**Project Completed by:**

EDUCAUSE

EDUCAUSE Live! Webinar GDPR + 6 Months: What We Know Now,

What We Wish We Had Known Then

November 19, 2018

1:00PM – 2:00PM Eastern

**EDUCAUSE**

**EDUCAUSE Live! Webinar GDPR + 6 Months: What We Know Now,**

**What We Wish We Had Known Then**

**November 19, 2018**

>> Welcome to EDUCAUSE Live! Everyone. This is Valerie Vogel, Interim Director of the Cybersecurity Program at EDUCAUSE, and I’ll be your moderator for today’s E-Live webinar. This event is brought to you in partnership with URMIA, the University Risk Management and Insurance Association. We’d like to thank Mindtree for their sponsorship of the 2018 EDUCAUSE Live! Webinars. Mindtree helps education institutions engage constituents with richer experiences, empower educators, and optimize operations. You are probably familiar with the interface for our webinar, but here are a few reminders. We hope you’ll join us in making this session interactive. Use the chat box on the left to submit questions, share resources and comments. If you’re tweeting, please use the tag #EDULIVE—that’s E-D-U-L-I-V-E. If you have any audio issues, click on the link in the lower left-hand corner. And, at any time you can direct a private message to Technical Help by clicking in the top-right corner of the Chat Pod. A drop-down menu will appear where you can select Start Chat With and Hosts. The session recording and slides will be archived later today on the EDUCAUSE Live! Website. Our webinar today is GDPR + 6 Months: What We Know Now, What We Wish We Had Known Then. The European Union General Data Protection Regulation (EU GDPR) went into effect on May 25, 2018. What has happened in the intervening 6 months? How have colleges and universities dealt with compliance, and what enforcement actions (if any) or interpretations have been taken? We are delighted to be joined by our two presenters from the University of Michigan-Ann Arbor: Sol Bermann, Interim CISO and University Privacy Officer and David Grimm, Associate General Counsel. Thanks to both Sol and David for being here today. And with that, let’s begin.

>> Thank you. Val, for the introduction and while David and I are in the same room, Dave CO-PRESENTING with you again. GP R, six months later this is going to be a Michigan centric journey, the presentation will be in two parts, a rehash of what is GET R and how it affects Universities and what we've done at the University of Michigan and some of the University lessons learned along the way. I'll kick us off and turn it over to legal particulars to David. Let's talk GDP R and thank you, Val for going over the disclaimer. Why GDP R? When I've done this presentation this is always what I'll call the shock and odd slide. Why does it come as a shock to people in the United States? We have a history around privacy and data protection and around the reasons that we care about data ownership and how that fits into our personal lives. The European experience has been tremendously different and I think this slide highlights the whys. Time after time as a trend end usually different context than we have in the United States and we'll get to that. Where does that begin, this European history particularly in the way of World War II and the Cold War? In the wake of World War II we saw that the United Nations declared privacy as a human right and the EU approached privacy differently from then on. The EU came together and Parliament said fundamental rights and freedom took natural persons and in particular their right to privacy. From 1995 on, the digital age, there's already acknowledge that privacy was a human right and for anybody that was a member of the University EU. How do we approach privacy in the United States? Policy speaking we in the privacy world see this as a sectoral approach. We see concern, that could be research and we make a law about it. Now just because we have this legal approach, as I'm quick to remind people we have a number of practices and professional obligations that also stress the important of privacy whether that's the amendment, 4th Amendment, Fifth Amendment, confidentiality expectations with our lawyers and doctors and even though we don't claim privacy as a human right in the United States we have laws and professional obligations because privacy is off value to us. While there might not be a law we definitely feel that it is a value proposition that has began our sectoral approach to laws. What does that mean fundamentally and we broke it down in this way. Here in the United States you can collect data unless the law says you can't. In the EU flip that on its head. It's vice versa and that's socio political background has informed a different approach to privacy, data collection and data usage. Now I'm going to turn it over to David to go into basics and get our tutorial going.

>> Thanks and again welcome everyone and thanks for joining us here today. We're going to have a couple of different components to this presentation. The first will be a backdrop and we'll go into what we learned and on that note about the backdrop, the law in the U.S. is that it's a very different animal to say that you can collect everything unless the law says you can't than to have the EU approach which says that you cannot collect anything until the law says you can. Before GDP R there was the EU data protection directive put into place in order to have a somewhat harmonious approach in the EU as to how data could be processed but the problem was that there was no harmonious regulation within the EU and so when the EU was looking at GDP R they put the approach that this was going to be something that really needed to apply to all. Before GDP R there was a situation with different laws in different countries leading to desperate applications of the University notion that was talked about, the protection of privacy and when GDP R comes around it's intended to make one law for the entire European union and unlike the data protection directive regulate both inside and outside the EU. That's the key difference. The GDP R regulates and as we all know the GDP R became effective on May 2018 and there's a lot of hesitancy and issues with folks knowing so of what the specifics of GDP R are What I'd like to do is break to down to the when, why and what as we go through this background informational piece. The when of GDP R which is really if you are located in the EU it clearly applies to you. However, as I just said if you are outside of the University EU the GDP R also tries to come and regulate what you can do when you are processing controlled personal data and does that by saying if you are offering goods or services to a data subject in the EU or monitoring the behavior of an individual in the EU you may have never set foot in the EU yourself, in both the physical presence is required and that's a big thing that I see when talking with a lot of individuals throughout the country is that it's still not entirely understood that really GDP R really only applies when you are in the EU proper and we'll get to scenarios in a few slides when it will and won't apply to academics in the U.S. and you'll see that come up again and the why is also important. A lot of institutions are sort of asking themselves and have asked themselves over the last six months, why should I worry about a law where regulation is coming out of the University EU when I'm not physically present there and that's a valid question. Notwithstanding the fact that you maybe collecting information within the EU and really trying to get at that information in which case the EU is likely going to argue the GDP R applies to you. The more important one for us at the University of Michigan is that we knew business with a lot of entities and individuals that are in the EU. It applies to not only individuals outside but inside the EU and they will likely try to get the flow down of EU requirements and that's another key component of that and then the what is really a big piece. When we think of TI I here in the U.S. and that's personally identifiable information, we think of things like name, address, home address, e-mail address, social security number but what we don't think of are additional items that the GDP R really adds in to the definition of personal information or personal data, things like IP address, which a lot of website's will utilize to be able to market things to specific individuals depending either on their location or if it's a static IP address you'll be able to determine some other things. You can use cookie IDs which tag individual users and that's why when you are searching Google and you are searching cat litter all cat videos start to pop up But other things you may not thing of as well such as content of exam papers and any information relating to a person is what the GDP R considered personal information. When you think about it in terms of why, what and when the why is an important piece. It's exactly what information constitutes personal information as that term is used in the GDP R. When you look at some situations where GDP R could likely apply in academia, we have three up here and I'll go through them quickly but it's important to understand that this is a purely U.S. institution can still have did GDP R application. Students from anywhere in the world, in the EU, Chinese citizens participate in study aboard in Italy, Belgium and France and those individuals are physically present in the EU and they would have an argument and so would the data protection authorities within the EU that you were monitoring their behavior while they were there and that means the GDP R applies. A campaign is collecting information from alumni residing at the EU. The residency requirement or physical location requirement of being in the EU and then finally a research con /SORGS in the EU. This affects us being a research institution and it's one of those where you do need to be careful with the data that you are taking in from your partner organizations and make sure that the GDP R requirements are in fact met. A couple of situations where GDP R likely doesn't apply, again, that all hinges on the location requirement. Think about a research group made up of citizens who were students at University of Michigan on campus and again it's one of those things where they are EU citizens and they are potentially subject while they are in the EU but when they are on U.S. soil it doesn't apply. If EU faculty are recruited at an academic conference in Florida or in California GDP R likely wouldn't apply. With that, we're going to stop here for questions in case there's questions about the background or the initial discussion that we've had here before we go onto some things we've learned over the last six months.

>> Thanks. It looks like we have one question so far. What about recruiting EU applicants either from on the ground in EU or on their visits to the U.S.?

>> That's a good question. One thing, if they are in the EU while recruiting them I think it's clear GDP R would apply. If they are on advised to the U.S. and you don't take information before they return to the EU which is less likely then GDP R wouldn't apply but if you continue to correspond with them and take information from them, let's say they provide governmental IDs when they are back in the EU then you are getting into situations where likely GDP R is likely going to apply.

>> Great. Thanks.

>> We have a number of questions coming in.

>> Val, you want to cue those up.

>> Do you have any references on the EU that you could share?

>> At the end of our presentations we're going to cover what early interpretations we've seen. The short version is there hasn't been a whole lot yet. Remember this is very new going into effect in May but we'll do updates at the end if that's what Zach meant by references.

>> Of course we can always return to that question if we need to. Is the key point-in-time when the data is collected? What happens if a current student later moves to the EU? Is their current data protected?

>> This is a little right for interpretation and it hasn't been interpreted as far as I'm aware by the data protection authorities in the EU? If you've collected a bunch of information on someone while they live in the U.S. and then they move to the EU, the short answer is there is not a background applicability, sort of retroactive to their time of moving that would apply. The longer answer is it depends and there could be some especially if you are continuing to take information and process that information while they are in the EU even if it was information that was collected before because it's really the processing activities that are the most stringent and looked at most closely.

>> Thanks. And so if an EU applicant comes to the U.S. and later wants to have data expunged is it all the data or just the data in the EU?

>> I think David covered that. It's got to be while they are physically approximated into the EU.

>> What about online recruiting students that maybe received by both U.S. and EU students?

>> I don't know, if you want to take that one.

>> Let's test and see if we have the same answer. If you are recruiting a student whether they are an EU student or not, if they are physically proximate in the EU, GDP R maybe applicable. It is going on at the same time and boundary is irrelevant.

>> Right. I think this really goes to, this question in particular goes to fundamentals of GDP R and you've said this a number of times. A lot of what GDP R is trying to cover is really just good data privacy and good transparency principles and if you are recruiting both students in the same recruitment letter or e-mail blast or what have you, and you are not able to really separate out who is in the EU and who is in the U.S., if you are not able to do that, it's really just good practice to do the things you would do to comply with GDP R even for U.S. students and that's likely short of offering them the rights that are afforded under GDP R but really sort of transparency, that's just good data privacy and good principles.

>> Any good campaign will have some opt in opt out option as well as requirements.

>> I'm going to ask a couple more questions and then maybe we'll hold some of these until the end. This one is about research data on EU residents. Are the people identifiable by the data itself? This is another one where it depends but if you have truly anonymous-ized the data because the test for GDP R is really anything that can identify an individual in any way. If it's impossible then it's safe to say GDP R doesn't apply. Today's day and age almost nothing is impossible when it comes to data especially if you have enough data points you can go back and re associate identifiers with individuals.

>> Thanks. And then two questions that might be related. How is your University tracking data subject to the GDP R and how do you individual subjects GDP R with your processors?

>> We'll talk about that as we talk about how we've gone about GDP R compliance at the University of Michigan.

>> Okay we'll hold off on that one. We're getting a few more questions but I think it would be helpful for you to continue to talk about what y'all are doing and then we'll answer these questions at the end. Does that sound good?

>> Sure. So what is our approach at the University of Michigan? This slides describes the path we took with this but we knew this wasn't a technical solution. We took a people, policy and process approach. Like any good large organization, strictly large higher ed organization we knew we needed to get as much stakeholders together as we could ranging from privacy role, my role, general councils role, David's role, student engagement and enrollment and folks from our clinical organizations and people far in between to discuss what GDP R meant and divvy up responsibilities. We needed documentation around privacy and as we built processes we created a number of artifacts, data registry and technology. In the mayhem that was a ramp up and immediate post May into June and July GDP R craziness we saw vendors promoting tools for a variety of things and we wanted to stay away from those. You can do it without a single technology touch. It might be a lot of people and policy but it can be done and for the most part that has been our approach today. Let's talk about the project itself. We started about three hundred days ago. It seems kind of crazy. We had what we called a core working group and that was myself and David. We also had a project manager and an analyst that could support us and this is somewhat of a rarity at Michigan but we felt strongly that because this was new and there was fear in the AIR around this we wanted expertise so GDP R Cher paw has helped us prioritize our work along the way and stay sane. We had a working group, twenty-five members that we really leveraged early onto both get the word out that, hey, we are working on GDP R compliance as well as they were really the key group we worked with to push out our data surveys to see what data flows we had that were potentially effective GDP R. Some of our major accomplishments, we development a survey and pushed it out and we're getting responses in to date. For folks that say I have a data flow that is maybe going to be impacted from GDP R, from that we of general council with support actually do the analysis to say yes we are impacted by GDP R and looked at what are the business interests that are actually going to be our validation of why we are processing the data. We developed a new approach to compliance going forward. I won't read everything on the list but some significant things we did from a privacy perspective even though GDP R has been a burden on and largely time consuming, we don't know how it will play out for higher ed, it's pushed privacy notice and privacy statements to get us better transparency about why we're collecting data and what we're doing with it and we've developed contracts with vendors and we developed a model that you've seen at some point or another I'm sure as you've gone to website's like CNN, Amazon and asking for cookie consent that those pop up all over the place in the wake of GDP R. And I'll give you a glimpse into all of these items. So, in addition to standard website privacy notice we created an overarching statement that we can refer to for good privacy issues. This is not website specific. This is more of an overarching University statement. I mentioned the cookies closure tool that's been vacant to a lot of our website's at the University. Not all, yet. So as you can imagine as a place that's as large and decentralized as a University part of our program is going to be getting these surveys, the privacy notices, the cookies closure tool, getting those pushed out more holistically across the University. We don't have a single choke point particular around website's that would say click here and we're all done. I mentioned the toolkit and you can see the URL at the bottom there is our website and not only does the toolkit provide links to the template privacy notice, the cookie disclosure tool, but we also actually have a step-by-step process to help our units analyze whether GDP R applies, and if they think it does, they submit a survey automatically into our program site. It may seem simplistic but for us that's a high level of automation and it's pretty exciting. What's in your GDP R toolkit and this by the way we are happy to share beyond this webinar. Any of these tools that you see here, this is the fun part. The wonderful part about being in higher ed is we are a community that is getting and sharing, so while these are made specifically for the University of Michigan we are honored and flattered if you want to use them at your institution and if you want to drop a footnote saying thanks Michigan we're always happy with that too.

>> I'm going to turn it back over to David and talk about GDP R land and while I don't want to say it's Much Ado About Nothing, you will say we've not seen the 4% billion dollar signs yet.

>> Thanks. I think one key is potentially yet and I think over the next several years we'll see the European data protection boards, and the EU trying to go after somebody but we haven't seen that yet. Really there's good news and some not so good news from an enforcement perspective. We'll start with the good news. Nothing substantial yet from the U.S. or higher ed perspective. There's a really good report that was put out by the information commissioner’s office of the University UK on November 6th. I highlight that because it's a really good insight into what the ICO in particular is looking at and how they are going after folks but also it's one of those things where University of Mississippi is actually mentioned in that report as a possible involvement but it was found there was no evidence data was transferred to the University of Mississippi. Note that they are in fact looking wherever the data may lead them and they want to make sure that U.S. institutions whether it be of higher education or corporate entities are in fact complying. As of October, which is the most recent data that we have. That ED Pb announced it has active cross border that are in place with a super set of that being two hundred and thirty-three procedures relating to mutual assistance between D PA's. That number is a little bit lower than some folks had thought but it is indicative that there are cases within particular countries that span multiple countries in the EU. Now we can talk about bigger numbers. The biggest find that I was able to find so far was 400,000 euro and it was essentially -- there's a little bit of backdrop here. It's funny. A Portuguese hospital was fined the 400,000 but it was under a regime where Portugal hasn't integrated GDP R. They are actually applying GDP R where it hasn't been implemented in the country and that's one of those unique situations that's out there. I will say that this is an interesting one. While the actual opinion itself or the backdrop is not publicly available yet so the only thing I could get on this was reporting out. What happened or what seems to have happened was the hospital had around nine hundred and eighty-five accounts in its case management system, which doesn't sound like a lot. The problem was there was only two hundred and ninety six doctors at the hospital. Three hundred percent of user base indicating there were a number of fake accounts in the case management system which lead to staffing psychiatrists having access to patient data and doctors that were in one specialty could see any number of other patients records that were not in specialty throughout the hospital. They were fined 400,000 euro and the hospital is challenging that. Obviously, it's the biggest fine that's been implemented so far. One key thing to takeaway here, there was no actual data breach. There was no proof that there was actual data to have been viewed by the individuals that could have viewed it. It was merely that there was a potential to have exposed personal data and that's what lead to the fine. It's a really sobering opinion once it comes out and I'm hopeful that it's translated so that we can take a look at it but it's one of those situations where it really is a good insight into what the D PA's in the EU and in the E E A are really looking at and it's not just that there was a breach or there was a complaint, obviously, that formalized the investigation into it but then working with, you know, looking at all those different things that come into play around the investigation through that even though there was not necessarily data viewed, they still had this astronomical find for not necessarily having a data breach.

>> There was one twist to that as we found out from our GDP R expert. The PTAs role in Portugal is actually personally funded based on fines. So what that means is there was an incentive for fining because they actually will be able to support their program through it. That's another interesting twist that even as we've normalized GDP R laws, how the D PA's operate are still often country unique.

>> That's a great point. At least from my perspective there's a conflict of interest. The next bullet I won't spend too much time on these but I do want to highlight some of the University numbers. According to the protection board the twenty-five D PA's throughout the EU received about eighteen thousand breach notifications by October. That's a pretty high number and one thing that I think maybe driving at least what appears to be lack of enforcement. There's so many coming in and they all have to be in investigated. As we see the D PA's staff up hopefully in response to this we'll get insight into how these eighteen thousand breach notifications are coming in and how they are going to be looked at. You are getting all these coming in. You are not necessarily getting the full-fledged investigations that are coming out of it and C N L, the French D PA, they received about thirty-seven hundred of those and they are actually pretty involved in a lot of these different things so they are not necessarily spread out equally among all twenty-five D PA's throughout the EU. Finally, C N L announced that twenty-four thousand five hundred organizations just in France alone reported that they appointed D PO and that's about thirteen thousand D POs, data protection officers and because of overlap between organizations because some can have external D PO, not necessarily in the same capacity, that's thirteen thousand individuals deployed in the D PO capacity in France alone which is pretty astonishing given it's only been six months and when you put that into perspective under the old framework only five thousand D POs were deployed in France. Largely, I think that's just because of how well publicized and how well documented this has been. I think everyone on this phone call on may 24th and 25th got about a thousand e-mails relating to GDP R. If the EU just stood downright now, you know, they could declare victory because a lot of individuals have stood up and taken note and gone through a lot of macerations required by the GDP R perspective and the biggest point I think a lot of this makes and I wanted to bring it up, it's not on the slide but I wanted to bring this up. If you look at enforcement that GDP R is going through and it's being challenged in some instances but it's rolling out and it's been enforced and they are fighting folks and investigating, I think potential for a similar law in the U.S. has increased. If you look at California data protection law and if you see other states have separate approaches I think you'll have a potential federal response that. When you are looking for a wall around it as a result of what GDP R has done in the EU and the ED Pb chair gave approach to the U.S. senate as well and we may be looking at that as a fallout of GDP R piece and it's a good thing as long as it's a workable and implementable solution. With that, I'll turn it over to SOL for what we have learned.

>> David covered probably the biggest point. We learned that the EU when they really decide to throw their muscle around can throw some muscle around. The whole world has stood up and paid attention. Not just higher ed. It has been an adventure for us in higher ed. What did we learn here at Michigan? If you are going to do this, get executive support and we had have wonderful executive support. David reports up to the general councils office and for three hundred days we've been providing monthly updates, twice a month updates to our general council and those were shared at the executive council level which is our president. Our president cared that we were taking it seriously, taking actions to mitigate risk at the University of Michigan. We have a very risk based approach. I think all of you know you could spend tens of millions and I think there are companies around the world that likely have, tens of millions of dollars, hundreds if not thousands of hours coming into compliance with GDP R. The amount of people and the amount of days we've spent on it, know this was not a technology project. Almost everything we've done outside the website and mild automation and maybe the cookie consent tool has been a process project. IT security and I know a lot of folks on this call are a part of IT security and a lot of you have been given responsibilities for GDP R and maybe they didn't pushback hard enough. Minimal we should be partnering with our general councils office. I have been working on this with my privacy hat on because it does fall into compliance daily of that role but I would not be doing this without the general counsel’s office and the amount of work David has brought to the table has been amazing. We cannot do this as a vacuum. During our first presentation we left you all the stakeholders we work with and we're happy to share those with you again, folks on the clinical side to folks in the student management office and others. We really tried to focus in a risk based way on processes that had the highest exposure to GDP R and at the conference there was a session and we called out what are the areas to be most likely GDP R? Admissions and alumni development engagements, research, particularly large data sets that might be flowing through that are EU research partners. International programs or study abroad and things like that.

>> We also know that the University of Michigan, this is not a command and control place. We have to provide education and tools and that's that toolkit that you saw. Finally, the other big lesson that this really I think put home for me as the privacy officer at the University is that we really did need more of long-term commitment approach to privacy at the University. This isn't just GDP R and done or common rule and done. Privacy is valued at higher ed and value founded in free expression, student growth and development, academic freedom and we should treat it as such and we have a number of laws in the United States as a privacy value statement. While GDP R is getting even greater than I am, that picture, what it really has helped me do is explain that privacy has to be something we engrain as a University because it's the right thing to do and not just a legal obligation.

>> David, I don't know if you have anything to add but I think if you don't we have about twelve minutes where we can ask more questions.

>> Great. Thank you both. I'll start with do you offer GDP R training and if so, to whom do you offer that on campus?

>> We aren't offering any training right now. I don't know that we will because GDP R affects so many different data areas and stakeholders and constituents. If I had it my way we'd have some sort of broad based data protection and privacy education and awareness and GDP R as a subject would help drive those conversations but the actual training itself, no. What we want people to understand is that we have the toolkit available to them, a program, general councils office if you have questions and a toolkit you can use to get self-help that always ties back to us so we can review privacy notices, review the data surveys.

>> And I think the only thing I would add there and I would potentially use the word training if I did very loosely is folks who are in our O RS P, office research and sponsored programs or procurement, we have sort of talked with them at a high level around what some issues are so they can spot them and bring them back. They are on the frontline's, so to speak and they are going to be looking at those and for them to be able to understand the process in which GDP R applies, they can come back to us as a program team and see what they are seeing and determine whether or not GDP R applies.

>> Thank you. This might be a question for you. What standard are you using to ensure compliance with GDP R rule? In miss standard or something like that?

>> So, that's mainly around the security phase. At Michigan we are striving to be a shop but GDP R doesn't specify this is the requirement we expect you to meet. It's more of a do good security and being able to show evidence of a security program should things go awry. That we haven't solved a miss standard here. Demonstrate a standard as being followed but if you are doing good security and you have it documented whether it's just a common set of framework on your own then having some evident is better than saying I'm making up security as we go along. We were already going down the path.

>> Thanks.

>> I think it's also important to note that security is only one component of GDP R. There's all sorts of other things around consent and legal basis and making sure you are honoring the rights of individuals and security is one component but don't lull yourself into a false sense of security saying we're good to go with GDP R. That's just not the case.

>> That's exactly why some should not be in charge of GDP R if all they are thinking is security.

>> Thank you both. This is more of an observation so perhaps both of you could comment on this. Legal willing to partner and pushback with IT equipped to do the data mapping exercise?

>> I'll try. So is this asking if legal is willing to partner and pushback if IT is the best equipped to do the exercise? At Michigan this has been a partnership. David and I developed the survey. Yes we have from a project management perspective special project support perspective more resources in IT. It's both really well here in that regard. I would hope that if David had said you need to do a survey and because you are privacy guy you need to help resources with this, I would not pushback. I'd say, yes of course or I'd say David, if I didn't have the resources, we need to figure out how to get those resources. A lot has come from my budget. It was easier to get things going from my end because we had the framework in place to ask for analysts and project manager and I had immediate budget to draw on.

>> I just want to say that I don't think it's possible to have done this level of work without a true partnership between SOL and his group and me and O GC. You need both aspects. You need to have that. Again, I don't know what exactly the question is in respect to pushback but I very much view it as a partnership and SOL and I are working to determine what the best path forward is and if either one of us had reservations, we've talked about them and we did all those things and then made sure that we were both on board before we moved forward.

>> I saw Kathy's comment in the chat but you were answering questions so thank you both for that. What is your experience in implementing the consent requirement for sensitive data?

>> I'll answer and then let David get in deeper. This has come up in the context of research and the good news, for all of you who are doing large scale research and you have an institutional review board, the IRB process itself pretty much meets GDP R. If you are doing a good job at the IRB in looking at confidentiality, ability for people to opt out of studies and are part of human subject research studies in particular, you are probably 95% of the way there but I'll let David finish off because we had IRB on a couple of questions.

>> I think that's exactly right. The IRB process gets you 95% of the way there and I think we added one paragraph to our consent to be IRB compliant. When you look at sensitive data, the question is, and you do need to have consent for that. Any data set isn't valid if you don't have all sets of data. That is difficult for folks that are in the IRB approved trials because they are used to signing those consents anyway and getting consent in front of somebody to get information really isn't that different than it has traditionally been. That's been our experience so far.

>> I'd also add that when you think about the legal basis, consent is one that often jumps to mind first. David has been great at cautioning us to not use consent as the legal go to because consent can be withdrawn. When you think about a student application, for example, if it's based on consent they are asking about sensitive information, ethnicity, demographics that could be considered on the GDP R definitions if we're replying on consent that means the applicant can withdraw that consent at any time so be careful with consent.

>> Thanks. Go ahead, David.

>> I was going to say SOL is right. You have to be careful around replying on consent because it can be withdrawn. You want to think about legitimate interests and necessity to enter into a contract as lawful grounds to be able to process information and look at those and see if they apply to your situation because that could give you a better way to retain the data at the end and not necessarily have that consent withdraw. That doesn't get into discussion around what do you do if U.S. law requires you to keep something but GDP R would honor the right to be forgotten? How do you work within the confines? I do want to make sure that that's a key component because it is one of those situations where if you are faced with violating one law or violating another law, the question then has to come down to an institutional analysis of would you rather be violating U.S. law or EU law and that's sort of an institutional decision that would need to be made because if you are in a situation where you have to violate one or the other, it's an unfortunate place to be but I think it's going to be a place we find ourselves specifically if we reply on consent for admissions data and somebody wants to exercise the right to be forgotten.

>> I think that answered a couple of questions about a situation where GDP R conflicts with other law. It sounds like the institution really has to make that decision.

>> Yep. That's exactly right.

>> Great. Thanks. Really quickly, you I'm hoping to get through one more question. I wanted to mention I few people asked about the GDP R data survey that's in your toolkit on the University Michigan website and we shared the link in the chat and it's in the slides and will be posted after this session today but just to let you know the GDP R is restricted to a login and we'll work with SOL and David to get that content and post it so you can see what the survey questions are. I wanted to let the group know about that. I'll try to ask one more question. Actually, I've got a minute left. What's been your experience with best practice, personal data or exercising the right to be forgotten?

>> Thankfully we've not had anything but automated what I'll call removal spans. Again, if you were at the EDUCAUSE national conference, this is referred to there. Our GDP R sites are you can upload an auto template span that says please remove me. We've not received a legitimate request. We're not even following up with what we can clearly say our automated responses are. Channels we've established and of course we'll review them.

>> I don't want to take too much time but I think that the key there as well is don't be afraid to ask for validation from the individual who is asking for it especially with data portability because you get spam or malicious request to delete data to someone. Now not only are you not complying but you are in a breach situation as well so always be careful.

>> Thank you both. Be careful. Thank you both. I know we didn't get to go through all of questions. I apologize for that. If you have questions you still wanted answered, feel free to e-mail us. On behalf of EDUCAUSE, URMIA, and our speakers, this is Valerie Vogel, and I thank all of you for joining us today for an engaging session and conversation. Before you sign off today, please click on the session evaluation link—which you will find in the bottom left corner of your screen. Your comments are very important to us. The session will be archived on the EDUCAUSE Live! Website, including slides and a complete replay. Please feel free to share it with your colleagues. And finally, please join us for the next E-live! Webinar on Thursday, December 6, to hear from our research team about Today's Higher Ed IT Workforce, 2018. On behalf of EDUCAUSE, this is Valerie Vogel. Thanks for joining us today for EDUCAUSE Live!

**End of Webinar**