3M | The experts in screen privacy.

GDPR Readiness FAQ

Enza Iannopollo, Forrester Research

Enza is an analyst on the Security & Risk team and a Certified Information Privacy Professional (CIPP/E). At Forrester, she covers data protection, privacy, analytics and the internet of things, with a focus on the impact of regulations and the technologies that underpin them.

GDPR is one of the most important changes in data privacy regulation in 20 years. It establishes how organisations must handle the personal data of their customers, employees, and business partners on an ongoing basis. 3M recently sat with Enza Iannopollo of Forrester Research to discuss the security measures, policies and privacy-compliance programs that many organisations are establishing to comply with regulations like GDPR. Enza provided insight into workplace readiness and emphasised the need for physical safeguards to protect against data privacy threats.

What's at stake?

Organisations can be fined up to 4% of annual global turnover or €20 M FINE

Here's what she had to say:

Q. Are workforces ready to comply with GDPR?

A. Our numbers show that only one in three companies worldwide is ready to comply with the General Data Protection Regulation (GDPR). Since GDPR enforcement begins May 25, 2018, it is clear that many organisations need to move quickly to finish their preparations.

Specifically, we are seeing firms struggle to meet the requirement to implement and document privacy training and awareness programs for employees. EU regulators have indicated that these programs are essential for GDPR compliance. Meanwhile, we have found that organisations meeting this requirement have improved their corporate privacy culture and established best practices that sometimes go beyond regulatory requirements.

Q. Are companies in specific regions more prepared than others?

A. 34 percent of U.S. firms say they are ready compared to 26 percent of firms in Europe.[1] Companies that are not GDPR compliant—whether they realise it or not—are taking a big business risk on their shoulders. Companies who think they are ready, but are not, are taking an even greater risk.

It's interesting to note that more companies in the U.S. believe that they are ready as compared to Europe. This has to do with the extra-territorial effect of GDPR. The regulation applies to all companies—regardless of their location—that process or hold the personal data of European Union residents. This means that not only European companies but also many U.S.-headquartered companies will be required

to comply with these stringent privacy rules.

We suspect that a superficial reading of the rules, combined with misleading and unfounded expectations of weak GDPR enforcement, may be challenging companies' perception about their readiness.

Q. What physical security and privacy safeguards are required by GDPR?

A. GDPR is a principle-based regulation. This means regulators don't provide organisations with a set of definitive actions to follow. Instead, organisations should think about GDPR requirements as a sort of "desired state" for their data-handling practices. It also means that organisations must identify and assess specific risks they need to mitigate to comply with GDPR requirements.

When identifying risks, firms must consider those that are presented by data processing, in particular, due to accidental or unlawful loss, unauthorised disclosure of, or access to personal data that is transmitted, stored or otherwise processed. It doesn't matter whether an unauthorised data disclosure happens because a hacker launches a sophisticated cyberattack on a company's website or because a stranger takes a picture of highly sensitive data displayed on an employee's laptop screen. Both are equally serious risks and need appropriate mitigation strategies.

Q. Is visual hacking a risk?

A. Absolutely. Just remember: The keys to the kingdom for many organisations come in the form of a username and a password. It takes only a quick look at an unprotected screen for an unauthorised individual to get those keys and gain access. And the risk grows with the increasing sophistication of social engineering.

A year ago, a journalist was hacked while working on a plane.[2] The hacker was able to describe details about an article the journalist was writing, personal emails he had sent, and upcoming work meetings—all information he said he captured from hacking the in-flight Wi-Fi. Or perhaps, the hacker simply gleaned it by looking at the journalist's laptop screen. The journalist was outraged, but he understood the message: while he was working on a sensitive article, in this case dissecting the profound and far-reaching privacy implications of Apple refusing the FBI's request to decrypt the phone of a terrorist, he forgot to protect the privacy and intellectual property of his own device. Like that journalist, many organisations make the same mistake of underestimating the risk of cyber and visual hacking.

Q. What are the benefits of implementing low-tech physical safeguards?

A. With nonstop news stories about large-scale data breaches, it's easy to forget that today's digital businesses still have to contend with physical security challenges. There are multiple benefits in implementing physical safeguards, such as video cameras for surveillance, locks for laptop cases and privacy filters for monitors, laptops, tablets and smartphones. Privacy filters, for instance, provide a sound mitigation strategy for privacy violation and data breaches. All it takes is some sensitive customer or employee data being exposed to the wrong set of eyes to result in a potentially highly detrimental—and highly publicised—data breach.

They can also support compliance for regulations other than GDPR. For example, a medical assistant was fired from a hospital at the University of Iowa a few years ago for breaching patient data privacy rules. She was accused of visually hacking a co-worker while he was examining a patient's medical record which is a HIPAA violation.[3]

Physical safeguards, such as privacy filters, can serve as a visual reminder to employees that security and privacy best practices are priorities for the organisation. And as always with visual privacy, it's not just about meeting compliance requirements. It's about protecting a firm's most valuable assets.

Q. How can companies leverage privacy to drive superior customer experience?

A. Firms that are executing robust GDPR and privacy programs are experiencing a number of business benefits beyond compliance. Delivering a superior customer experience is one of them. The way your organisation protects your customers' data can have a direct impact in building—or destroying—the underlying feeling of trust that your customers have with you.

We know, for example, that customers do switch to competitors as a result of a privacy breach.[4] Furthermore our research of consumer privacy attitudes highlights that 30 percent of individuals refuse to complete an online transaction if they read something that they don't like in the company's privacy notice.[5]

If you are committed to protecting your customers' data and your employees recognise and reflect this commitment in their customer interactions, it can set you apart from the competition.

Q. Are there any companies who stand out for their commitment to privacy and security?

23% of the Fortune 100
have embraced privacy as part of their corporate social responsibility (CSR) efforts.

A. Privacy has shifted from being a niche topic for legal departments to a core value for many organisations. Today, CIOs and CMOs are among the executives who believe that protecting data assets from attacks and misuse is among their top priorities. Our research found that 23 percent of the Fortune 100 have embraced privacy as part of their corporate social responsibility (CSR) efforts.[6] About 70 percent included security in their CSR reports.

We also noticed that firms committed to privacy and security benefit by being open and transparent about how they handle personal data. This can be an extremely valuable way to provide assurance to customers, employees and business partners alike. But operating in accordance with this commitment is not simple. Often, organisations must change the way they operate to bring these commitments to life and establish a corporate culture that recognises privacy and security as core values.

Q. Are more regulations like GDPR in the works?

A. There is no doubt: GDPR signals a trend. We recently completed a new piece of research that analyses the privacy regulations and practices of 54 countries.[7] It's clear that regions such as Asia-Pacific are looking at GDPR as the possible evolution of local privacy rules. Elements of GDPR, such as data residency, are also being embedded in data privacy rules in Latin America and Russia. Finally, the European Parliament is now working to update the requirements of the current ePrivacy Directive. Details still need to be hammered out, but the plan is to align eprivacy requirements to GDPR.

[1]Forrester Business Technographics Security Survey, 2017
[2]Digital Trends, "Apple vs FBI shown in different light as journalist hacked mid-flight," Jan. 25, 2016
[3]Veriphyr, "Medical Assistant Fired for "Shoulder Surfing" and Breaching Patient Data Privacy," 2011
[4]Ponemon Institute, "The Impact of Data Breaches on Reputation and Share Value," May 2017
[5]Forrester Research Consumer Technographics European Online Benchmark Survey (Part 2), 2016
[6]Forrester Report "The Future of Data Security and Privacy: Growth And Competitive Differentiation," 2017
[7]Forrester "Interactive Data Privacy Heat Map," 2017

FORRESTER®