One year from GDPR: What You Need to Know

SOPHOS
Security made simple.

May 25, 2018 is a date that should be etched in red on the calendars of any company that does business in the European Union (EU).

That's the day companies must be in full compliance with the EU's General Data Protection Regulation (GDPR), which requires them to take specific steps to more securely collect, store, and use personal information.

For companies just beginning their efforts to comply, there's not much time left. This paper is designed to help those organizations get on track.

Companies ignore GDPR at their peril

First, a dose of reality: Companies not in compliance at this time next year face brutal fines for violations.

For example, NCC Group came up with a model that extrapolated from the fines actually imposed for breaches by the Information Commissioner's Office and calculated what they might be under GDPR.

Under this model, British companies that were penalized for breaches last year could have faced fines totaling £69 million under GDPR, rather than the £880,500 they collectively had to pay up. TalkTalk, which last year was slapped with the biggest fine ever in the UK for a data breach – of £400,000 – would have faced a bill of £59m, calculated NCC, while Pharmacy2U, which was fined £130,000, would have faced a bill of £4.4m.

Those are sobering numbers, especially in light of a January report from (ISC)2's EMEA council, which covers issues concerning Europe, the Middle East and Africa. According to the report, organizations aren't doing too well, having accomplished precious little in the first year they had to get things in order. The council warned of what it sees as poor acceptance of accountability across organizations and an apparent belief that the task ahead is one for the specialists – either legal or technical.

Meanwhile, a recent report by Crown Records Management found that nearly a quarter of UK businesses surveyed said they had stopped preparing for GDPR, with 44% saying they didn't think GDPR would apply to them once the UK leaves the EU in March 2019 as a result of last year's Brexit vote.

Since those companies will still be doing business in the EU, that's an unfortunate and potentially costly assumption.

Size matters not

Another point of confusion for companies is about size. Specifically, do small businesses face the same requirements under GDPR as the big enterprises?

Let's address the question:

GDPR requires that any company doing business in the EU – no matter the size – more securely collect, store and use personal information. Like the big guys, smaller companies face fines for violations that may occur.

But the regulation accounts for the fact that smaller businesses lack the same resources as larger enterprises. UK-based data protection consultancy DataHelp makes note of the differences on its website:

Under the current law, as contained in the Data Protection Act, (DPA), the same rules apply, regardless of the size of an organization. However, the General Data Protection Regulation (GDPR), which will replace the DPA and which is expected to come into force sometime in 2018, recognizes that SMEs require different treatment from both large and public enterprises.

One area of concern for small businesses is the GDPR requirement that companies hire a data protection officer. But that part is for firms with more than 250 employees. Though smaller firms may still need to employ someone in this role if handling personal data is core to their operations, it may not have to be a full-time employee, but rather a consultant, which could be less costly.

Daunting as it all may seem, small businesses can take comfort in this: as long as they can demonstrate that they've put their best foot forward to meet the requirements of GDPR, regulators will work with them on any problems that might arise.

The key is to bring in the right consultants and document all actions taken.

Now what?

Now that we've outlined what's at stake, let's look at some concrete steps companies must take to be taking to be ready for May 2018.

In a recent article on Sophos' Naked Security site, we reviewed a 12-point checklist published by Ireland's Office of the Data Protection Commissioner. The compliance practitioners we talked to have repeatedly cited that list as particularly helpful.

The checklist is as follows:

1. Be aware. It's not enough for CEOs, IT staff, and compliance officers to be aware of what GDPR requires. Employees from the top to the bottom of an organization need to be extensively educated on the regulation's importance and the role they have to play.
2. Be accountable. Companies must make an inventory of all personal data they hold and ask the following questions: Why are you holding it? How did you obtain it? Why was it originally gathered? How long will you retain it? How secure is it, both in terms of encryption and accessibility? Do you ever share it with third parties and on what basis might you do so?
3. Communicate with staff and service users. This is an extension of being aware. Review all current data privacy notices alerting individuals to the collection of their data. Identify gaps between the level of data collection and processing the organization does and how aware customers, staff and service users are.
4. Protect privacy rights. Review procedures to ensure they cover all the rights individuals have, including how one would delete personal data or provide data electronically.
5. Review how access rights could change. Review and update procedures and plan how requests within new timescales will be handled.
6. Understand the legal fine print. Companies should look at the various types of data processing they carry out, identify their legal basis for carrying it out and document it.
7. Ensure customer consent is ironclad. Companies that use customer consent when recording personal data should review how the consent is sought, obtained, and recorded.
8. Process children's data carefully. Organizations processing data from minors must ensure clear systems are in place to verify individual ages and gather consent from guardians.
9. Have a plan to report breaches. Companies must ensure the right procedures are in place to detect, report, and investigate a personal data breach. Always assume a breach will happen at some point.
10. Understand Data Protection Impact Assessments (DPIA) and Data Protection by Design and Default. A DPIA is the process of systematically considering the potential impact that a project or initiative might have on the privacy of individuals. It will allow organizations to identify potential privacy issues before they arise, and come up with a way to mitigate them.
11. Hire data protection officers. The important thing is to make sure that someone in the organization or an external data protection advisor takes responsibility for data protection compliance and understands the responsibility from the inside out.
12. Get educated on the internal organizations managing GDPR. The regulation includes a "one-stop-shop" provision to assist organizations operating in EU member states. Multinational organizations will be entitled to deal with one data protection authority, or Lead Supervisory Authority (LSA) as their single regulating body in the country where they are mainly established.

Making it your own

Those approached for the Naked Security piece cited in the main article noted how they've taken the guidelines of Ireland's Office of the Data Protection Commissioner and put their own organizations' stamps on it. Craig Clark, information security and compliance manager for IT services at the University of East London, is one of the experts Naked Security spoke with.

From a project point of view, Clark suggested the following be completed or nearly completed by mid 2017:

- C-Suite awareness
- User awareness
- DPO appointment
- Information identification
- Updated privacy notices
- Updated data protection policies
- Updated information sharing agreements
- Approved Data Privacy Impact Assessments
- Identification of any cross-border transfers
- Establishment of Data Subject Rights Management protocols
- Privacy by Design implemented into the project methodology

"A lot of guidance is still to be written by the ICO [UK Information Commissioner's Office] but I'd want at least the above to be implemented," Clark said.

Brexit doesn't exempt UK companies

As mentioned in the main article, some assume they are free of GDPR because the UK is leaving the EU. That is not true. The following facts apply:

1. British Prime Minister Theresa May sent a letter to the president of the European Union officially triggering Brexit in late March 2017. The exit process will take at least two years to complete, meaning those UK companies will still be a part of the EU on the day GDPR takes effect.
2. Once the UK is no longer part of the EU, many of those companies will still do business with companies that are in the EU. That alone will keep UK businesses on the hook for compliance.

Therefore, companies should approach GDPR as they were before Brexit happened.

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

Oxford, UK

2017-05-17 RC-NA (MP)

SOPHOS