QuickLaunch University Webinar Series Transcript
Data Privacy and GDPR: Is Your Startup Ready?

October 10, 2017

Presented by WilmerHale Partners Dr. Martin Braun and David Gammell.

Dave: Hello, everyone, and welcome to today's QuickLaunch University webinar. My name is Dave Gammell and I'm a partner and co-chair of the firm's Emerging Company Practice. Over the past few months, we've explored many different legal issues faced by entrepreneurs in early stage companies as they begin to build their businesses. Today, we are going to hear about European data privacy legislation and what U.S. startups should do now to comply. If you're interested in going back and listening to our previous sessions where we covered the basics of forming a company, founder equity, and more, the links to the recordings are posted on our website, and links are included in the email reminders you received about this webinar.

Now, I'll quickly introduce our speaker. Again, my name is Dave Gammell and I'm the chair of the firm's Emerging Company Practice, which focuses on advising startups from incorporation throughout their life cycle. Leading today's presentation is my partner, Dr. Martin Braun. Based on our Frankfurt office, Martin's practice is focused on outsourcing information technology and data protection law. He has advised German and multinational companies on all aspects of data protection law and general compliance issues including cross-border flows of personal data, data security, electronic discovery, and general document retention issues. Last, I want to mention to you that our firm has a number of online resources available to you. First, our WilmerHale Launch website is a resource for entrepreneurs, which has many helpful features and interactive tools for founders such as an equity calculator, a document generator, and collaborative videos with some of our partners. Our cybersecurity and privacy and communications group maintains a blog and an active Twitter page for ongoing updates in those areas. With that, let's get started. Martin, over to you.

Martin: Thank you, Dave. Hello and welcome, everybody. This is Martin Braun in Frankfurt speaking. I would like to walk you through key issues of the GDPR, especially in an emerging company context. I have been extremely busy over the past months advising clients of all sizes on GDPR issues. And the general observation is that large companies have typically started probably a year ago to prepare for GDPR but there's still plenty of companies out there who have not really started. The focus of this presentation will be issue spotting and walking you through the topics that I see most often in practice as being relevant and questions that are being asked. A focus will be the question, is the GDPR applicable to me and my company, and to the international transfer issue which also is just so often relevant. We could, of course, do a full day seminar on all topics but, again, the goal is that you will know in an hour whether the GDPR is applicable and what the core things may be that you need to check into next.

If we move on to the general background, where are we, where are we coming from? Data protection has been very important to Europeans for quite a long time. There is the famous European data protection directive which was enacted in 1995, which is ancient date. And so, basically, at the time when the internet was just taking off. The European Union decided that it is about time to update this legal framework. It was a long and very tedious process to update data protection law but it did succeed. And so, that's where we are today. There's adopted legal text which has been published in the official journal with a two-year warning. We have already used up one year of that warning. And on May 25, 2018, which is about 200 days from now, the European General Data Protection Regulation or GDPR will have full legal effects.

The first thing to mention in this context is that, and that's the good news, that European Data Protection Law will be much more harmonized than it has been in the past years. This regulation does not have to

be implemented or transposed in national member state laws, but the GDPR is the law regarding data protection in all member states. So, having the text of the GDPR will allow you to navigate really almost all data protection topics in all E.U. member states. Actually, the areas that remain for member states to regulate are quite limited. And the things that are relevant in practice, from my experience, are employee data protection which is expressly talked about in general. And so, member states will have National Law dealing with this topic. Then, there is the alignment between freedom of speech and data protection which covers all the media-related topics. That's, of course, huge, potentially. And the area of research is also subject to quite far-reaching national provisions and options to do things differently. So, anyway, that's bad news for pharmaceutical companies who were among the strongest supporters of the initial draft of the GDPR because they were hoping for uniformed laws. But pharma research and HR are, of course, two key areas which have not really been successfully harmonized. So, unfortunately, that is not as good as it looked in the beginning of the legal process.

The other thing everybody needs to know and if you have just read a small paragraph about the GDPR anywhere, you probably have heard that the big news about the GDPR is that the fines for noncompliance increase or can increase dramatically. The framework for fines for noncompliance has been raised to a maximum amount of 20 million Euros for violation or, and it's the higher of the two, 4% of the global annual revenue of the respective group of companies as the maximum fine. There's another threshold of the GDPR, which is 2% in 10 million, so you can kind of go through this long text and then always write 2% or 4% next to the relevant provisions. But, of course, even the 2% are painful. The background for that was that some European regulators felt that, especially, large internet companies would not really be terribly impressed by lower fines. There was a French CNIL decision against Google some years ago where they levied the maximum fine of the current French law, which was one million, and the impression was that that's not enough to really impress Google. So, they levied higher to have this additional framework. There are quite a lot of people saying that data protection law is the new antitrust law. As you know, antitrust goes up to 10%, but within the 4% we are already somewhat in that range. This is, of course, a reason why data protection is being taken much more seriously on a board level at basically all clients that I've been working with. Everybody has decided that it's just impossible to ignore the obligations under the GDPR.

If we go to the core principles of the GDPR on the next slide, I would like to quickly walk you through some key topics and define terms which are a bit different from what I typically see how Americans approach many of these terms. These terms have not significantly changed compared to the current legal framework. So, the GDPR is not a complete revolution of the old data protection law being totally turned upside down and turned into something new. It's rather a further step in the development of the existing framework, and a lot of the terms and the concept look very familiar with some tweaks to them.

The first question is data protection lies to personal data, what is personal data? That's the topic that has been discussed for a very long time in Europe. There had been various decisions by all kinds of courts including the European Court of Justice. The GDPR kind of follows the established line of reasoning. And the definition of personal data is a very wide and broad one referring to any kind of information that can be linked or attributed to a human being, directly or indirectly. So, there's no threshold like I understand in many of the U.S. laws, where social security information would be personal data but the name of an individual may not be protected. Under the European regime, the name is clearly personal data, an email address is personal data, telephone numbers are personal data, photos are personal data. In most instances, IP addresses, device IDs, and other things are very likely to be personal data if they can be somehow attributed to an individual that they will be. So, the entire ethics sector has to take a very careful look at this and is likely subject to this data protection regime.

The opposite of personal data is anonymous data. The European Data Protection Authority had issued some guidance on when and how can personal data be turned into anonymous data. Again, the high level threshold is this is difficult to do. It's not just crossing the names out and leaving the data set as is,

but there's much more to really generating data that can be considered anonymous in the European sets. The GDPR also talks about pseudonymous data or pseudo-anonymous data which is kind of in between, which is data that is not directly attributable but taking some additional information to that pseudonymous data will then allow you to identify any individual. Pseudonymous data is still personal data for all purposes of the GDPR. But the GDPR recommends to review at all stages of processing activities where the data could be stored in pseudonymous form to further reduce risks to data subjects.

Finally, in this definition of so-called special categories of personal data, that is the category that is subject to additional and extra protection. Health data is one prominent example, sexual orientation, racial background, labor unit affiliations are other examples. And there's a few things where this data is protected even more than other kinds of data.

The term processing of personal data is also extremely broad. Basically, any handling of personal data in any way will fall under the definition of processing, including just like being able to perceive or to look at data. So, there's no need to actually have the data and process it in a company's IT systems to be processing personal data. But having remote access to a customer system, for example, to maintain software or do other kinds of support activities will qualify as processing of personal data. So, again, this is also extremely wide.

The general principle under European Data Protection Law is that all processing of personal data is prohibited. A very German approach in a way, everything is prohibited until and unless you find a legal basis for the processing. And the GDPR in Article 6, of course, have a list of legal justifications for processing personal data. So, the typical approach and way to review these questions is, is it personal data? Usually, yes. Second, what's the legal basis for the processing? And then you go through the list in Article 6. The list has not really changed compared to the old data protection law under the data protection law directive. So, processing can be based on consent of the individual. Processing can be based on the need to process that personal data for purposes of a contract with the data subject. Processing can be based on legitimate interest by the entity that wants to process the personal data but there needs to be a balancing of interest against the interest of the affected individual. And if there are indications that the interest of the affected individual overrides the interest of the entity that wants to process the personal data, then that is not a valid legal basis. So, that list is always the list and there are six or seven things in there but, I think usually, it comes down to the three, maybe four topics that have to be evaluated in the specific circumstances.

The GDPR also contains a list of general principles regarding the processing of personal data. These are somewhat abstract but are still relevant. So, there's a general principle that any processing of personal data should be transparent and we'll be talking about information obligations in a minute. There's a general principle that personal data should always be collected and processed for a specific purpose. And if the entity that is processing the personal data wants to change the purpose, that is again something that needs to be justified. So, it is not the spirit of the GDPR to collect data just in case it might be useful one day, but it's the opposite. Whenever personal data is collected, the affected individual should be told this is the purpose, this is the legal basis, this is how long we store the data, and anything else, again, has to be subject to a legal basis.

There's a general principle that data should be minimized. So, only the data that's really needed should be collected and processed, and data that is no longer needed should be deleted. So, there's a general principle that personal data should be accurate and if it's not accurate, it needs to be rectified. There's a general principle yet basically just overlap between the principles. Data should be deleted when it's no longer needed and stored only the very minimum. And there's a general principle that data needs to be protected more from an IT security perspective. So, all of these principles, of course, don't have much effect if the data is not protected against illegal third party access.

And, the final principle, the entity that is controlling the processing of personal data needs to be prepared to demonstrate compliance with the requirements of the GDPR, which is called the accountability principle. And that is the one other big overarching theme under the GDPR. There's a need to do much more documentation of what's actually going on in the company. Understand what kind of systems have what kind of data, understand what kind of third parties are gaining access to personal data of a company, and documenting who has the data, and why do they have the data is one crucial step. And typically, really the step number one for any company that wants to get seriously started on preparing for GDPR. The first thing is the data mapping, as it's usually called, to understand what's really going on. And then, to be able to build on top of that understanding in being clear on what's the legal basis for the processing, and so forth.

There's a crucial distinction in the GDPR and we'll get to that in a bit more detail between so-called controllers and so-called processors. The controller is the term for the entity that really controls the means and the purposes of any processing of personal data. So, that's the entity that really decides and, of course, at the same time, the entity that is the prime target for any regulatory enforcement. At the same time, the processor is an entity that will just process personal data on behalf and under the instructions of a controller. So, the processor is just working or processing for somebody else, which, of course, results in more limited set of obligations. Again, we'll get to that in a bit more detail because that is, from my experience, extremely frequent in day-to-day life for a company, especially in a transatlantic context. And at a high level, at this point in time, there are additional restrictions in any kind of transfer of personal data to recipients outside of the European Union. A transfer includes making available or being able to access. So, again, it's a wide and broad term. And there is, again, another list of justifications for international data transfers, which we'll get to in a second. I just wanted to kind of give the key point to navigate.

So, these are the substantial material principles of the GDPR and the starting points for a framework to find out whether the GDPR applies because of the nature of the activities. The other side of the coin is the question of the territorial scope which is, I would assume, of particular interest to the participants of this call. Assuming that there are a lot of companies that may not have European offices yet and they would still be wondering would my company be subject to GDPR. So, the answer to all of that is Article 3 of the GDPR, which I have reprinted here in full. The reading of this provision reveals that there is a distinction in the first paragraph. It says that the GDPR will apply if the controller has a so-called establishment in the European Union. In a way, that's pretty easy. So, any company that has, let's call it, an office or an establishment in the E.U. and has that establishment process personal data, will be subject to the GDPR.

You may have heard of the famous Google case before the European Court of Justice some years ago, where the European Court of Justice took a very broad view of what does that, in the context of the activities, mean which is part of this first paragraph. And the answer was that this is actually a wide definition that there's no requirement that the establishment actually processes personal data itself. It's just that the activities of the establishment are somehow related or a part of the data processing activities. In Google's case, they had a marketing and sales office in Spain which was truly just selling advertising and all the search engines. Data processing was done out of California but the European Court of Justice, nevertheless, said that the two are so closely linked both from the perspective of somebody using the search engine, filling the search bar and at the same time, the advertising on the same screen. So, from the user perspective, it's one thing. And from the financing perspective, one would not exist without the other. So, even the sales office, which did not do any data processing, would still be sufficient to trigger this requirement.

You see in this first paragraph, that it does not matter whether the processing itself actually takes place in the European Union. The starting point is the establishment. And establishment has very little requirements. It can, worst case, be like one salesperson permanently in the E.U., which could be an

establishment already, or a mailbox, or something like that. So, that is the first category, having an establishment in the E.U.

The other category, second paragraph of Article 3, is those controllers or processors who are not established in the European Union. They can still be subject to GDPR without an office, without an establishment. And there's two categories and that's really a change to the old system. The GDPR has now moved really into a target market principle which is something that already exists in consumer protection law. So, this is somewhat familiar wording. So, if an entity or controller not having any offices in the E.U. offers goods or services to somebody who is based or who is located in the European Union, then the GDPR applies. So, a website that sells goods and services to people in the E.U., and somewhat targets the E.U. with a pretty low threshold would be subject to GDPR in these activities. And the other case which is the B situation, even if there's no offering of goods or services to individuals in the E.U. If the behavior of people who are in the European Union is monitored by somebody who has not established in the E.U., this monitoring of behavior activities will be subject to GDPR.

This is, as everybody has been repeating targeted at any kind of online advertising tracking related activities, which is now supposed to be all subject to the GDPR. We have looked into this for a number of clients in the past weeks and months, and it continues to be amazing how broad this applicability is, unfortunately. We have been dealing with Japanese insurance companies who have Japanese people who bought insurance in Japan and then traveled to Europe, and then accessing that company's website. And if that website has cookies and tracking, it looks like the B case may be relevant. So, while the Japanese people who are dealing with their Japanese insurance company while they are in Europe and access the website, that they may still be protected by GDPR. It's probably not the situation that is of prime interest for regulators but, again, all the cookie and tracking-related activities probably will be of much higher interest.

So, that is the overview. It is easier for data protection authorities in the E.U. that GDPR is applicable. It's much, much easier to argue that it is applicable than it was before. Before, there were all kinds of complicated legal argument to be made to make these claims and companies have largely gotten away with not really embracing the interest of regulators but that is likely going to change.

We go to the next slide. Maybe one addition, Article 3 also expressly talks about processors. So, a processor that has an office in the E.U. will be subject because they do have an establishment and if it offers goods or services to people in the E.U., or monitors the behavior, it is also in. That is different from the existing data protection law where the processors had better arguments to say that they're not subject to GDPR.

There's a third situation where GDPR may actually apply, and that is somewhat indirectly, for the American startup that successfully finds European customers. These European customers will be under significant pressure from their compliance obligations, that whenever they transfer data to a third party, whether in Europe or in the U.S., or anywhere else, that they need to make sure that the quality of protection of any personal data that they make available to the third party is basically as good as the GDPR. So, even for those companies who have now gone through Article 3 and said, "Okay, we are not in." They would still likely encounter their European customers demanding that they at least provide contractual guarantees that they treat data in line with GDPR requirements, whatever the contract may look like. So, this indirect effect is also something that I'm really seeing quite often.

Once we have established whether GDPR is applicable, next question is, what does that mean or what are the consequences? We go to next slide. I have listed some of the classics. This is not an exhaustive list but it gives you an idea. Probably the most scary piece is Article 27 of the GDPR which says that in general these non-European companies that are subject to GDPR are obliged to appoint a representative

in the European Union. And that representative would be, of course, the representative that could be served in the event of regulatory action or even in the event of individuals having complaints or want to bring lawsuits. I have not really seen a lot of offerings of companies that would offer to serve as a representative. And it's a pretty dangerous business because, in the event of fines, the representative could also be in. So, they would likely demand far-reaching indemnification. And I would say it's still an open question where the American companies will decide to read and understand this provision and say, "We'll still ignore it and see what happens." Not appointing a representative is, of course, again an offense that can be punished by significant fines. But for companies that have no intention to ever move into Europe, that may still be a real large strategy even though I can't truly recommend it from a legal perspective. And we may see companies offering this kind of service to serve as a representative.

The GDPR has certain obligations to appoint a data protection officer within the company, which is a rather independent individual who is supposed to be the key contact and key player in data protection as Article 37. The GDPR now has a uniformed hand your pin notification of breaches obligation. Until now, some member states have it, others don't. Now, it's really a uniform thing which is, in general, good because everybody will play by the same rules. Processors have to notify the controller for which they are working and controllers have to notify the authorities usually within 72 hours. And in certain cases, they also have to notify the affected individuals, the data subjects.

There are general obligations regarding the security of processing activities, IT security. I find most of my American clients to be quite well-prepared to comply with these high-level requirements. There's no specific set of IT security requirements in the GDPR, it's just something that has to be good enough for the data that is actually being processed. There's no specific help in referring to substandards or anything. But I find American clients to be very aware of any kind of cyber risks. In most cases, the IT security is something that may have to be documented but not necessarily have to be upgraded.

I mentioned that the GDPR requires a lot of documentation. Article 30 is the most prominent example. There needs to be a register of processing activities, something that controllers need to do but even processors need to do, to have something ready if the regulator asks in terms of being able to show what kind of data is being processed, why, and for which purposes, and how long, and so forth. There are some more high- level principles which, from what I've seen, nobody really knows what they will mean in practice. Data protection has to be implemented by design and by default. There's some idea that if you sign up for a website that in an ideal world, according to the GDPR, the user would sign up. There would, of course, be a legal basis for certain processing activities which are required for fulfilling the contractual obligations, no problem. That's covered by the purposes of the contract. And anything else should, by default, be turned off. And then the respective website in our example would have individual consent for each individual thing that can be separated for different purposes. And so, there should not be one consent agreeing to everything, and the consent should not be linked to the willingness to enter into a contract with the data subject.

This is all scary and so far from current reality that this is something that really has to work through individuals with all companies and some compromise, I guess, will have to be made here. Again, the GDPR tech is really robust in this regard but companies are just finding a certain level of risk in complying with these obligations necessary to just maintain their business models.

Data controllers have to inform data subjects about any data processing activities, that's Articles 13 and 14. And data subjects have certain rights. They have a right to request correction of the data. They have a right to request information about what kind of data control it has, that the famous right to be forgotten. So, a right under certain circumstances to require that the controller delete certain data and a few other things. I think we have to see how much interest the data subjects will really have in practice to exercise these rights. The rights are there but they have been there since 1995. And so far, there hasn't really been a significant amount of interest. But depending on the complexity of the operations, it

can, of course, be creating a lot of work to actually comply with these obligations that they distributed through all kinds of IT systems.

If we go to the next slide, I wanted to talk a bit more about controller-processor relationships. You remember the definitions of a controller and the processor. The GDPR now has a long list of requirements that any agreement between the controller and the processor need to include. First of all, the obligation is to have a contract. The good news is it doesn't have to be on paper but it can be in electronic format. But, again, this long list of individual items that need to be checked off to comply with Article 28. So, there's something about the obligation to follow instructions, there's something about software process, there's something about the deletion of data at the end of the contract, and so forth. And just as a general warning, the parties cannot override the actual relationship. So, if two controllers exchange data, they cannot just create a controller process agreement and claim that one is the processor of the other. The data protection authorities will always look at what's really going on. And if the alleged processor takes its own decisions regarding certain processing steps then, or it's for purposes of the alleged process as well, then they will not agree to the fact that there is the agreement and that should be followed.

There's no real standard set of templates for these contracts yet, but there will be probably in the coming weeks or a few months. So, this is largely going to be standards where you have the contract template that has the magic words on it and then everybody yawns and just signs it because it needs to be signed. Some of the large cloud players have already issued press releases and they have updated their documentation. I know that Microsoft has, Amazon has, Salesforce has. So, they all have this ready and they make this kind of agreement available as part of their standard package when they act as a processor for their customers. That's all included with the promise from their side that it has everything that's needed from a GDPR perspective. It may, of course, not be the best option for the customer but still, it's there for compliance purposes.

Let me briefly talk about international transfers of personal data, and on the next slide, I have put the core topics that are in fashion these very days. So, the general principle as I explained is no transfer without additional checks for a legal basis. GDPR says that the level of protection should not be undermined. There are a couple instruments to do these transfers. One of them is the so-called Privacy Shield which is the successor to the famous Safe Harbor regime, which was invalidated by the European Court of Justice some, two years ago I think. Privacy Shield is currently under review and the European Data Protection Authority and the European Commission will publish the results of their review in the next two or three weeks. It's to be hoped that they will agree that the Privacy Shield should be maintained and should not be suspended. But there are some doubts whether Privacy Shield will really survive. There's also some court cases which would take another year before they would really be decided. But there's a lot of doubt whether Privacy Shield is really going to stay in the mid and long term.

Another option is the set of so-called Standard Contractual Clauses. Here, we have the very latest development of last week. The Irish High Court decided that there are also doubts regarding the validity of the Standard Contractual Clauses and they will refer that question to the European Court of Justice. And so, it could be that the European Court of Justice decides that this is not a viable means for transferring data to the U.S. Again, this will not be decided until early 2019, in my expectation. And this would really be the doubt side. If these clauses were to go away, there would be no easily available means left to accomplish these data transfers, and nobody would really know what to do. I just read some statistics that 80% of German companies rely on Standard Contractual Clauses in some way. And if they would fall away then nobody would really know. The good news is that the European Commission is currently working on declaring a few more countries adequate, basically making them equal to E.U. standard and removing all obstacles. It looks like Japan and Korea are very good candidates that could happen by the end of the year, which would make that short list of countries a

little longer than it already is.

If we do a quick check just to tell everybody about supervising authorities on the next slide, there is some guidance on what the GDPR means and how the authorities will actually interpret it available. But the bad news is it's still somewhat limited. There are four official papers by the so-called Article 29 Working Party, which is the club of the European Data Protection Supervisor Authorities that deal with very specific issues. They issued a press release, I think, yesterday saying they also have something on breaches on the international transfers and consent in the pipeline but that's pretty much it for now. There will be, of course, a couple more things by February.

The National Data Protection Authority's individual units are also somewhat active. And, again, depending on the footprint of the company, this is of course of high interest. So, if your company has a London office, then the information commission on the U.K. and their website would, of course, be of significant interest. There's pretty good guidance out there by the ICO, by CNIL, the French regulator. The Germans are trying their best in the German language, of course. And, yeah, it's something to look at depending on the geographic footprint.

A few final remarks before we go into the questions on the next slide. The authorities have publicly stated that they will enforce the GDPR as of May 25 next year and there will be no formal additional grace periods of any kind. In smaller audiences, they will admit that they will not stop actively and proactively harassing companies from that day. So, it's probably more that if somebody complains, they will stop using the instrument they have been given under GDPR. But just for lack of resources, they will not be able to actively chase companies at least as long as you are not Google, Facebook, or some of the other famous names. They may, of course, face thorough corrective enforcement from that day.

Companies, as I mentioned in the beginning, the large companies have started preparing. I think from September, October this year, there's another step in intensity in preparing for GDPR. And the expectation is that from January, everything will go crazy. Companies are updating their controller process agreements with third parties. That's something that often takes time due to the number of contracts. Companies are working on finalizing their data mapping exercise to understand what they are really doing. And we will see an amazing amount of updated website terms and conditions, policies, consent, and so forth in the phase between, let's say, February and May next year.

Member states are updating their national data protection laws. I told you, in the beginning, there's not much left to regulate but those updates are being made. Germany has already done it. The U.K. has just published a large bill. Austria is pretty much done. But there's a lot of companies which are in the middle of updating. So, if you have local offices in European countries, there will be developments there. And that's, unfortunately, another biggie. There's a second piece of legislation that is so-called E-Privacy Regulation which will replace the so-called Cookie Directive, which deals with everything internet and everything telecommunications. The E.U. is somewhat scrambling to find a compromise on the final text of this regulation. The official aim is that that will also enter into force in May 2018, which would give companies a very short period of time to actually prepare for this new regime which would cover everything from cookies to OTT messaging services, and all kinds of other online topics which, of course, are affecting everybody. The European Parliament was supposed to vote on a draft this week but due to a disagreement of the various committees, they have postponed. So, if you open the news in the coming days and weeks, there will be something on this new framework every day. I think it's too early to make predictions as to the content except for it's gonna be bad, hence very restrictive.

I think that's what I had prepared. I'd be more than happy to answer questions for the remainder of the hour. I think we have received some questions a while ago. It's already giving to the presentation. There was one question on the effect on the U.S. of all of these, and possible evolution of the U.S. privacy scheme. Of course, the U.S. is a bit difficult, especially from Europe with the current administration to

make any predictions about laws being changed or modified. I think there is no truly active activity in the U.S. right now to change any national laws. There's probably a bit different perception of national security and the importance of that versus data protection. So, the Europeans tend to be more on the data protection side and they just tend to be a bit more on the national security side. And unfortunately, there is a chance that there will be more clashes. Let's see how the decision was won about the Privacy Shield this week. Next week in October somehow could be next, and the Standard Contractual Clauses could be third.

We also have a question on data privacy impact assessments which is one of the things that have also been introduced with the GDPR. So, the GDPR requires that certain processing activities that are in very broad terms, somewhat risky or more risky than normal for the processing. It undergoes a so-called privacy impact assessment or data protection impact assessment. There's guidance from the Article 29 working party. That's one of the documents that I had on the list on when this should be done and how it should be done. And there's a lot of service providers advertising that they have the ultimate formula on that. There is, from what I'm hearing from the authorities, they are somehow scared to be run over by the enormous amount of these privacy impact assessments. So, I think, there's still some hope that this will be reserved to truly crucial and critical processing activities involving sensitive data like health data or doing real surveillance type of processing activities. But, yes, that is part of the assessment.

Once you have done the data mapping, those high-risk processing activities should be identified and should be scrutinized in more detail. And the result of that should be documented. So, that when the authority ever has any questions that you have that paper trail to document what you do. In terms of what processes can and should actually do, again, this is a new uncharted territory. The controller-processor agreement will typically have language that the processor will assist their controller in conducting this kind of analysis. What that really means in practice, I think, remains to be seen or it has to be determined on the basis of the individual circumstances. The controller should know what's going on because it's the controller's responsibility after all, what the processor is doing. It's maybe that there are certain situations where the processor actually knows more and better about the processing than the controller where the processors will probably have to have some additional documentation of what is being done with the data and how it's being done, which brings us back to the general documentation purposes.

There's also a question on best practices or templates for creating the records of processing activities or the register. There are some templates out there that the French CNIL has published in the Excel file in French, which is available on the CNIL website. Where they have, again, given rather practical keys template approach which is good. The German authorities have also published something, it's not fully officially published but that's available for those who know how to find it. We have an English version of this because we have translated that and we found it difficult just the headings of the respective table to look at it. There are some other organizations, non-BPO or private sectors which have published what they think should be done. So, there's some pieces available but, again, there's no one template that would simply work for everywhere in the E.U.

Dave: Thank you very much, Martin. I think that's probably all the time we have for questions. It sounds like the GDPR is a real evolution of the protection of personal data. It seems like there's some good news in that that it's harmonizing the law across the E.U. The bad news is it sounds like it's a lot of work for our clients to understand the law and how it applies to their operations. And the even worse news is failure to comply could result in new and much larger fines. It also sounds to me like, if you access or handle personal data of an E.U. subject, if you have an office in the E.U. or if your business has E.U. customers where you could indirectly be dealing with personal data from an E.U. subject, you have to look at what your business activities are. And as a first step, map where you're getting the information and what you're doing with that information, how you came to have it, and who have consented. Because it sounds like the thresholds for consent, while we didn't spend time on that, have

increased dramatically as well.

So, with that, I'm going conclude our presentation since we're running out of time. I want to thank you all very much for joining us. We hope you'll join us for our next session on Tuesday, November 7th, where our colleagues will talk about initial coin offerings and the challenges startups should consider before selling tokens in an IPO. You'll receive the information about this topic in the coming week. As a reminder, we'll email a copy of the slides to all registrants. If you have additional questions about any of the topics discussed today, please feel free to reach out to us. Our contact information is on the last slide in the deck. Thank you again for your attendance and participation.

For more information, please contact:

Dr. Martin Braun
Partner, WilmerHale
+49 69 27 10 78 207
martin.braun@wilmerhale.com

David Gammell
Partner, WilmerHale
+1 617 526 6839
david.gammell@wilmerhale.com