What to do to make sure you're ready for GDPR

Neil Hodge (http://www.complianceweek.com/authors/neil-hodge) | May 16, 2018

Don't look now, but a very important data privacy deadline is just around the corner.

Following two years of warning, new rules come into force on 25 May that protect the privacy rights of EU citizens worldwide. Organisations based anywhere in the world that hold, process or interact with personal data on any EU citizen are bound by the rules, even if they have no physical presence in any of the 28 EU member states.

The EU General Data Protection Regulation (GDPR) (https://www.eugdpr.org/) was adopted throughout the European Union (EU) in April 2016 and it creates some significant changes. Chief among them, it extends the definition of "personal data" so widely that it now includes genetic and biometric data, as well as online identifiers, such as an IP address. It also strengthens and increases the rights of data subjects, tightens the rules on consent, and introduces the "right to be forgotten" so that EU citizens can ask for websites to delete their details.

Europe's previous data regime applied only to "data controllers", meaning those who collected and ultimately owned the data, such as companies retaining customers' personal information, such as addresses and credit card details. However, the GDPR now holds data processors—essentially, third-party vendors that may be privy to the same information—jointly liable for protecting that information, too. In practical terms, this means that companies need to have assurances that their suppliers and contractors also have measures in place to comply with the GDPR.

The regulation also includes detailed compliance requirements, such as appointing designated data protection officers if there is regular or systematic monitoring of data subjects or large-scale processing of special categories of data. The most difficult requirement is perhaps the need to report any breach to the relevant data protection supervisory authority within 72 hours. In certain circumstances, organisations would also need to notify those individuals affected in the same timeframe as well.

No doubt, preparing for the GDPR may be a compliance headache for some companies, and even those that have been trying to embed the necessary processes and controls to comply with the new rules may find that their efforts are not as fault-free as they hope.

Data protection experts are emphatic about what an organisation's first reaction should be if it believes that it is not fully GDPR compliant as the deadline approaches: Don't panic. They point out that regulators are not proactively looking for signs of data breaches or non-compliance, and suggest that—unless a company is already known to them for having lax data protection controls—organisations should not expect any kind of regulatory inspection or demand for information on spec.

As a result, says Justin Coker, vice president EMEA at IT security software vendor Skybox Security, organisations shouldn't try to "compliance cram" to meet an unrealistic deadline if they have left their preparations too late. "The risk associated with this behaviour is that organisations will end up with processes that aren't efficient, scalable, strategic, or worse—compliant," he says.

The first step organisations should do to check they are compliant with the regulation is to "re-read it, or at least a summary, and complete a quick checklist," says Dr. Guy Bunker, SVP of products at data security company Clearswift. "To be honest, you will probably find a few deficiencies in what you have today," he says, and "complacency, or neglecting to think that the rules apply to particular aspects of business, will be one of the biggest dangers for organisations in the future," he adds.

Alice O'Donovan, a lawyer at McGuireWoods, advises compliance professionals to "take a step back" and check that the organisation fully understands all the data it holds. "It may sound basic, but ensure you have documented all the personal data you hold, where it came from, why you process it, and who you share it with. This is probably the most important step toward GDPR compliance," she says.

It is also important that the organisation has a plan for working toward full compliance with the GDPR. In terms of covering the basics, says O' Donovan, organisations should ensure they have a clear, concise privacy notice in place, which is separate from other terms and conditions, and is easily accessible.

Among other issues, it must clearly describe what data is processed, how it is processed, why it is processed, and should inform data subjects of their rights regarding the data the company is processing about them. She adds that organisations should check that all data processing agreements (effectively, any agreement under which another organisation processes personal data on behalf of your organisation) are GDPR compliant too.

Running a GDPR compliance gap analysis to find last-minute weak spots is also a must, says O'Donovan. This has two stages. "First, assess where the greatest areas of risk lie for your organisation. For example, do you transfer personal data outside of the European Economic Area EEA)? Do you process 'special categories' of personal data, or personal data relating to children? Do you engage in surveillance activities? Second, assess where you do—and don't—comply with the GDPR, and cross-reference it with your list of risks. If you aren't compliant in any area that poses a particularly high risk, work toward mitigating that risk as a matter of priority."

The importance of staff training shouldn't be overlooked. "It is not sufficient just to put a new data protection policy on your staff intranet and forget about it—you need to foster a culture of transparency and accountability toward personal data throughout your entire organisation," says O'Donovan. "Training on data protection and security, the requirements of the regulation, and the rights of data subjects should be offered to all employees. Humans are your greatest asset—but they're also your greatest potential weakness."

Experts say there are several areas where organisations can slip up and fall foul of the regulation. Transferring personal data across borders poses significant compliance risks: What constitutes a "data transfer" is not always obvious, and the transfer does not have to be deliberate. For example, if a company has European and U.S. offices, a data transfer will take place if a staff member in the United States even so much as views an EU contact's personal data on their computer.

Failure to comply with a data subject access request will also be an area where organisations that are unprepared will find compliance difficult. Data controllers will now have only 30 days to comply with subject access requests (SARs), unless they are particularly onerous or complex, and failure to process them within that timeframe leaves organisations subject to the higher range of fines under the GDPR. As a result, experts say that organisations should have a subject access policy in place and ensure everyone in the business knows what to do if they receive a SAR.

There are other potential pitfalls that organisations could easily overlook. Gary Brooks, head practitioner at data advisory consultancy The Data Support Agency, says that some of the key areas where companies will fall foul of the regulations include the continued use of pre-ticked boxes to assume consent. "These practices are no longer allowed. Consent has to be on the basis of a clear affirmative action. Furthermore, if the organisation is handling any data of children under the age of 13, then parental consent and validation is needed."

In short, says Brooks, "if you don't have an identified legal basis for having the information, you shouldn't have it. Some data will need to be "refreshed" by obtaining consent, trimmed or deleted, and as a result of the changes, marketers, in particular, should review contact databases, he says.

O'Donovan says that organisations may stumble over their failure to be transparent. "One of the key data protection principles under the GDPR is transparency, which essentially means that you can use personal data only for the purpose or purposes you have told data subjects you will use it for, and no other incompatible purposes. Breaching this fundamental principle is subject to the higher band of fines under the GDPR," she says.

"Many organisations are at risk of forgetting that there is a very important distinction between the lawful basis for processing under the GDPR (such as consent, legitimate interests, and so on), and the purpose of the processing. If you haven't told a data subject about the purpose of the processing, then using their data for that purpose is unlawful—irrespective of whether or not it's in your legitimate interests to do so," she says.

Being able to access documents quickly is also going to be a key part of GDPR compliance—and non-compliance, say experts. "At the end of the day, you need to be able to provide evidence of your compliance with the GDPR," says Rashmi Knowles, CTO (EMEA) at IT vendor RSA Security, who believes that it is vital that organisations are able to document and prove their attempts to comply with the regulation. "So, the final check should be to make sure the documentation covering your processes and technologies is clear, regularly updated and available at short notice should the regulator come knocking."

"GDPR compliance is as much about how people use data and the processes in place to control that use as it is the technology required to monitor and report that usage," says Akber Datoo, managing partner at regulatory technology provider D2 Legal Technology. "GDPR compliance requires a holistic people, process and systems perspective."

12 steps to take now to prep for GDPR

The ICO has provided companies with a data protection "self-assessment" toolkit on its Website, as well as 12 step that organisations need to review now to be compliant with GDPR. They are:

1. **Awareness** - Decision makers and key people in you organisation need to appreciate the impact that changing to the GDPR is likely to have.
2. **Information you hold** - You should document what personal data you hold, where it came from, and who you share it with. You may need to organise an information audit.
3. **Communicating privacy information** - You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.
4. **Individuals' rights** - You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.
5. **Subject access requests** - You should update your procedures and plan how you will handle requests within the new timescales and provide any additional information.
6. **Lawful basis for processing personal data** - You should identify the lawful basis for your processing activity in the GDPR, document it, and update your privacy notice to explain it.
7. **Consent** - You should review how you seek, record, and manage consent and whether you need to make any changes. Refresh existing consents now if they don't meet the GDPR standard.
8. **Children** - You should start thinking now about whether you need to put systems in place to verify individuals' ages and to obtain parental or guardian consent for any data processing activity.
9. **Data breaches** - You should make sure you have the right procedures in place to detect, report, and investigate a personal data breach.
10. **Data protection by design and data impact assessments** - You should familiarise yourself now with the ICO's code of practice on Privacy Impact Assessments (https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf) as well as the latest guidance from the Article 29 Working Party

Having appropriate IT systems in place to find requested customer data quickly will be a key determinant in how well prepared organisations are to meet the compliance challenge, say data specialists. Christian Polman, chief strategy officer at market analytics firm Ebiquity, says that "if by now there hasn't been a review of your data practices and policies, it's critical to move fast to understand exactly what data you hold on file and where it might be shared, and to understand the role third parties play in your consumer data ecosystem and associated contractual risks."

"Ultimately, businesses need to work toward having a comprehensive GDPR governance policy to know exactly which parties and departments are responsible for data," adds Polman.

Even if some companies are still not fully aware of what their legal duties are under the regulation, they are likely to be aware of the tough sanctions that regulators have the power to mete out for non-compliance: for example, serious breaches of personal data can incur fines of up to €20m (U.S. $24.5 million) or up to 4 percent of global annual revenues—whichever is greater. Other enforcement options include the power to issue warnings and reprimands, order compliance, and impose restrictions or bans on processing data.

Many companies and data experts have mistakenly said that regulatory enforcement will not be active from 25 May, and that organisations will be dealt with leniently if they can demonstrate that they are "on a compliance journey". However, EU data regulators are keen to set the record straight: The United Kingdom's data protection authority, the Information Commissioner's Office (ICO), has said that "there will be no 'grace' period" and that it will be regulating the new rules from the date they come into force, pointing out that "there has been two years to prepare."

However, in a conciliatory move, the ICO likes to emphasise that it is a "fair and proportionate regulator" and that those organisations that self-report, engage with the regulator to resolve issues, and that can demonstrate effective accountability arrangements can expect these circumstances "to be taken into account" when it considers any regulatory action.

(Article%2029%20Working%20Party), and work out how and when to implement them in your organisation.

11. **Data protection officers** - You should designate someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements. You should consider whether you are required to formally designate a Data Protection Officer.
12. **International** - If your organisation operates in more than one EU member state, you should determine your lead data protection supervisory authority.

Source: Information Commissioner's Office (https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf)