ZoneFox

GDPR – 5 Key FAQs

The answers to your top 5 questions around GDPR

Analyze. Detect. Protect.

Introduction

As far as laws go, for the information management and security community, the General Data Protection Regulation (GDPR) falls firmly into the "game changer" category. When it comes into force on 25 May 2018, it will effectively replace all data protection legislation across the EU - including the UK's Data Protection Act (DPA).

Ushering in bolstered rights for individuals, a raft of new reporting and other obligations on the part of businesses - not to mention a rather daunting new fine tariff; this is precisely the type of once-in-a-generation overhaul that can cause sleepless nights for even the most seasoned CISO.

Here at Zonefox, our very own insider threat protection offering has been hardwired with facilitating better compliance for its users. GDPR readiness has been on our radar right from the get-go - and we've even put together a range of materials to help you make sense of it all. As part of that support, we've put together our Top list of common questions we're asked, and answers to help make the transition over to GDPR as painless as possible …

1. How does GDPR differ from Directive 95-46-EC (The Data Protection Act)

Certain areas of the law have been strengthened, while some brand new concepts have been introduced. Big changes include the following:

+ **Enhanced rights for individuals.** These include the right to be forgotten (i.e. data erasure) and the right to have data transferred to another data controller (data portability).

+ **Data protection by design and accountability.** When launching new products and services or introducing new technologies, organisations must be able to demonstrate compliance. This may include carrying out a data protection impact assessment.

+ **Transparency.** Organisations are under a duty to provide extensive information to individuals about how their data is processed.

+ **Breach notification.** Certain areas of the law have been strengthened, while some brand new concepts have been introduced. Big changes include the following:

+ **A new requirement to notify supervisory regulators** (the Information Commissioner's Office (ICO) in the UK) where a personal data breach has occurred.

+ **A new fine regime.** GDPR introduces much higher fines than the upper limits currently in place under The Data Protection Act.

2. Do I have to "worry" more about GDPR than the old DPA?

Under The DPA, the ICO currently has authority to issue monetary penalty notices of up to £500,000 for serious breaches. By contrast, for a serious breach of GDPR, data controllers will be liable for a fine of up to 4% of global annual turnover or up to 20m.

For other breaches such as failing to keep proper breach log records or failing to report, the fine can be up to 2% of global annual turnover or 10m.

So from a purely financial perspective, the potential consequences of GDPR non-compliance are significantly greater than under the old regime. What's more, information about sanctions imposed will be in the public domain - so possible reputational risks to the business also need to be considered.

Say, for instance, it becomes a matter of public record that you were unwilling or unable to report a serious breach to the ICO in a timely manner - or that you weren't equipped to rectify a breach swiftly. Faced with this, it's going to be tough to convince security-conscious customers that you are a 'safe pair of hands'.

3. So do I now have to report all data breaches?

Unless a breach is unlikely to result in a risk to the rights and freedoms of the individual, the need for notification to the ICO is triggered by any incident which leads to "accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to" personal data. In most situations, there is also a requirement to notify the data subject of the breach.

So let's take the example of a rogue insider who steals data from your organisation. If his haul includes customer account information - or internal personnel records, this almost certainly would be a reportable incident. If the theft is confined to files relating to your upcoming new product range, despite being a catastrophic loss to the business, this wouldn't fall under the requirement.

4. Will a data breach always lead to a fine under GDPR?

Unless a breach is unlikely to result in a risk to the rights and freedoms of the individual, the need for notification to the ICO is triggered by any incident which leads to "accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to" personal data. In most situations, there is also a requirement to notify the data subject of the breach.

So let's take the example of a rogue insider who steals data from your organisation. If his haul includes customer account information - or internal personnel records, this almost certainly would be a reportable incident. If the theft is confined to files relating to your upcoming new product range, despite being a catastrophic loss to the business, this wouldn't fall under the requirement.

In essence, the ICO will need answers to a number of questions:

- Were you able to report the incident within 72 hours of you becoming aware of it?
- Can you explain what happened, who was affected, the consequences and the measures you took to rectify it?
- Do you have a clear incident response plan - and did you follow it?
- Do you have an incident log?
- For the data processing operation in question, did you carry out a privacy impact assessment?
- If necessary, did you consult with the ICO for further guidance?

Similar to under the DPA, you are under a duty to implement "appropriate technical and organisational measures" to keep data secure. There's an ongoing duty to take into account the "state of the art" to ensure your framework is up to scratch; something that becomes especially relevant when upgrading your security infrastructure.

WIth this in mind, Zonefox is designed to support your compliance strategy. On the one hand, it provides an intelligent early warning system by rapidly detecting behaviour indicative of data compromise. On the other, it gives you the type of full forensic record you need to satisfy the regulators. Who was behind the breach? When did it happen? What was taken? Where did it go? Zonefox gives you visibility on all of this.

5. Does Brexit change anything?

GDPR is a EU Regulation (as opposed to a Directive); so it comes into force automatically across the EU next May - without the need for an Act of Parliament to trigger it. The UK will still be part of the EU on that date, so as far as UK businesses are concerned, GDPR is happening.

For further help and information about how to prepare for GDPR and on how Zonefox supports it, head on over to www.zonefox.com/gdpr

About ZoneFox

ZoneFox helps businesses around the globe protect their business-critical data against the insider threat. Our award-winning technology provides the 360 visibility of activities around your data – the who, what, where and when – by monitoring user behavior and data movement both on and off the network, and instantly alerting to anomalous activities.

Security posture is strengthened, business-critical information is protected and regulatory compliance is supported.

Like to Learn More?

ZoneFox.com

Youtube.com/ZoneFoxVideo

@zonefox

alerts@zonefox.com

Argyle House,

Edinburgh,

EH3 9DR

+44 (0) 845 388 4999

ZoneFox