Preparing for General Data Protection Regulation

by A&O Corsaire

What is GDPR?

GDPR is legislation introduced by the European Union in April 2016. Compliance with its terms become mandatory in May 2018, with **fines of between 2 and 4% of global turnover for non-compliance**. Despite the UK being scheduled to leave the EU, it is widely anticipated that the provisions of GDPR will remain a legal requirement for UK businesses.

The biggest change to businesses is that consent to use personal data must now be explicitly given, and there must be a legal basis for processing each item of data.

Does it apply to me?

If you **process**, either as a controller or processor, the **personal data of any data subjects who are in the Union** – regardless of whether the processing takes place in the Union or not – **then GDPR applies to you**.

What do we mean by processing and controlling?

Processing means any operation which is performed on personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination restriction, erasure or destruction.

The "**controller**" is the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

The "**processor**" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

What counts as "personal data"?

Personal data means any information relating to an identified or identifiable natural person (data subject); who can be identified, directly or indirectly, in particular by reference to an identifier such as name, ID number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person. For the purposes of GDPR, a data subject is a living person who is in an EU Member State.

GDPR Principles

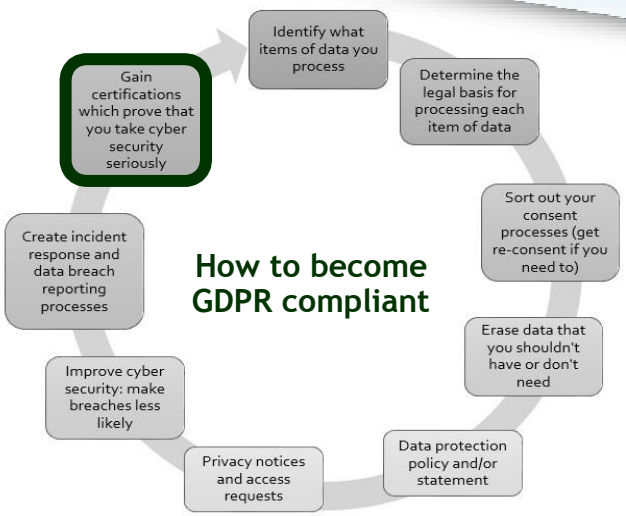
In order to be compliant with GDPR legislation, data must be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary in relation to the purposes
- Accurate and kept up-to-date
- Kept for no longer than is necessary
- Processed in a manner that ensures appropriate security

You must be able to demonstrate compliance for accountability.

You must protect the following:

- Right to be informed
- Right of access
- Right to object to processing
- Right to rectification
- Right to erasure
- Right to notification
- Right to not be profiled
- Right to portability



Cyber Security

24% of small businesses have a strict password policy

The relevance for small and medium sized businesses

According to the Federation of Small Businesses, the types of cyber-crime most commonly affecting small businesses in 2016 were phishing emails (49%), spear phishing emails (37%) and malware attacks (29%).

In 2016, 46% of all cyber attacks were directed at small or medium-sized businesses.

4% have a written plan of what to do if they are attacked online

2% have a recognized security standard such as ISO27001 or the Government's Cyber Essentials Scheme

Cyber security is now even more essential in your business, with risks of incurring large fines if data breaches are not reported to the governing authority within 72 hours.

CONTACT

A&O CORSAIRE LTD
www.corsaire.com
sales@corsaire.com
+44 (0)20 7096 9352