New privacy laws: how financial marketers can stay ahead of the curve

Mike Nemecek: Good morning. I think we're ready to get started. We're excited you joined us today to talk about something that really could be a boring subject. We hope to avoid that, obviously, by focusing on areas that are relevant to you as marketers.

Mike Nemecek: I'm your host, Mike Nemecek, and I'm joined by Paul DeLeeuw. We're going to be speaking about changing privacy laws in the U.S., and how marketers can be prepared for those changes.

Mike Nemecek: A little bit of background on why we're having this discussion. DDM is a full-service marketing firm, and we work in complex, highly regulated industries. I work in the financial services industry, mainly with asset managers. Paul is an interactive team manager and works with a broader range of industries, including medical device, healthcare, as well as the financial services industry.

Mike Nemecek: We want to share our perspectives, have smart conversations to help you be equipped and informed on relevant topics. That's really what we're here about today. We're not pitching product or talking about specific projects we've completed. Our intent is to have real conversations that benefit you, in your role, at your firms.

Mike Nemecek: I do want to just remind you, we're not lawyers, but we do work with lawyers on a regular basis. We don't want to sound like lawyers as much as possible. (My apologies to lawyers that may be listening to this recording later). We're not going to be over-technical is what I mean by that. Feel free to submit questions to the chat anytime during the webinar. We'll try and work those in as they're relevant, and you don't need to wait for the question and answer time that we have at the end. If there are technical questions that come up and we don't know the answer to that, no worries. We'll find the answer and we'll get back to you after the webinar in an email. So we're happy to deal with the tough questions, as well, if they come up.

Mike Nemecek: In general, laws are changing. That's nothing new, but it is impacting how marketers are doing business. We want to focus on B2B business implications, as well as some of the B2C implications as well.

Mike Nemecek: Some of the trends we've seen, basically, some of these privacy laws started in Europe. Over time the U.S. is starting to bring some of those to our states. The laws of Europe are influencing some of the laws in the U.S., so they're not completely different, but there are a lot of similarities.

We're going to try and give you some highlights on that as well in the discussion.

Mike Nemecek: California's the first state that really started to pass some of these privacy laws. There are some other states that are following. In fact, federal regulation may be following as well. There's a couple of things to keep an eye out for over the next couple of months. We hope to go through some of those details here in the discussion today. With that, I will turn it over to Paul.

Paul DeLeeuw: Thanks, Mike. I appreciate it. Good morning to our participants, or if you're catching us later on the replay. We appreciate that. As Mike alluded to, this is really focused on the new laws that are happening in the United States.

Paul DeLeeuw: But I wanted to start off with an overview of privacy. What we talk about when we mean user privacy, customer privacy, client privacy. A lot of the regulations that are being passed and laws that are being discussed in the United States really took a lot cues from GDPR. Because GDPR is probably a fairly familiar exercise for a lot of people, we thought it would be worth doing a quick review up at the top of GDPR. As we get into CCPA, which is California Consumer Privacy Act, which is really the Act that has the most steam right now. As usual, California is trailblazing. They took a lot of cues from GDPR. There's other states that are following along. We'll do a little bit of a comparison. They're, I would say, 95% similar when you look at one versus the other.

Paul DeLeeuw: So if you did work to be compliant with GDPR, a lot of that work is going to be reusable, and you're not going to have to do it again with CCPA. But there are some key differences, and vice versa. I wouldn't give you a target to say, "You need to hit one or the other." I would say, "It's really a both/and especially if you're operating in Europe."

Paul DeLeeuw: With that, I'm going to jump into the first slide regarding privacy. In general when we talk about privacy, providing privacy means providing an environment where personal data is protected. When GDPR was passed and announced, and people started dissecting it, one of the themes of GDPR is that the people who are on your website, as a marketer, you need to look at the data that you collect on them as their personal data. You may be the one collecting it, and you may be the one who is looking at and analyzing it, but from the EU's perspective and now from the Californian perspective, it is the end user's data. That means they have the right to come back and ask, "Well, what data do you know about me and how are you using that?" "If I'm uncomfortable with that, would you delete it? Would you provide me with a copy of it?”

Paul DeLeeuw: There are some provisions, even in GDPR for saying, "Yes, we can do this much, but we can't do this much." We'll get into some of those details a little bit. Because a lot of them, again, carry over when we get into the United States.

Paul DeLeeuw: GDPR is the general data protection regulation. It was passed by the EU. It began enforcement basically a year ago, May 2018. The rights here are interesting because they cover EU citizens and not EU companies. Hopefully this is a bit of review, but essentially, there's some onus even on companies that are in the United States and elsewhere to make sure there's a level of compliance with this. Because if there is an EU citizen that is transacting in personal data with your website, they have rights under the GDPR that effect how you run that website, what you collect about them and what you disclose to them that you collect.

Paul DeLeeuw: Now, of course, it's an international thing, and the enforcement of it is fuzzy. If you dig into U.S., the International Privacy Shield Laws, there are mechanisms in place where EU citizens can basically pursue some kind of regulatory action that can be effective in the United States. It's more complex because it's offshore. But it's something to be cognizant of, especially if you know, "Yes. I do have customers that ..." They may not even be necessarily EU citizens, but they're residents in the EU at the time that they transacted with you. There's some statutes there that apply.

Mike Nemecek: Just to that point, I get that question quite a bit. "Does GDPR really apply to my firm? We're a U.S. asset management firm. We don't really do a lot of work outside the U.S." But to that point, maybe their customers are in Europe when dealing with the website. Would you say that it applies to those firms?

Paul DeLeeuw: Yeah. I would say that it applies to those firms, because they may be in a variety of situations in which GDPR can apply. Essentially, if you have any kind of long-term residency within Europe, you can pursue action under GDPR. Europe is a very consumer friendly regulatory mindset. And so, even though you may not be officially a citizen of the EU, because you were there, and because there was personal data crossing borders, there's a potential there that needs to be monitored and taken care of.

Paul DeLeeuw: So when it comes down to what rights does that person then have, well, as I said before, all that personal data that they give you is their data, from the EU perspective. It's the right to request your data, what do you know about me, and how do you use that data? The right to request erasure, or this is sometimes called, the right to be forgotten, which essentially means somebody can reach out to you and say, "I want you to delete all the data that you have about me." You need to have a process in place that covers that.

Paul DeLeeuw: Now one of the interesting things about that is, that it does not need to be an automated process. A number of companies who are concerned about this think there's going to be a technical investment, a time investment in creating some kind of a tool that scrounges up all the personal data that you have on somebody, and automatically deletes it. The advice that has been shared with us, and that we share with our clients is, don't take any action to create any kind of automated system for that. We don't have a good sense of what the volume of those requests is going to be. But if it

becomes problematic, then it's worth taking the time to invest and putting those tools in place. The best place to start is to come up with a procedure. How do we handle this if this requests come in?

Paul DeLeeuw: Importantly, because they have the right to request your data and the right to request erasure, you should have a privacy policy, somewhere on your site that's exposed, that you publicize, essentially. So if you see those cookie banners on people's websites, a lot of what they're doing is they're taking that cookie banner, and they're also putting in there, "... and we've updated our privacy policy," or, "You should review our privacy policy at this link." Within that privacy policy you should provide some kind of guidance on if they want to request their data, if they want to request erasure, they want to be forgotten, how do I contact the right person in your organization in order to take care of that. Your privacy policy should help determine what those steps, what the next course of action is.

Mike Nemecek: What are some of those data points that are relevant when we talk about personal data?

Paul DeLeeuw: Yeah. We'll get a little bit deeper, because when you get into CCPA, it's actually more stringent, I would say, than GDPR in terms of what they consider personal data. GDPR covers things that would be obvious, if you have somebody's name, their government ID number, whether that's a social security number or driver's license number. In some cases they can consider the IP address personally identifiable, especially if that IP address is tied to a residency as opposed to a corporation. They would consider that personally identifiable.

Paul DeLeeuw: But where CCPA takes that further, and we'll get into this a little bit further into the presentation, is there's also metrics for, if I look at your browsing history, could I use your browsing history to infer who you are as an individual, or when it comes to obvious pieces of data collection, like loading somebody into a CRM or an email marketing automation. Once you've collected email address, they consider email address personally identifiable, even if you have the kind of email address that's 12345@yahoo.com and it doesn't have your name in it. That's still considered personally identifiable information because that can be tracked across the web from site to site all of your history. CCPA goes a little bit further than GDPR in terms of determining what is personal information.

Paul DeLeeuw: There's other things that fall in there, that I think are also fairly obvious. Health data is covered by there. Of course, we have HIPPA. That doesn't really affect financial clients as much. But when you get into also, account data and accounting information, now that's when you start to get into the exceptions that you have. Say you had an account, and they have a login into your website. They say, "I want to know what data you have about me, and I want to request that you erase that data." Well if they still have an open account with you, you obviously have a business need to keep some amount of personal information so that you can continue to operate

their account. But you could say, "Okay. Here's the data that we have that we could eliminate."

Paul DeLeeuw: For example, we know where you've been on our website. We could delete the information on where you've been on our website without any significant business impact. So you have to be able to justify from a business perspective, we need to keep some level of information in order to, for example, continue to provide account service or continue to provide in other industries, warranties, service, that kind of thing. You need to have some level of information.

Paul DeLeeuw: Similarly, with your employees, your employees will be covered by this personal information as well. There's a separate part of it. I don't want to get into the HR discussion, because again, we're marketers, not HR people. But there is a level of that as well, where you should be protecting your employees' privacy. What data you know about them. How do you get rid of it if they're terminated, all of that kind of thing should be addressed on some level.

Paul DeLeeuw: A couple of more notes here with GDPR that become relevant. Marketing purposes are an acceptable use for limited personal data. Names, emails and contact info. The basics that make up personal data, you can collect this kind of information without an explicit opt in. There are parts of GDPR that trigger a opt in process. Generally, that has to do with if you're selling the information elsewhere. If you're simply collecting information so that you can add somebody to your mailing list, and so that you can do internal marketing analysis, that is all fine. But when you cross into doing research or collecting additional information and then potentially selling that information, that's where you have to provide an explicit opt in.

Paul DeLeeuw: So for marketers, in general, with GDPR, unless you are in the business of actually selling that data, you're probably safe simply providing a privacy policy and saying, "We collect this data for marketing purposes." You do not have to provide an explicit opt in process in order to continue to collect that data.

Paul DeLeeuw: Another note here is that GDPR requires what they call in Europe, a state-of-the-art and security practices by data controllers and data processors. Now as the operator/owner of the website, you are considered a data controller in GDPR parlance. Whereas we, if we're your marketing firm and we're hosting your website for you, we would be considered your data processor, your ISP on some level is considered a data processor. If you're hosting with a third party like Azure or AWS or Linode, they would also be considered a data processor. They might house your data, but they don't claim any kind of usage of it. It's simply a place where it lives.

Paul DeLeeuw: But let's dig into that term, state-of-the-art, because in the United States, we think of state-of-the-art as meaning cutting edge or the very latest in practices. In the European Union, that really is more of the state-of-the-

art, meaning standard practice regarding security. They would want to see, for example, something along the lines of ISO27001 or 27002. They want to see that you have a data security process, that you have policies that cover it, that you have an owner for data security and data privacy. That's essentially a person in your organization has that as part of their concern. This is probably part of why if you've gone to work with outside vendors, and your IT department wants to get involved with that, they want to get involved because they know from a compliance perspective, they need to make sure that your vendors have these baselines in place. That they have a security process and a policy. That they have data security. That they can speak to, "Here's what we do to protect your data and therefore your customers' data."

Mike Nemecek: Part of the reason GDPR came about was because Europe was trying to protect individuals from privacy breach, data breaches.

Paul DeLeeuw: Correct. Yup.

Mike Nemecek: Part of what they're looking for is what happens if there's a data breach. Right?

Paul DeLeeuw: Yup. Yup. That's exactly what they're looking for. When I take this and I move towards the United States side of things, California was actually the first state to pass any kind of a data breach law. That happened back in 2004, so they were really quite ahead of the game on that. That has very similar regulations in terms of they want to see that if you are a company of a certain size and stature, with a certain number of customers, they want you to have security policies and processes in place. This is one where California was leading a little bit on the data security side of things. Especially when it comes to, when there is the data breach, if there is a data breach, hopefully there's not one. But if there's a data breach, what do you do? Do you have a policy in place? Who do you notify? There are some standards and practices involved there that already exist in California law prior to CCPA.

Paul DeLeeuw: CCPA just takes some of that and expands it to mean consumer privacy, individual privacy, personal information. Really expands personal information to mean something much larger.

Paul DeLeeuw: Under the previous laws in California, personal information was really much more restrictive. Meaning, if you had somebody's name then you knew that was personal information and you were responsible for notifying of breach. If you have somebody's social security number, you knew you had to identify someone of breach. But if you basically didn't have either of those two pieces of information, then everything else was fair game. If it couldn't be tied back to somebody's name, or social security or government ID number then they weren't as worried about it and it didn't trigger the whole breach notification process. Whereas, under CCPA that's much more expansive because the idea of personal information has expanded. We'll get into that a little bit more in a little bit.

Paul DeLeeuw: What does this mean for us? For GDPR? You are a data controller as a person who operates. Presumably you operate a website where your clients can go and get information. They can download their fact sheets. They can see how the performance of the funds they invest in are doing. Maybe they have a login aspect of it. A lot of times they don't. But you might be collecting some analytics or you may have some kind of interconnection with a CRM or something along the lines of Pardot. You're collecting data about your users. You're a data controller.

Paul DeLeeuw: You have to be able to justify why you collect and retain personal information, if you do so. You need to be able to report data breaches to the appropriate EU regulatory body. If you have data that is regarding European citizens or European residents, you should have a process in place that allows you to report a data breach. I believe the regulation is within 72 hours, you are responsible for reporting any data breaches of personal information to the appropriate EU regulatory body.

Paul DeLeeuw: In many cases, that can be different depending on which country in the EU it is. There isn't an overarching agency there, so you may be coordinating with agencies at a country by country level. You can be fined 2-4% of revenue if you're found negligent. If you have compliance in place, and you are following good standards and practices, you may still be fined, but that fine is going to be on the much lower end. But if you are found negligent, you don't have good standards, you didn't have a policy for how to handle a data breach, or you didn't do due diligence with vendors to make sure that you had a plan for how to handle that, then you could be considered negligent. You would be on the higher end of that fine scale there.

Paul DeLeeuw: Interestingly, with that, you cannot pass your liability onto the data processor. There are cases where you might contract with your hosting provider or your marketing agency or whoever you're working with who's going to build and host your website, and it's probably very tempting to say, "Let's put in that contract that if there's a data breach of some kind that our vendor is liable for any damages that we could incur." Under GDPR, that is not allowed. You can put it in the contract, but it's effectively not enforceable under the case of GDPR.

Paul DeLeeuw: That said, data processors, as well as data controllers are required to implement state-of-the-art security practices as well. Separately, they can be fined. If you did have a data processor who had a data breach, you might be fined basically for not doing due diligence, if you were negligent in that aspect. But the data processor may also be fined separately for not doing what they need to do. That's the critical aspects of it and why it's very important for folks on our end of things to be implementing these data and privacy policies on your behalf. You can, certainly, under that contract require us to report data breaches to you. We're required by the law as well to notify you. You're the data controller. It's then your responsibility to notify the appropriate regulatory agency. But we are compelled to report those data breaches to you as data processors.

Paul DeLeeuw: That's the GDPR overview, but there's a lot of areas where we've already dug into. CCPA as well, and said, "Here's where things are similar. Here's where things are a little bit different." Let's dive into that a little bit more.

Paul DeLeeuw: Personally identifiable information. I put 2.0 on here. Because really this is a big expansion on what is considered personally identifiable information for CCPA. Previously under the data breach, under the previous data breach laws, as I said before, if it was your name, if it was your government ID number, that would be considered personally identifiable information. Pretty limited amount of other things that would be considered personally identifiable information. It was, not necessarily tough to enforce, but it meant that as a company there were many fewer instances of where you would need to report a data breach to the government if you had any kind of an issue.

Paul DeLeeuw: If you didn't keep somebody's name in your database, if you didn't keep that ID number in your database, you didn't have to really worry about it. You could have a data breach. You could take care of it on your own. You might report it in the case of if you didn't understand what the data breach was, you might work with a regulatory agency to help you understand what happened with the data breach or to help investigate. Because there might be somebody who, for example, hacked your website, and you might want to go after them. But if it's not at that level, you could essentially keep it under wraps if there wasn't personally identifiable information.

Paul DeLeeuw: But there's a lot more in this 2.0 version. Under CCPA, any information that can be used to identify an individual is considered personally identifiable information. That can include things like login tokens. Let's say you allow somebody to create a user account. You didn't have necessarily their name or email address, but you created a login token for them and they could use that in the future. That could be considered an individual's information. If they know it and can track it, that's personally identifiable. IP addresses count. That's the address of your computer when you're browsing the internet. Every computer has a unique IP address, and you can track that, not only across your site, but from site to site to understand where people are going.

Paul DeLeeuw: Browsing history. If you can put together a browsing history and say, "Well there's a very high likelihood that this person or that this browsing history correlates with an individual user," at that point, it's personally identifiable information. Even machine learning behavioral analysis, there's new techniques for ... This is often getting used for login pages. But there's new techniques where the machine can identify who you are based on looking at you through the webcam, is an obvious one. But based on how you scroll through the page, what you look at first, what you do with your mouse cursor, what you type in and how quickly. All of those things can be used to build an individual profile. It ends up looking like a fingerprint in a sense. Your digital fingerprint.

Paul DeLeeuw: Now Google and others are using that kind of information to determine, "Are you a robot or not?" Number one. They're always trying to prevent scriptors from automated form sending and hijacking and things like that. Also, depending on how detailed they get with that information, they can use it to identify you and use that in, let's say, a login process. But also then use that to track you from site to site to site without using cookies or other means of tracking you in a more specific way. That all becomes personally identifiable information, which really expands the scope of what you want to be thinking about in terms of data breaches and when that needs to be disclosed.

Paul DeLeeuw: Now that's really something that your IT department is going to want to be thinking about more than you, but it's going to impact that relationship that you have with your marketing firm, with your outside vendors, the people that manage your websites. They need to understand what those pieces are and help you understand what they are, so that you can then put together a relevant privacy policy.

Paul DeLeeuw: CCPA specifically, California Consumer Privacy Act, greatly expands personally identifiable information regulations. Comparable to GDPR, I would say even more expansive than GDPR. Similar to GDPR, it adds the right to be forgotten. It adds the right to your data, so you can always request a copy. As a consumer, I can request a copy of my data from the sites that I visit.

Paul DeLeeuw: The right to opt out. When we talk about the right to opt out, specifically what we're talking about is third party data collection. If you have Pardot, for example, doing tracking on your website to assist in marketing automation. If you have Google Analytics tracking your website so that you can understand your traffic flow, you have to give people the right to opt out of that third party data collection. That's part of your privacy policy. Again, this is another instance where a lot of people are ... If they don't already have a banner because they didn't worry about complying with EU's cookie notice regulations, they're adding banners now to say, "Here's your privacy policy. Here's what we do and here's where you need to go to opt out if you don't want us to use this information with third parties, to sell this information but, and also, here's how you request that data. Here's how you request the ability to be forgotten and get a copy of what we do know about you."

Paul DeLeeuw: There's the disclosure requirements. Very similar disclosure requirements to GDPR. If you've done the legwork on GDPR, of creating that privacy policy and crafting it and putting it in front of your customers, you're 95% of the way there. But the opt out piece of it, you may need to work into that privacy policy. "Here's where you go to opt out. Here's how you tell us that you do not want your data shared with third parties." Whether that's Google or Facebook or data collection agencies or analytics firms, all of that kind of stuff, you can do an opt out.

Paul DeLeeuw: One thing that you can do though is, if you have anonymized that data, ... So Google Analytics, for example, typically is considered anonymized because they do not allow you to provide personally identifiable information through their service. You can't identify, "Oh, this user is Jane.Doe@gmail.com," and then track that person through the site using Google Analytics. You could do it yourself, using your own tools. But using Google Analytics, they have an anonymization factor in place.

Paul DeLeeuw: However, with Google Analytics, you could get things like IP addresses, and geo location data that does become personally identifiable. It will be interesting to see over time how Google, Facebook, Pardot, Salesforce respond to some of these regulations and the tools that they're going to give you to make sure that you can check some boxes and say, "You know what? I really just need them to be anonymous." I like to know some of that other information, but if you can get it to a level where I can't personally identify anybody, then you can continue to use those tools without worrying about the opt out piece of it. As long as it's anonymized. You have an onus to then be able to prove, "This is how we anonymized it." That can be as simple as saying, "Well, we use Google Analytics," or, "We use Pardot, and we turned this on and we trust that Pardot has an anonymization in place that helps us cover ourselves, cover our requirements there."

Mike Nemecek: As a marketing firm, there's only so much that we can do. With websites, for example, the cookie removal process, the code that actually implements that. We do work with lawyers in the area here that have a program that's focused on GDPR and CCPA. I'd be more than happy to pass on their contact information. If you have any questions, they have an established compliance plan as well as ongoing support after the plan is in place. Feel free to reach out to me. This is Mike. If you have any questions on how to get in touch with lawyers, that can really do this sufficiently for you.

Paul DeLeeuw: Essentially what this means, similar to the GDPR slide, what does this mean for us? Like GDPR, you should be considering where and why you collect information about the consumer, your customer, the visitor of your website. What are you collecting about them? Where is it going? How is it being stored? Is it personally identifiable or is it anonymized. You need to provide some disclosure of what that data is, why you're using it, so that those customers, those end users, understand what data you have about them and how you use it.

Paul DeLeeuw: Unlike GDPR, you have to consistently provide the opportunity to opt out of third party data collection, no matter what the purpose of the data collection is. Unlike GDPR, GDPR has that loophole where if you're using it for marketing purposes, and you're not selling the data, you don't have to necessarily provide that opt out. You still do have to provide the ability to give them that data and erase it if they request it. But you don't have to give them the ability to opt out, upfront, the same way that you do under CCPA.

Paul DeLeeuw: The definition of personal information is expanding greatly. Those previous triggers for what you had to worry about with data breaches before, that's a much larger ball of hurt that could be in there if you don't understand what collection you're doing and what kind of data you have. Data breach penalties, rather than being a percentage of revenue like GDPR, this is more about how many users you have and the incidents that you have. $750.00 per user, but it can scale up to $7,500.00 if they say essentially that you're negligent, that there was intentional violation of the law that you were aware and you did not implement the appropriate data security and privacy elements.

Paul DeLeeuw: So although CCPA, itself, doesn't say, "Hey, you have to be certified under some specific set or that you have to have an internal process owner." What it is suggesting, if you read between the lines is that, "if you don't have a process owner and an understanding of data privacy and data security, we can find you negligent if you do have a problem."

Mike Nemecek: Does that mean staffing?

Paul DeLeeuw: It could potentially mean staffing. The place that I recommend people start is if you don't already have a policy in place for how you would handle a data breach, start there. Figure out what that policy is. That can precipitate from there. "Hey, you know what? We actually need to have somebody who is in charge of data security." That's probably going to be somebody who is in IS or IT. They need to be thinking about it.

Paul DeLeeuw: If you're a financial firm, you probably already have that person. In fact, a lot of that staffing probably already exists, simply because of the other elements of compliance that are inherent in financial regulation.

Paul DeLeeuw: Now that said, they're used to thinking about data security probably from a different perspective than what GDPR is. They may need to be brought up to speed a little bit on added roles and responsibilities. They might say, "Yeah. We need to staff a little bit more because we have some other elements of this that we need to be considering." But I think, generally, if you're a financial institution, you probably have those people in place already. Hopefully, they are aware of what their requirements are, their compliance requirements.

Paul DeLeeuw: Expanding beyond the CCPA. There's other states and the federal government that are considering similar legislation. The next three that are the furthest along are New York, New Jersey and Maryland. When you get into those three, they're also very much taking their cues off of GDPR. They probably got started around the same time as California and just aren't as far along in their process yet.

Paul DeLeeuw: But there's also at the federal level, The American Data Dissemination Act. That's one that's working its way through the House right now. It probably has more support at this point, on the left than on the right. There's some question as to how far it will go. But as always with these

things, when the states end up leading and you have multiple regulations happening across different states, then when the federal government catches up and puts theirs in place, it just creates more complication.

Paul DeLeeuw: One thing that we're hopeful, and that we're keeping our eye on is that there does end up being a national standard that comes into place and that we can flag hopefully a fewer number of exceptions to that. Where, "Okay, where your requirement for California is a little bit higher than your requirement for general, the federal level." Because, of course, California is such a big economy, and there's so many citizens there that were participating with it, they kind of end up setting the bar by their nature.

Mike Nemecek: Let's just talk about timing real quick. GDPR was May 2018. California's coming up in January-

Paul DeLeeuw: January 2020.

Mike Nemecek: 2020.

Paul DeLeeuw: That's when they want to have everybody be essentially compliant with the new law.

Mike Nemecek: From what I understand with California, it is a bit of a moving target. They're not-

Paul DeLeeuw: It is. The main Act has been passed and will come into play. However, there's already amendments and adjustments to that, that are coming in. One of the interesting ones ... This again, I'm going to do a little bit of a comparison to GDPR.

Paul DeLeeuw: In GDPR, if an individual citizen has an issue getting their information or having somebody erase it or there's a data breach that they find out about that they're affected by, there's significantly more process in place for an individual consumer to come forward and take legal action against whatever company they feel is appropriate.

Paul DeLeeuw: In CCPA, it's a little bit more business friendly in that they are centralizing that on the Attorney General. Essentially, the attorney general's office would be collecting complaints, consumer complaints and issues, and then making a determination probably based on some guidelines that are not part of CCPA. Simply that the attorney generals, themselves, can determine what those guidelines are of when they say, "You know what? We've heard 150 complaints on Facebook. We're gonna do some investigation. Where we've only heard two complaints about Microsoft, we're not gonna worry about it until it hits some threshold."

Paul DeLeeuw: There's a little bit more of a business friendly aspect to that because you have the Attorney General, the Attorney General's office, hopefully a little bit in your corner warding away individual legal action. There are some circumstances, especially regarding data breaches, specifically, where

individuals could come together under a class action lawsuit and go after an individual company. Of course, it's the legal system, so anybody can sue anybody at any time for any reason, is what I've been told by many lawyers.

Paul DeLeeuw: But under CCPA, it's the Attorney General that has the most authority. But that is one of the amendments that's going through is, they are discussing and debating whether or not to alleviate that from the Attorney General and make it something that an individual can take action directly, can take legal action against the company.

Paul DeLeeuw: So there is some, always in motion with California there. There's three or four amendments that all have varying states of support. I don't think any individual one of them is looking like it's going to pass at this time. But now that the main regulation is in place, the adjustments to it are already coming out of the woodwork. Especially as companies start to understand and disseminate what's in the new Act. I'm sure there's some level of lobbying effort going into making sure that they can make their end of things reasonable, that they're not being over regulated as they go forward.

Paul DeLeeuw: Wrapping up, the big takeaway is, if you haven't already done this for GDPR because you're not as worried about Europe, then the big takeaways are you need to review what data you collect. That's your first place to start no matter what. Is understand what data do you collect? Is it personal data? Is it anonymized data? Could we identify a user based on this?

Paul DeLeeuw: Therefore, what is our policy around data retention? What do we do with it? Do we sell it? How do we analyze it? Who owns it? Can you justify that data? More than once in these audits, people look at their website and say, "You know what? I don't even remember having that form on our website." But it collects some data that I don't think anybody has ever used or looked at. It may be simpler to just get rid of that form than to keep it up there if it's collecting something that you're not really using and is personally identifiable, which most contact forms, for example, would be.

Paul DeLeeuw: You probably want to have a contact form of some kind on your website, so you want to be thinking about, "Okay. Who does that go to? How do we use it? Does that person end up on a list somewhere? What do we do with that?" You want to disclose that information as you uncover what information you have, where it gets collected, where it lives. Disclose to your clients and customers via a public privacy policy page. You want to publicize that privacy policy page. You should have something on your homepage somewhere that identifies, "We have a privacy policy. Here's where to go if you need to opt out of anything, here's where you go to do that, and how you contact us to request your data or have us erase it."

Mike Nemecek: Thank you, Paul, for going through that in detail. If you have any questions, feel free to submit it to the chat here. I think we answered a bunch of questions as we went along, but feel free to submit those. We muted lines so you wouldn't hear any paper shuffling or other things going on for some of the other callers. But feel free to submit questions. Otherwise, we'll just assume Paul did a really good job of going through the detail and was perfectly clear the first time.

Mike Nemecek: Well, we'll give you a couple of minutes here to go ahead and ask some of those questions.

Mike Nemecek: So, all right. I don't see any questions here at this point, but if you have other questions that pop up, feel free to reach out either to Paul or myself. Our contact information here is on the screen, or you can submit through teamddm.com. We have a contact form there and we'd be happy to get in touch. Let you know if we have any other information. Thank you, and have a good day.