NAVIGANT

On Healthcare

HEALTHCARE

THE IMPACT OF THE GENERAL DATA PROTECTION REGULATION ON HEALTHCARE

Announcer: Welcome to Navigant On Healthcare, offering insights for healthcare leaders striving for success in an evolving industry.

Host: Welcome to Navigant On Healthcare. I'm your host, Alven Weil, and today we're joined by Brian Segobiano, an associate director at Navigant's life sciences risk and a compliance practice. An expert in data governance, Brian helps clients manage their enterprise information by developing solutions to support analytics, legal and regulatory investigations, data privacy and security programs. He's particularly focused on helping clients build and operationalize programs to demonstrate compliance with the European Union's general data protection regulation, or GDPR, as its commonly known, and it happens to be the topic of today's podcast. Welcome Brian.

Brian Segobiano: Thanks, Alven. Appreciate the introduction and pleased to be here today.

Host: So, Brian, can you provide us with some background on the GDPR, what it is, and how it impacts healthcare and life science organizations both in the EU and the U.S.?

Brian: Yeah, absolutely. I'm happy to do that. So, the GDPR, the general data protection regulation, is a comprehensive privacy regulation that governs the processing of personal data of individuals within the EU. So, I think just kind of setting the table, the background for it, sometimes it's helpful just to understand the history of privacy in Europe, which goes long before the GDPR. So, really today it stems from a concern over certain atrocities that occurred actually back in World War II, the way that personal data was used to have the significant and devastating effects on individuals.

SPEAKER

BRIAN SEGOBIANO

Associate Director
Navigant
+1.312.583.2749
brian.segobiano@navigant.com

navigant.com

About Navigant

Navigant Consulting, Inc. (NYSE: NCI) is a specialized, global professional services firm that helps clients take control of their future. Navigant's professionals apply deep industry knowledge, substantive technical expertise, and an enterprising approach to help clients build, manage and/or protect their business interests. With a focus on markets and clients facing transformational change and significant regulatory or legal pressures, the Firm primarily serves clients in the healthcare, energy and financial services industries. Across a range of advisory, consulting, outsourcing, and technology/analytics services, Navigant's practitioners bring sharp insight that pinpoints opportunities and delivers powerful results. More information about Navigant can be found at navigant.com.

At that point, Europe said things like this can never happen again. There started to become a series of different disparate country laws enacted, and the most recent regime that Europe is under is called the Directive 94/95. What the directive is, that's really a set of guidelines on how personal data can be processed by companies. Each of the local European member states would adopt a different, somewhat disparate version of how the law would work within their country. Certainly, a lot of things changed since back in 94/95. The Internet was not what it was today. Organizations were not as digitized as they were. In a single household, you may have one person, or one computer, where there are multiple people logging onto, as opposed to today where a single individual has many devices. On top of that, the different country laws were, as I said, very disparate, a lot of conflict between what was allowed and required in one country versus the other.

So, the GDPR was meant to harmonize all those and truly be a regulation that was uniformly adopted across all the member states. So, what's so significant about it is the material, territorial and personal scope. On the material side, it's not simply focused on the processing of customer data. This is any person, whether they're a customer, an employee, a contact, a vendor, etc. so it's very broad in that sense. Territorially, it covers any individual within the EU. So, for even U.S.-based companies, if they do not have a presence in EU, it's important to know that if you are offering goods or services to individuals within the EU, even if you do not have a physical presence there, this is something that applies to you.

Lastly, the personal scope is very much expanded. I think, if you're looking from a U.S. perspective historically, we kind of think of personal data as the more sensitive items that could have an extremely negative impact on us if they were breached, whereas personal data under the GDPR is much more broad. It's just name, contact information is considered personal data, even an IP address, or an online identifier is considered personal data. So, very broad in that sense. The GDPR defines certain principles about how this information can be processed, that has to be done in a lawful, minimal, a transparent manner, and there's very significant fines for noncompliance. There's requirements, such as doing things like creating data inventories and conducting certain assessments and maintaining a set of policies and procedures that organizations need to have in order to demonstrate compliance.

So, U.S.-based organizations certainly need to be aware that, even though they don't have that presence, that this is something that likely impacts them if they are providing goods and services to the EU, they should start to assess their current posture. What data do we have? What elements are personal? Where does it live? How long do we keep it? Who do we share it with?

I think for healthcare and life science organizations, obviously there's going to be a particular focus on the clinical data that we're collecting, whether it's trials for pharmaceutical and medical device corporations, or if it's the other clinical data that healthcare providers may have on hand. As you start to go through your journey of where you're likely on a path of becoming a digitized or more a digital organization that's connecting directly with your consumers, how do those future plans in your digital roadmap impact the personal data that you may not house right now, but that you plan to in the future?

Host: So, I think most of us have heard of HIPAA regulations. How is the GDPR different from HIPAA?

Brian: Certainly. So, there's a number of ways where the GDPR is different than HIPAA. So, first on the material side. Obviously, HIPAA covers in the U.S. what we call the protected health information, where the GDPR covers what they call "personal data," which is an incredibly expansive definition that includes something as simple as a name or a contact information, an IP address even. It's anything that makes an individual identifiable as the specific terminology. So, even if it's not a direct personal data element, if we can use that information to cross-reference with another data set and identify that this is, in fact, Brian here, that can make someone identify one of the GDPRs materially, there's certainly differences there.

Territorially, HIPAA is obviously under a U.S. regime, whereas the GDPR covers the EU. I want to clarify that there's often a misconception that it's European citizens that are covered under this and it's actually anyone within the

border of the EU. So, Brian is a U.S. citizen. If I go over to the EU, I am covered by the GDPR, whereas an EU citizen who is outside the EU at that time is not covered. So, the territorial scope is a bit different, as well. On the entity that it's looking to enforce upon, the GDPR divides companies in what they call controllers and processors, depending on if they are deciding what they call the means, the processing, of the personal data, whereas HIPAA is looking more closely at a specific set of what they call covered entities and the BA agreements that are associated with those.

Then, one final difference is that HIPAA focuses heavily on the disclosure of information. So, understanding that it doesn't cover as much the collection and the storage of it really on the disclosure to other parties, where the GDPR really covers the entire data lifecycle, the collection of information, notification you give the individual when it is collected, where it's stored, transferred to, how it's used, all the way through the final disposition of the data. So, very expansive lifecycle that is covered of data management under the GDPR.

Host: So, Brian what are the most critical actions organizations need to take in order to comply with the GDPR?

Brian: Yes, I think the critical actions are going to depend on the risk profile of an organization and it can change wildly from a pre-commercial to a commercially-operated entity, but the key starting point is the data inventory and that's something required under article 30 of the GDPR. This is basically a registry, or a matrix, of all the processes that impact personal data of EU individuals throughout the organization. Identified attributes like:

- Who is the information about?

- Is this about patients, or employees, or customers?

- Where is this information stored?

- Who else has access to it?

- How long do we keep it around?

Things like that…So, really building that inventory sets the landscape and you can start to assess where your risk areas are.

From there, conducting what are called data protection impact assessments, or DPIAs, are another requirement of the GDPR. Taking those highest risk or those most sensitive processes. Again, looking things like your clinical data or broad data about your entire customer or employee base would be good areas to start to focus on doing a deeper dive to understand if you have any potential compliance gaps. From there, you're at a good spot to start remediating what those gaps are that are in a risk-based approach. Those remediations could be things like making sure that we're updating our notification or our informed consent for our patients, ensuring that you have a mechanism to handle what are called data subject rights.

So, under the GDPR, individuals may have the ability to request and receive from an organization erasure of their personal data, transfer their data or access to their data. So, making sure you understand what all those different rights are and there's more than just those that I listed. Something in place to handle those is key. Then you start to look at your retention of the information. Can we start to purge data from our systems? Which, while burdensome, really, when you start to look at a security landscape, at a legal risk landscape, starting to purge unnecessary data is really a good thing for your corporate housekeeping.

From there, focusing on what are our other specific risk, what are our third-party risk, do we have processes in place to make sure that our vendors are treating the data in a compliant manner as well. And then forward looking, especially within the healthcare life science space, going back to that customer journey as we start to explore more ways to have connected health, combination drug device products, IoT in general, telemedicine… All those things that may be on the roadmap are incredibly commercially beneficial, but we need to make sure that we're not increasing our compliance risk as we go about collecting that personal data.

Host: So, what areas would you say companies have faced the most significant challenges implementing and operationalizing programs in response to GDPR?

Brian: That's a great question. I think it certainly varies by industry. I do think that, what I've generally found, is that within healthcare and life science organizations there is a bit of a good foundation of a culture of privacy just given what the value proposition is there, but some things that are difficult even within the healthcare life science industries is that journey of moving from what we call a culture or a people-managed privacy program to adopting and following more formalized policies and procedures, and then ultimately into something that's technology-driven and automated -- what we'll call a fully-integrated compliance and privacy program. I think that change management process can be difficult.

So, I think, going through that initially, what we need to do is develop some documentation policies and procedures and we're relying on training, but we need to have a forward-looking focus on:

- How can we automate and build a roadmap so that all of these requirements aren't living in disparate silos?

- How can one requirement feed into the other and it makes it easier and the organization is enabled to be privacy-forward?

So, I think another area that seems to be a struggle is because you start to work with other entities. It's remediating contracts and third party, or customer agreements. So, many organizations are going through this whether they are the one that controls the data or they're using a processor and they're reaching out to one another to say we need to add certain addendums on to our agreement we have, and one party may have some preferred language. Another party may have their own preferred language. So, I think that process of remediating those contracts to get the proper clauses in there, proper protections, the back and forth on what's acceptable to one organization versus another can be another difficulty that an organization needs to work through.

Host: What are some successful approaches you've seen from clients with whom you've worked in developing GDPR programs?

Brian: Yeah, another great question. So, one of the key things I would say has been successful for clients that we work with at Navigant is establishing what we call privacy office. So, this is a representation of what we call liaisons from different parts of the business. They should represent the different functions throughout the organization. They should represent the different data subjects that information has collected on. They should represent the different geographies where the organization works, bringing this group of liaisons together to socialize, enhance, adopt and roll out the policies, procedures or documentation, the three that are required of the GDPR, is very successful. Really having this be a ground-up approach where those key stakeholders provide feedback on:

- We're developing the new privacy policy...where do you see the difficulties may be for us to follow this, or where can we enhance this?

- How would this work for our HR function, our customer-facing function?

Things like that are important. The next one I'll mention is integrating with other key initiatives that are data governance in nature throughout the organization. We've talked about privacy, but really this is a data management issue, as opposed to specific privacy issue. You'll find in global organizations that legal is more than likely going through some type of a transformation, or efforts to streamline their processes for things like legal discovery and in case management. Your IT team and your security teams are probably going through a data governance classification security assessment exercises and really the heart of all of these things is just understanding what information we collect as an organization and how is it governed, protected, shared...things like that. So, bringing together those other key stakeholders while upfront can put a few more people in the room and may develop different opinions and can be political. For long-term success in an organization, it really does need to be an integrated part of your broader data governance strategy and then even above that your digital strategy as a global organization.

That takes me in saving the last key, which may be the most critical one, but it's identifying the commercial advantage of privacy. So, there's no taking away that regulations like this are costly. They're burdensome. They put strain on the financial and the human capital resources of an organization, but looking long-term, I think a great analogy is something, like we talk about eco-friendly organizations. Years ago, there were a number of regulations passed that were burdensome for corporate organizations to put certain policies and procedures and protections and agreements in place to be more eco-friendly, or green. We kind of fast-forward to today and that's really advertised now by those organizations to the commercial advantage. We want to do business with organizations that are green, or eco-friendly, or even just good corporate citizens that go out and do right in the world. I think in the healthcare and life science space, this can be particularly advantageous. We're helping to enhance and protect the health of consumers and we also want to assure them that their privacy is protected, especially when we're going on that digital journey of things like telemedicine, more direct consumer engagement, connected devices, connected medical products. It's important that we reassure the patients that -- in addition to helping with your health -- we're also protecting your privacy. So, I think that advertising that as a commercial advantage is a good proactive way to start engage the rest of the business beyond legal or compliance or IT, whoever's owning the initial adoption of GDPR, to get the rest of the business to buy in.

Host: Brian, one last question for you. Now that we are beyond the May 25th deadline, what do you see is the next operational challenge for organizations related to emerging laws, business and technology?

Brian: Great question. So, looking forward, now there's -- most organizations are in the state, at least that we're seeing, where there's probably been, especially recently, maybe a bit of a scramble to develop a lot of documentation, new policies, new procedures, new documents. Some of that may have been done in somewhat of a silo within the compliance function, but looking forward, this has to start to become a part of that broader data governance structure in an organization. So, if they have not already, they're starting to take the privacy program and engage the security teams, the legal teams, analytic teams, other customer-facing parts of the business and embed and bake privacy into operations and find synergies within that.

So, I think part of that is also identifying where technology may be useful to run the program. So, many organizations may have built a data inventory in Excel, or conducting data protection impact assessments and remediation plans, just managing them through loosely shared documents and email, but these requirements are this is not an end date. This is really just a beginning for privacy. So, these requirements are not going away. So, where can there be technology or tools to facilitate that process of -- we need to continue and update those inventories, conduct assessments, hold people accountable for the mitigation actions? There can be software providers that may be able to help in that space. Then, looking for in that sense, its continue to maintain the program. As we said, this is a beginning, not an end. So, the next time we're developing a new process that involves personal data, it should flow through that evaluation process where we're doing assessments of it when we need to. We're putting in our data inventory. We're remediating third party vendor contracts, where necessary.

Along those lines, it's continuing to monitor the landscape for emerging regulations. So, GDPR is incredibly extensive. It impacts, certainly the EU and organizations doing business in the EU, but we're seeing a lot more regulation emerging in the U.S. So, it's adopting components of the GDPR. So, for example, the data breach notification under the GDPR, there's a very tight 30-day window to notify supervisory authorities of the personal data breach and we're seeing in states, like Florida and Colorado, where those things have been mimicked. There's a number of pending legislation out there in different states like California that are evaluating the potential to adopt certain data subject rights and other iterations of those things. So, monitoring that landscape is key for organizations going forward, and to be able to proactively plan for privacy.

One additional piece of legislation we should certainly discuss here is the California Consumer Privacy Act, which was recently passed in certainly what was a bit of a rush. This is significant because it's the most comprehensive U.S. privacy law, much more comprehensive than some of the explicit ones we talked about like state data breach laws and introduces a number of those GDPR requirements to the U.S. It will impact organizations that have customers and others that they do business with in the state of California. It will not go into effect until January of 2020, so there's some time.

There will certainly be some changes that happen, but it's relatively clear, at least, what the key attributes of the law are at this point. Things like having the registry, the processing activities, providing notice to individuals whose personal data is processed, having a mechanism for those individuals to request access to their data, information about the data, to lodge a complaint, potentially. There is a particular section that focuses heavily on we'll call the "data economy," or organizations who collect personal data of individuals and then profit by sharing and reselling that information. Often not, something that our healthcare and life science clients are engaged in, but certainly if that is something that's a part of your business, you will want to be aware of this law. Like the GDPR, it expands the definition of personal data to individuals that can be identifiable, not simply no covering PHI, or data under HIPAA. The data subject rights and the control of their data are surely enhanced by this law and that seems to be something that will certainly remain.

In some cases, going back to the data resellers, the organizations may be required to reimburse or offer some of their financial incentive to individuals whose personal data they're reselling. So, for organizations that have already gone through a GDPR assessment and implementation, they think a lot of this is just geographically porting some of policies and procedures and documentation to include California and maybe more in the U.S. as time goes on. If you have not, I think this is the time to start developing those data inventory, so you understand what data you have in your organization, where is the personal data, where is it flowing, how is it protected, who are we sharing with, those types of things that will give you a good baseline to begin evaluating your organization against the California law and also the coming laws, like those that are sitting right now in the U.S. legislature.

Host: Brian, extremely informative stuff. Thank you so much for your time.

Brian: Appreciate it, Alven. Thank you very much.

Announcer: That concludes today's episode. Be sure to check in with us for future installments of the Navigant On Healthcare podcast series on navigant.com/healthcarepodcast. Navigant On Healthcare is a podcast series produced by Navigant's healthcare practice. If you enjoyed this episode, please share with friends and colleagues on social media. Learn more at navigant.com.

linkedin.com/company/navigant-healthcare twitter.com/naviganthealth

©2018 Navigant Consulting, Inc. All rights reserved. W75856

Navigant Consulting, Inc. ("Navigant") is not a certified public accounting or audit firm. Navigant does not provide audit, attest, or public accounting services. See navigant.com/about/legal for a complete listing of private investigator licenses.

This publication is provided by Navigant for informational purposes only and does not constitute consulting services or tax or legal advice. This publication may be used only as expressly permitted by license from Navigant and may not otherwise be reproduced, recorded, photocopied, distributed, displayed, modified, extracted, accessed, or used without the express written permission of Navigant.