Crowe

Q&A

Privacy on Steroids

Why U.S. Financial Executives Still Need to Focus on GDPR

An Interview With
Pamela Hrubey of Crowe

The European Union's General Data Protection Regulation (GDPR) came into force on May 25, 2018, leaving more questions than answers for senior-level financial executives in the U.S. regarding how the new regime could affect them.

Financial Executives Research Foundation (FERF) spoke with Pamela Hrubey, a managing director in the Crowe risk practice, regarding GDPR, why U.S. financial executives should care about it, and what an organization should do now that the compliance deadlines have passed.

FERF: How would you summarize the General Data Protection Regulation for nonexperts?

Pamela Hrubey: I would say at a high level that the GDPR replaces the former EU Data Directive, with more focus on compliance. The GDPR is aimed at protecting the personal data of residents of the EU. Of course, it also applies to anyone doing business in the EU.

The regulation itself is focused on highlighting the importance of the rights of an individual. Various reports about the GDPR note that people have the right to be forgotten. They have a right to be given much more detailed information about the personal data that a company might hold about them. New requirements for best practices in information security also must be addressed.

The GDPR takes existing privacy regulations and amps them up – puts them on steroids, if you will – and for the first time puts data subjects clearly in an ownership position regarding their personal information.

Of course, many companies have focused on the fines and penalties for not complying with the GDPR. The notion that a company would pay 4 percent of its annual global revenue as a fine or up to 20 million euros, whichever of the two is larger, certainly draws a lot of attention to the regulation.

FERF: Why should a U.S. company focus on GDPR compliance if it's a European directive?

Pamela Hrubey: I think this is a very important question. European regulators have clearly stated that the GDPR applies to anyone who is either doing business in the EU or who is processing the personal data of a resident of the EU. EU regulators have signaled in the language of the regulation – and in their communication with U.S. regulators and in discussions in the press – that they fully intend to address noncompliance with the scope and obligations that are outlined in this regulation.

The problem with challenging the applicability is that an organization may be openly tagged as noncompliant and thus suffer reputational damage even if it were to win a compliance argument over the longer term. I have heard some other experts say that this "take-it-up-in-the-courts" approach is unlikely to work because of the precedent that the U.S. has set with broadly applied U.S. laws such as the *Foreign Corrupt Practices Act*, which applies a very broad compliance brush to companies in the EU and elsewhere.

I suppose that U.S. companies overall would be well-advised to consider changing consumer expectations regarding privacy and data protections and at a minimum putting in place a strategy for addressing at least the key elements of the GDPR in order to protect their reputation.

FERF: Most of the discussion around GDPR is focused on customer-facing business lines. How does that compliance touch the finance suite?

Pamela Hrubey: It might help if I give a specific example that highlights the importance of compliance-related leadership and support coming from the finance suite.

Compliance with the GDPR requires many functional areas within an organization to look at their existing policies and procedures. Certainly, you're right that media attention has been on the data subject rights that a consumer has under the GDPR, but there's also a big risk lurking in most organizations that probably should receive the same amount of attention or even more.

That risk, and thus this example, relates to doing business with third parties. Often, at least in my experience, the finance function ends up with at least partial responsibility for procurement-related activities. Maybe it's reviewing potential third parties to determine a short list that a business executive might then review, or perhaps the responsibility is associated with ensuring an appropriate contract is in place, recognizing that the contract is likely going to come from the legal department.

Certainly, the third parties that organizations work with also are accountable to follow the GDPR under this new regulatory structure. In the end, when there's an issue, the organization hiring a third party ultimately is the accountable entity. The headlines will say, "A data processor working for this important company had a data breach," and then all the text after that is about the important company, not that data processor. It's really important that an organization has a strong third-party oversight capability. I want to say again, it is very fair and appropriate that business functions play their role in that process, but most of the time the third-party due diligence and all of the oversight of the relationship – forming the relationship and maintaining the paperwork – lies in the finance function. Finance, then, and financial leaders have a huge responsibility. They figure out how to make due diligence, contracting, and ongoing oversight as easy as possible and as inexpensive as possible so that the organization is protected in the increasingly networked way that organizations work.

FERF: Given the fact that it's coming out of the EU, given the fact that there are all these underlying separate issues that could touch on the finance suite, how would you describe the state of readiness for the GDPR among U.S. companies?

Pamela Hrubey: I suppose the biggest factor is that, to be fair, the GDPR is complex and very detailed. Compliance is challenging, just from the scope of the GDPR and the parts of a typical organization that the GDPR touches.

Another factor is that some companies started their efforts to comply after waiting to see if the European data protection regulators were going to come out with something more specific that defined or demonstrated what compliance looks like. I'm going to come back to that in a moment. The other factor – perhaps the major factor that remains – is that some companies may just have believed, at least for a period of time, that the GDPR didn't apply to them. As time goes on and more information filters out, the need to comply has become more clear, I think, to many companies.

Back to this notion of the European regulators coming out with more specific guidance about what compliance looks like. Indeed, the chairperson of the European Data Protection Board says that entity – the EU group of leaders responsible for oversight of the GDPR – intends to continue to come out with guidance documents that will clarify expectations. The guidance documents tend to be fairly lengthy, so they don't come out very quickly. When they do, they provide some helpful content. I think it's worthwhile continuing to watch for those guidance documents and keeping an eye out for the lessons they might include.

FERF: What should U.S.-based financial executives be looking for as far as compliance with the fact that the deadline for compliance has passed?

Pamela Hrubey: European regulators and, in fact, the chairperson of the European Data Protection Board have come out hawkishly stating that there is no grace period for implementing the GDPR. Someone sitting today who has done nothing is in a position of risk. That said, regulators are not staffed, for the most part, to implement spot inspections or even to conduct compliance audits unless a data subject has actually made a specific complaint.

Financial executives are in a strong position to help their organizations understand the importance of complying with the GDPR from a reputational standpoint and to remind their colleagues about the importance of paying attention to third-party relationships, recognizing that the typical organization that does business in the EU probably is not immediately in the crosshairs of the regulators. That said, it is time for organizations to start working on the GDPR if it applies to them and they have not yet done so.

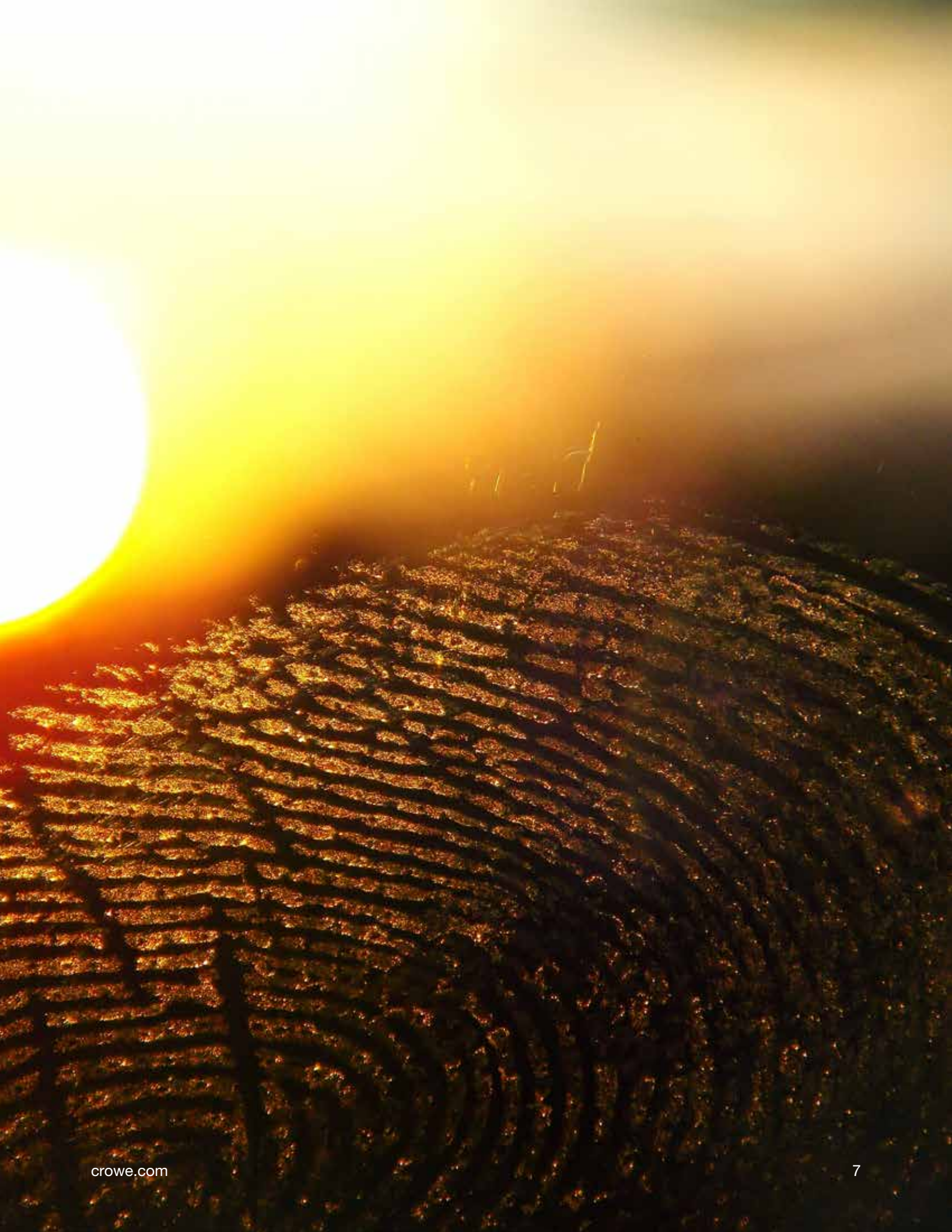
FERF: What advice do you give to a company looking to play catch-up in terms of GDPR compliance?

Pamela Hrubey: I suggest that a company conduct a high-level GDPR gap assessment – often with external resources, because there tends to be a limited number of GDPR experts within any specific organization. That gap assessment gives a company the opportunity to understand where its biggest issues might be. With those biggest issues come the biggest risks. Then a prioritized project plan can be prepared, and an organization can begin to work through that plan.

In the case of the GDPR, it is so important that an organization not let perfect compliance be the enemy of good compliance. It should just get started. Document all efforts. Document the rationale for the risk-based decisions that it makes as it goes about attempting to be compliant. Just get started.

Finally, companies should not be afraid to put something in place now that they know going in must be improved upon later. This point, I think, is hard for financial executives, who are charged with making investments in programs like this really worth their while, really worth the cost. Too often I see companies that want to make a perfect solution so that the business is affected as little as possible so that the reputation is protected – all the right reasons. There just becomes an ongoing gap that is harder and harder to close as time goes on.

Any effort that a company can make, even recognizing that it's not perhaps putting in place the ultimate solution, is probably better than waiting for some project team to build the perfect mousetrap.



Learn More

Pam Hrubey
Managing Director
+1 317 208 1904
pam.hrubey@crowe.com

This Q&A discussion originally appeared on FinancialExecutives.org in July, 2018.

crowe.com

AUDIT-19002-002D