list through this re-engagement campaign, asking people to stay on, a lot of people are not gonna open it or they're not gonna click. So that is a risk. I do think you can use some of those tools that hopefully your email provider will provide to you that allows you to use IP addresses or some other way of geolocating so that you can maybe segment out just the people who are in the EU or who you're not sure if they're in the EU. And I would say if you're not sure, go ahead and treat them like they're in the EU. We wanna be cautious.

21:41 AB: Those methods are not 100% accurate. There are some risks, but I think with this, it's a pretty low risk. We're talking about people who have opted in in the past and you're just doing your best to get their new consent. I think that segmenting based on the best information you can get is probably gonna get you where you need to go. But again, as I mentioned in the last training, a lot of this of how you comply and what you decide to do is a matter of your risk tolerance. I can tell you what the rules are and what the law requires, and then you've gotta decide for your own business whether the risks outweigh the cost of putting this into place.

22:14 AB: But so what a re-engagement campaign means is, you're sending hopefully a series of emails to the people that you need to get their affirmative consent, showing them the value of staying on your list, making sure you grab their attention, maybe you're offering them an incentive to stay on your list. All of those things are fine as long as you're very clear with what they're consenting to. And you might wanna do four or six emails because people may not open all of them. People get busy and we don't see everything, we don't click on everything. But you're gonna need to have their affirmative consent in a way that you can document it if you're gonna keep emailing them after May 25th.

22:50 AB: Now, if you've been using double opt-in all along, which I described earlier, where you're already sending an email asking people to affirmatively opt-in to your list, you don't need to do this re-engagement. I will tell you, I was delighted when my assistant and I sat down, we were looking at our own systems to see how we could become GDPR compliant and she reminded me that we were doing double opt-in, it's a decision we made literally years ago and I had just forgotten. So, our compliance is very easy, we're very lucky that we made that decision. We already

have a pretty engaged list with using that double opt-in.

23:20 AB: So that wraps up our session on affirmative consent. If you have further questions, definitely pop on over to our Facebook group, the Legal Road Map Facebook group. You do have to be let in but just ask for an invite and we will admit you, as long as it doesn't look like you're a crazy person, we're pretty liberal about who we let in. I pop in there and answer questions from time to time. We have an engaged group of business owners who are also answering questions, so that's a great place to post your GDPR questions. And as I mentioned, we do have the full training that I did where you can see screenshots and different examples of how you might comply with GDPR at awbfirm.com/gdpr. Thank you so much for joining me. I'm going to do a minitraining next week, that's gonna be minitraining number three on Facebook Live, going over the use of cookies on your website. So, if you're using the Facebook ad pixel or Google Analytics, that is cookies and there are new rules that are gonna apply to you. So, definitely tune in next week. I will post that on the Facebook page when that is gonna happen and that will be on the podcast as well, so you can tune in there also. Thanks everybody, have a wonderful rest of your week.

[music]

24:31 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 5-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 5-minute IP Audit Worksheet now at awbfirm.com/podcast.

Thank You for choosing Scribie.com

Cross-check this transcript against the audio quickly and efficiently using our online Integrated Editor. Please visit the following link and click the Check & Download button to start.

<https://scribie.com/files/57f6c10230714e2794b3500c07f599c1b96e31ba>