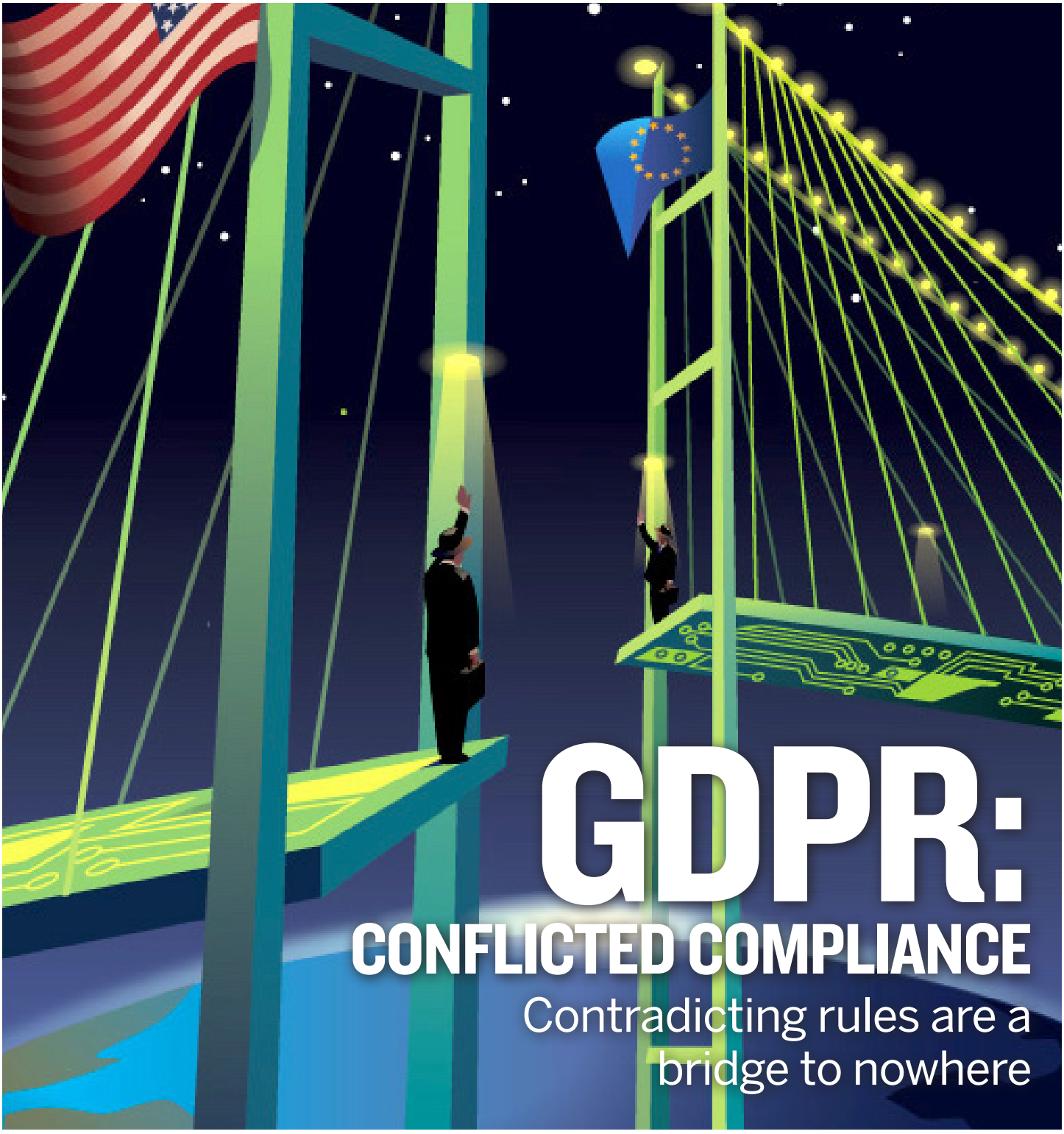

GDPR:
CONFLICTED COMPLIANCE
Contradicting rules are a bridge to nowhere

Illustration by Kim Johnson

ebook

An SC Media publication

Sponsored by

RSA®

How GDPR will conflict with, well, almost everything

Balancing governance, risk and compliance is complicated enough in the U.S., especially for companies in highly regulated industries. Throw in international requirements and now you're dealing with regulations that contradict U.S. regulations directly. Evan Schuman explains.

As CISOs struggle with preparing to comply with the imminent demands of the European Union's General Data Protection Rules (GDPR) in May 2018, they are having to deal with some inherent contradictions between Europe's view of security and privacy and that of the U.S government and industry compliance regulations.

Consider the EU's Right to be Forgotten (internalized within GDPR) versus U.S. Treasury rules for bank financial records to be kept for at least seven years. Or consider the same Right to be Forgotten versus the U.S. Combat Methamphetamine Epidemic Act of 2005, which requires purchasers of the over-the-counter medicine pseudoephedrine, commonly known by the brand name Benadryl, to be tracked via a federal database. Could an EU citizen demand to have overseas money transfers to a Swiss bank account deleted or to have unlimited access to congestion medications, contrary to U.S. rules or laws?

As a practical matter, most observers argue that GDPR regulators will likely bow to reasonable law enforcement concerns such as the drug and financial record examples. But it gives a peek into the rough road many U.S. CISOs will have to travel as they try and become GDPR compliant.

That said, the minefield for a multinational company CISO trying to avoid GDPR conflicts is vast, circling U.S. federal laws, federal agency rules, state laws and state agency rules, municipal laws and municipal agency rules and even industry rules such as Health Insurance Portability and Accountability Act (HIPAA) for healthcare and Payment Card Industry Data Security Standard (PCI-DSS) for payments, as well as the same groups of rules/laws in every country, including GDPR conflicts within Europe.

For the most part, though, other than some law enforcement data retention requirements, the conflicts are matters of severity (such as how quickly breaches must be reported or how long data should be retained) as opposed to outright conflicts. Much of the controversy involves GDPR's expansive definition of Personally Identifiable Information (PII).

"Given that GDPR dictates stricter handling of PII, it seems highly unlikely that you would find a law anywhere that *requires **less*** strict keeping of data," says Anne P. Mitchell, an attorney specializing in e-mail law and the author of section 6 of the CAN-SPAM Act of 2003.

Although, Mitchell says, some aspects of GDPR — such as thinking of an email address and an IP address as PII — reflect "a dramatic change from (U.S.) law."

"No other privacy law in the world matches its breadth and scope, and the compliance obligations it imposes on covered organizations are more granular and exacting than anything that came before it," says

OUR EXPERTS: GDPR

Bret Cohen, attorney and partner, Hogan Lovells US LLP
Barak Engel, CISO, Amplitude Analytics
Philip Gordon, co-chair of the privacy and background checks practice, Little Mendelson.
Christoph Luykx, director of government relations for EMEA, CA Technologies
Anne P. Mitchell, attorney

GDPR

99

Number of articles in the 11 chapters of the GDPR text

– European Union

Washington, D.C.-based attorney Bret Cohen, a partner with Hogan Lovells US LLP.

Mitchell adds that GDPR's stated jurisdictional scope is also a sharp change from current approaches. "It fairly uniquely specifically states that it applies to anyone anywhere in the world. What GDPR does is it forces everyone to finally comply with the laws of the receiving industry."

Anne P. Mitchell, attorney

The absence of direct conflicts, however, does not mean the absence of impressively awkward policy conflicts when it comes to GDPR.

"Speaking specifically to email, as that is one of the primary places — other than HIPAA — that U.S. federal law comes into play in terms of handling PII, GDPR is much stricter in terms of the requirements for acquisition and handling of email addresses, so, in that sense, there is a conflict between the U.S. federal law and GDPR," Mitchell says. "In the U.S. it is acceptable and permissible to acquire someone's email address through any legitimate means and put it on a mailing list. I hasten to add that the U.S. is just about the *only* first-world country that permits this," she notes.

> "I don't call it a conflict. I call it a different approach."
>
> *– Christoph Luykx, director of government relations for EMEA, CA Technologies*

"However, up until now, it didn't necessarily rise to the level of a conflict with the laws of other, similarly situated countries — Canada's CASL (Canada's Anti-Spam Legislation) comes to mind — because, for the most part, each country's laws are focused primarily on businesses and citizens located in that country," she goes on. "GDPR very specifically states that the GDPR applies to any email sender, wherever in the world they are located, if they send email in violation of GDPR to a resident of the EU, and GDPR gives a private right of action to residents of the EU. Taken together, these two suggest that CAN-SPAM and GDPR are in direct conflict, as CAN-SPAM permits what is known as 'opt-out' email marketing and GDPR requires explicit opt-in."

The trap is that most email administrators can't keep track of all of the required GDPR categories. "For many email addresses on many mailing lists, you can't possibly know where the user is actually located," Mitchell says. "So *not* complying with things like CASL and GDPR and instead relying on CAN-SPAM in terms of how one handles email PII, is email Russian roulette."

A similar perspective is offered by Christoph Luykx, who is a Brussels-based government lobbyist for CA Technologies with the official title of director of government relations for Europe, the Middle East and Africa (EMEA). Asked about GDPR differences with data requirements in the U.S. and elsewhere, Luykx says "I don't call it a conflict. I call it a different approach."

Given that the differences between GDPR and other rules are matters of severity or timing, Luykx says some CISOs might be tempted to separate data involving EU citizens and anyone who happens to be situated in an EU country at the time of an interaction.

But he questioned how practical that would be, giving an example of dealing with different breach disclosure timeframes. "What are you going to do? Report after 72 hours to the Europeans and wait to report to (U.S. states)?" Luykx asks.

52%

Percentage of UK businesses that believe GDPR will have little or no impact on their company

– 4D Data Centers

That forces the issue of definitions. The breach disclosure section (Article 33) seems to spell out obligations precisely: "In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons."

And yet, how specific is that? With a data breach of a Fortune 1000 company, what exactly does "having become aware of it" mean? Is that the moment someone in IT noticed some unusual activity in a traffic log? When it was reported to a supervisor? When it was reported to the CISO and CIO as a possible but far-from-confirmed breach? Or is the company not "aware of" a breach until the final forensics report confirms that it actually happened, potentially months after the first pattern deviation was noticed by an employee?

Or could the company be "aware" only when the CEO is briefed? Or does it wait until the CEO is convinced of a breach, rather than merely being told? Yes, awareness is anything but a precise point — so how could 72 hours after "awareness" be at all clear?

"In an ideal world, you immediately know that there has been a breach," Luykx says, adding that that isn't how the data world works.

Christoph Luykx, director of government relations for EMEA, CA Technologies

Luykx says that GDPR, while problematic, is only one of his current global compliance headaches. In Japan, for example, there is the Personal Information Protection Commission, which recently changed its name from the Specific Personal Information Protection Commission. (Did it decide that "Specific" was a little too specific?)

But that Japanese data effort itself is more concerned with what other countries are doing. Its homepage details active meetings with privacy/data officials in Australia, the Czech Republic, Luxembourg and New Zealand.

"There are tons of uncertainties around this right now and that just makes everybody's job harder," says Barak Engel, a veteran CISO who just published a book called *Why CISOs Fail Security*. Engel's held the CISO and CTO titles at multiple companies. Speaking to the issue of whether or not GDPR conflicts with existing global rules, Engel takes a more cynical — although probably correct — view than most.

> "The real conflicts lie in the legal environment and privacy culture."
>
> – Barak Engel, CISO, Amplitude Analytics

"I know there is an entire industry devoted to 'identifying' these supposed conflicts and making money off of 'resolving' them, but I'm not entirely sold on the practice," he says. "The real conflicts lie in the legal environment and privacy culture. And the solution is to be able to switch mindsets and actually understand what each side of the Atlantic is seeking."

That's not to say that Engel sees no global data security/privacy compliance challenges. He cites China's data security rules, which Engel understands to forbid remote access.

It is safe to say that U.S. companies have seen more than their fair share of remote access security issues, especially with franchisees purchasing consumer-level remote access security for businesses. Put simply, making it easier for employees to access your

24%

Percentage of UK companies that stopped preparing for GDPR after Britain triggered Article 50 to leave the EU

– Crown Records Management

sensitive data when they are off-site also makes it easier for thieves to do the same.

But Engel finds the Chinese ban impractical. "If it is truly now impossible to serve Chinese consumers while using remote access, then it becomes incredibly difficult to do basic security maintenance, such as patching, log monitoring, and the like. Not everyone has a budget that allows them to send somebody on a plane to their China [distribution center] every month with a USB key with patches," Engel says. "It makes it impossible to do good security management for any sort of real-time developing event."

> "I wouldn't put it past European legal courts to second guess U.S. law."
>
> – Bret Cohen, attorney and partner, Hogan Lovells US LLP

Mostly, though, Engel finds the attitude differences from GDPR to U.S. rules and laws the critical factor. Consider the Right to be Forgotten again — the favorite component to GDPR that the experts like to site because it provides some of the best examples of differences of approaches.

"The U.S. has a Constitutional right to freedom of speech. That is not the same in the EU," Engel says. "In the EU, you can put in your privacy policy anything you want because it doesn't matter. The right of suppression is supreme to the clauses in your privacy policy."

Barak Engel, CISO, Amplitude Analytics

In the U.S. currently, a company's privacy policy is the supreme rule, so much so that the U.S. Federal Trade Commission sanctions companies when they deviate from their own policy.

Engel also argued that some U.S. lawyers are reading the GDPR phrasing for precise loopholes or fine-print arguments they can make. They'll find, he says, that those arguments are unlikely to persuade any EU officials.

"The European Union is not the U.S. in how they treat these sorts of rules," he says. "That's not how the EU works. That's how the U.S. works," Engel says. "Europeans care about the *spirit*, not the *letter* of the law. (Looking for precise wording to escape is) an American lawyer thinking in American terms."

That's a key reason why seeming conflicts between GDPR and U.S. regulations cannot be ignored. Some attorneys have argued that EU officials will defer to U.S. rules — especially law enforcement rules — in most cases.

But the wording of the GDPR doesn't quite support that. In Article 18, for example, it allows for exceptions this way: "or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State." That Union is the European Union and member states are countries that are part of the European Union. That clause does not force a regulator to cede ground to any foreign rules.

American lawyer Cohen agrees. "Processing of information for a non-EU legal purpose is not a justification for processing under Article 6. (But) that doesn't mean that categorically that you can't do so," Cohen says. "Foreign legal obligation is the most relevant basis for processing, for arguing that it is a legitimate interest. There just isn't an absolute exemption."

Without such an absolute exemption, what does that leave U.S. CISOs?

"We have to rely on European authorities to interpret that balancing test," Cohen

24K

Estimated number of private-sector Data Protection Officer positions that need to be filled

– IAPP

says. European courts "don't necessarily consider certain U.S. legal requirements to be legitimate grounds. I wouldn't put it past European legal courts to second guess U.S. law."

Another problematic area with GDPR that Cohen sees is Article 22, which restricts any automated decision making. Says Article 22: "The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her."

Bret Cohen, attorney and partner, Hogan Lovells US LLP

Remember all of those machine learning plans your CIO wanted? And the automated processing and business analytics using various algorithms? With GDPR, you now need to announce your intention to do so and you must get explicit consent. And before you say "No problem. I'll just throw it into the terms and conditions that no one reads. If they don't click yes, they can't use the service," it's worth noting that that time-honored U.S. trick is unlikely to survive GDPR scrutiny.

"Accepting terms within a long terms of service document bundled together with other disclosures cannot serve as consent within GDPR," Cohen says. "For the most part, we call it consent in the United States" but not so much for EU officials.

Cohen elaborates: "The GDPR states that an individual's consent for a business to collect and use their personal information may not be effective when the provision of a service is conditional on that consent, and the use of the personal information is not necessary for the provision of the service. In the United States, consent for certain types of secondary data uses, such as marketing, is routinely required as a condition of using the service, and bundled with other consents. This approach may not work under the GDPR."

Another attorney specializing in privacy, security and data matters is Philip Gordon, co-chair of the privacy and background checks practice at the San Francisco-based law firm Little Mendelson. Gordon expresses concerns about U.S. companies now having to treat European employees in Europe and in the U.S. — along with U.S. employees temporarily and permanently based in Europe — differently courtesy of GDPR.

"No U.S. law requires notification if an unauthorized person acquires employees' compensation data whereas, under GDPR, a compromise of compensation data could trigger a breach notification obligation. From an employee relations perspective, the multinational employer would have a difficult time justifying notification of the breach only to EU employees," Gordon says.

"GDPR requires EU employers to provide each employee with a data processing notice and to confer on them certain data rights," he continues. "The U.S. parent corporation can easily justify not providing notice or similar rights to U.S. employees not just because it is not legally required to do so, but also because the U.S. employees do not expect to receive a notice or to be able to exercise rights with respect to their data that are not established in U.S. law." ■

For more information about ebooks from SC Media, *please contact Stephen Lawton, special projects editor, at stephen.lawton@haymarketmedia.com.*

If your company is interested in sponsoring an ebook, please contact David Steifman, VP, publisher, at 646-638-6008, or via email at david.steifman@haymarketmedia.com.

2

Data types covered by GDPR: Personal (e.g.: name, phone, birthday) and sensitive (e.g.: Social Security Number, biometric data, race)

– Minereye