Where to Be on GDPR: Keys to Compliance Just Months Before the Deadline

FEATURED EXPERTS

Heather Egan Sussman, Partner and Co-Head of the Privacy and Cybersecurity Practice Group, Ropes & Gray

Deborah Housen-Couriel, Senior Legal and Regulatory Consultant, Konfidas

Hugh Jones, Chief Privacy Officer, Sytorus

Much of the technical aspects of full compliance, or Technical and Operational Measures (TOMs), should be up and running, as the process can easily take more than three months, ***Deborah Housen-Couriel*** *says.*

As the May 25, 2018, deadline approaches for compliance with the European Union's General Data Protection Regulation (GDPR), most companies should already have completed a good amount of the work it will take to meet the regulation's many complex requirements — which govern the tracking of individuals by enterprises, the retention and processing of personal data and the transfer of information across national borders. And yet, while more than half of organizations say that GDPR compliance is their top priority, according to a recent PwC report, several surveys suggest that most have not yet started — or are lagging — in their implementation. Preparing for GDPR can be a daunting proposition, but it's a small price to pay to avoid potential fines of up to €20 million ($23.7 million) or 4 percent of an enterprise's global annual revenue, whichever is greater. With the compliance deadline now less than six months away, RANE spoke to three experts to give companies a better sense of how far along toward full implementation they should be and what steps they should take to close the gaps.

Obligations for Enterprises, Large and Small

Hugh Jones says that many US-based entities are uncertain whether or not they need to be GDPR-compliant — and the answer depends on **whether they have an exclusively non-EU clientele**. If they hold, process or even host the personal data of EU citizens as a core element of their day-to-day activity, they will have some level of obligation to comply. Jones, who is based in Dublin, said that approximately 40 to 50 percent of Irish companies have achieved a measure of readiness, with many organizations expending some level of effort to be fully compliant by May. "It also implies that 50-60 percent are ill prepared or ignoring it," he adds. A growing refrain is "That's like Y2K. It'll never happen," Jones says. He notes that some small organizations are **not expecting robust enforcement**, based on past privacy regulations, but basing an organizational plan on such an assumption isn't recommended.

Part of the challenge is a **lack of official milestones** for organizations to meet, although EU regulators have organized conferences and training events and are now issuing guidance to encourage organizations "to understand GDPR and take it seriously," Jones says. "There's no hard and fast rule, no prescribed sequence, but there are best practices on how to use the remaining six months."

Given the sheer complexity of what needs to be undertaken, companies cannot afford to waste any more time. "You've got to start," **Deborah Housen-Couriel** says. "Earlier is

better, and you have to be able to show to regulators that your organization is seriously engaged with taking care of your GDPR obligations."

"Putting in place processes to implement those rights (like the 'right to be forgotten') will likely take time and could require development of technical solutions." ***Heather Egan Sussman***

Understanding Ownership and Taking Inventory of Data

It's critical that first and foremost, organizations must understand who owns the data they collect, according to **Housen-Couriel**. "It belongs exclusively to the data subjects. The GDPR views this as a fundamental human right." This is the case, regardless of "whether its being transmitted, stored, collected or created." The approach is separate from some other understandings of data privacy, in terms of the required protections: "The EU's concept behind the GDPR is that data protection addresses aspects of the person's identity that need to be protected in very stringent and transparent ways."

Enterprises should have a process underway already to do three things, Housen-Couriel says:

- First, **locate where personal data is** that they have collected or processed.
- Second, they need to start to think about — if not finish the process — of **determining their data trail**: Do they know what happens to the personal data when it reaches them from their website, from an employee form, from a customer form, wherever that endpoint is. Does the company know how to map out the path that personal data makes through the organization, from initial collection to eventual storage of that data?
- Third — and the thing that companies often don't pay attention to — is they should be thinking about **how to minimize data collection**. That involves answering such questions as, "What does that data look like when it flows through my organization, and where is it stored and backed-up? What does my company no longer need and how should we eliminate it?"

"This is going to be such a significant change in the ways companies think," Housen-Couriel says. "Individuals are going to have to be more careful what they agree to. Companies need to be more up front about what data they collect."

Heather Egan Sussman says that with so much at stake, "The most important thing is to have a plan in place." She advises clients to **establish a GDPR compliance team** that will champion the process of (1) documenting existing data flows, (2) implementing relevant policies and procedures, (3) training employees, and (4) managing third-party vendors to meet the requirements under the GDPR. Members of such a team may consist of stakeholders within the organization's business units whose activities impact processing of EU data flows, such as legal, compliance, IT, information security, HR, marketing, finance and procurement departments.

Selecting a Jurisdiction + Naming a Data Privacy Officer

Key considerations for organizations will be **selecting a jurisdiction for compliance and, if needed, naming a data privacy officer, or DPO**, according to **Jones**. In all 31 member states, components of data legislation should be enacted and enforced identically. Enterprises will be bound to comply with the findings of that jurisdiction's court and supervisory authority.

The criteria for selecting a jurisdiction would appear to be moot, since the GDPR is set on the principle that enforcement and interpretation of the Regulation will be identical in each

EU member state. But the primary driver for selection will be the jurisdiction in which the **key data management policies are determined for the organization** – i.e. where is the Board of Directors based, where is the DPO located, where is most personal data acquired, processed and managed? The reason for this selection of a jurisdiction is less about the convenience for the organization, and more about a) the obligation to be transparent regarding decision-making within the organization, and b) spreading the enforcement burden evenly across the 31 Supervisory Authorities which make up the 'policing structure' for the GDPR across the region.

__Hugh Jones__ says that many US-based entities are uncertain whether or not they need to be GDPR-compliant. But if they hold, process or even host the personal data of EU citizens as a core element of their day-to-day activity, they will have some level of obligation to comply.

One caveat is that US-based companies might be tempted to select the United Kingdom as its home jurisdiction, but with Brexit looming, "it's not clear that will be adequate jurisdiction, or will provide an adequate level of data protection compliance or enforcement," Jones says. Still, for the moment, with the Brexit negotiations trundling on, the UK remains a full member of the EU, and an acceptable jurisdiction in which to be based.

The GDPR contains two provisions to **prevent jurisdiction shopping**, Jones says.

- One is that **any EU member may appeal what it considers a lenient court ruling or lax enforcement** by another EU jurisdiction, which would be heard by the European Court of Justice (ECJ). "The relief of an apparently lenient decision, and then to have it taken out from under them, presents a double-whammy for companies — the perception that you tried to avoid the responsibility in the first place by opting for an apparently lenient or "soft" jurisdiction, and on top of that a punitive measure, a slap on the back of the head, for trying to dodge your responsibility."

- Jurisdictions must also bear relation to **where an organization physically processes its data and makes data-related policy decisions**, Jones adds. That means it's in an organization's interest to consider their criteria for selecting a location "not necessarily based on how aggressive the enforcement capability is going to be, but where the substantial processing of data is going to be."

Jones adds that at a benign level, the GDPR encourages organizations toward better quality data, better communications with customers, more accurate understanding of customer preferences, lower reputational and operational risk, reduced costs through reduced data storage overheads, improved balance sheet through considered selection and close monitoring of service providers, and ultimately, improved marketing "hit rates" through better quality data and improved business intelligence. "Even without the impending GDPR, all of these benefits are desirable, so it makes sense to implement these solutions," he says. "At its most benign, the GDPR just acts as a motivation and a catalyst."

Housen-Couriel says that organizations must also determine **where their DPOs reside in their internal hierarchies** — whether the position is part of the legal department, the IT department, or at the board level. She adds that legal departments will "really need to be up on aspects of data protections that are fundamental rights, and they have to be aware that they're dealing with a new level of compliance."

Ironing Out Technical and Operational Measures

Companies should also consider and prioritize areas that may take more time, **Egan Sussman** notes. For example, GDPR grants rights to data subjects, such as the **right to erasure (otherwise known as the "right to be forgotten")** and **the right to object to the processing of personal data in certain circumstances**. "Putting in place processes to implement those rights will likely take time and could require development of

technical solutions," she says. **Similarly, new requirements for contracts may require potentially drawn-out negotiations with the company's vendors.**

Additionally, much of the **technical aspects of full compliance, or Technical and Operational Measures (TOMs), should be up and running**, as the process can easily take more than three months, **Housen-Couriel** says.

- "Tech people will tell you they will need time for dry runs and corrections, trials and last-minute fixes, et cetera," she says. "It's really a hard challenge because in a very, very short time-frame organizations will need to understand: 'What do my processes look like?'" she adds.

- Bottom line, it's critical "for an organization to be able to show they have a plan for compliance to GDPR, that they have people in charge, that there's a point person who has spoken to the regulators in charge."

*"You've got to start," **Deborah Housen-Couriel** says. "Earlier is better, and you have to be able to show to regulators that your organization is seriously engaged with taking care of your GDPR obligations."*

RELATED READING

- Getting Ready for GDPR, *RANE*
- The GDPR Deadline Is Fast Approaching; How Enterprises Are Preparing, *Network World*
- Pulse Survey: US Companies Ramping Up General Data Protection Regulation (GDPR) Budgets, *PwC*
- Survey: 61 Percent of Companies Have Not Started GDPR Implementation, *IAPP*
- Data Breaches Will Soon Cost Companies in Europe, *The Wall Street Journal*
- The General Data Protection Regulation: A Primer for US-Based Organizations That Handle EU Personal Data, *Program on Corporate Compliance and Enforcement, New York University*

ABOUT THE EXPERTS

Heather Egan Sussman, Partner and Co-Head of the Privacy and Cybersecurity Practice Group, Ropes & Gray

Heather Egan Sussman leads the Privacy & Cybersecurity Practice Group at Ropes & Gray. Her practice focuses on privacy, cybersecurity and information management. Heather routinely guides clients through the existing patchwork of privacy and security laws around the globe, including the EU's General Data Protection Regulation, US federal and state laws, as well as self-regulatory frameworks, including those covering online advertising and the payment card industry. She manages teams of local counsel around the world to deliver seamless advice for clients that operate across many jurisdictional lines, developing comprehensive privacy and cybersecurity programs that address competing regulatory regimes

Deborah Housen-Couriel, Senior Legal and Regulatory Consultant, Konfidas

Deborah Housen-Couriel is an expert in global, regional, and Israeli cybersecurity law and regulation, as well as international telecom law. She specializes in the areas of cyber and data protection law, comparative regulatory strategies, cybersecurity professional accreditation, and countering cyber-enabled terrorism.

Hugh Jones, Chief Privacy Officer, Sytorus

Hugh Jones is a certified Data Management consultant who is closely involved with the development and introduction of compliant Data Management policies and practices within a wide range of clients in Ireland and overseas. Jones delivers training, provides professional advisory services and is a frequent speaker at local and international Data Management events. Through his experience as a business and IT Project Manager, Jones supports organizations striving to achieve and maintain a level of familiarity with the EU Data Protection legislation, as well as helping them to design their "adoption journey" toward full compliance.

ABOUT RANE

RANE (Risk Assistance Network + Exchange) is an information and advisory services company that connects business leaders to critical risk insights and expertise, enabling risk and security professionals to more efficiently address their most pressing challenges and drive better risk management outcomes. RANE clients receive access to a global network of credentialed risk experts, curated network intelligence, risk news monitoring, in-house analysts and subject matter experts, and collaborative knowledge-sharing events.