Top 6 misconceptions about GDPR

We've been helping thousands of businesses with their GDPR preparation, which means we've been asked pretty much every question there is to be asked on the topic. So, we thought we'd summarise the most common questions we get asked, and provide some practical answers for anyone who is currently on the path to GDPR compliance.

1 I only have to worry about GDPR if I get breached, right?

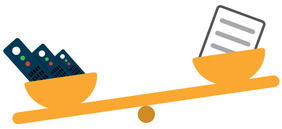
Not true. Privacy and GDPR related questions are now common in a B2B environment, and poor responses will be a commercial inhibitor. Furthermore, citizens have new rights that they will try to exercise; poor preparedness to deliver against those rights will incur considerable overheads. Finally, let's not forget that European authorities also have the right to audit organisations at their discretion, not only before or after an attack.

2 Where does GDPR give me the list of security things that I need to do?

It doesn't. If you're hoping for a list of dos and do nots, unfortunately you're out of luck. GDPR defines outcomes, not the means of delivering them. It also demands careful consideration and shouldn't be approached with a tick-box mentality. Additionally, Security is a strong component within GDPR, but it definitely isn't the only one. Equally important is to ensure that the information that you're trying to protect has been acquired legitimately and is being used appropriately.

3 What products do I buy to be GDPR compliant?

Wrong question! Worse than that: a dangerous question. GDPR imposes a positive approach to privacy on the organisation and security needs to be considered wherever personal information is present. Buying an "edge" product isn't going to make you compliant, but building out the right balance of process, education and technology will.

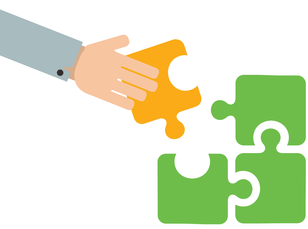


4 It is a EU thing, so not being a member of the EU gets us out of it, surely?

Even if your country is not a member of the European Union, your organisation still needs to comply with the law if it handles EU citizen data (which it most likely does). This is a slightly evolving landscape right now, but the minimum that should be anticipated in local law is parity to GDPR, with some countries pursuing even stricter standards. GDPR encourages a more mature approach to data privacy and one that is woven in to the fabric of an organisation. This is a very good thing!

5 Tell me about those fines again?

Potentially big; 4% of global turnover in the worst instance, per significant infringement. There will be some proportionality shown; the size of the infringement, effectiveness of reporting, the scale of the effort made to be compliant, the type of information lost, the type of organisation being fined. However, all indications are that each respective organisation being fined is likely to find the experience painful, by their own relative terms.



6 Didn't the EU already have laws on this front? Surely I'm compliant already?

Across EU member states the laws were inconsistent, openly flouted, somewhat weak and with insignificant consequences for failure. GDPR raises the bar, standardises across member states and has a much more robust fining system to better encourage compliance. It's an improved landscape and organisations simply must make it a very serious priority.

It's not too late!

Head to our website for more GDPR support — More help

Ready to look at GDPR in more detail? — Watch video