Be Part Of The...

Trivolution

Change • HR • Consultancy

Newsletter: Issue #24 Autumn 2017

GENERAL DATA PROTECTION REGULATION

What is General Data Protection Regulation (GDPR)?

The GDPR will apply in the UK from 25 May 2018. The government has confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR. The law aims to give individuals more control over their data and to create a uniformity of rules to enforce across the continent.

Why should businesses care about GDPR?

Although this law comes from the EU, it will have a global impact. It will affect any business holding personal data on customers, prospects or employees based within the EU, and such businesses need to be preparing for the change now.

If businesses ignore this law, they can be fined up to €20 million, or 4% of their global annual turnover.

AWARENESS

You should make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR.

They need to appreciate the impact this is likely to have and identify areas that could cause compliance problems under the GDPR. It would be useful to start by looking at your organisation's risk register, if you have one.

Information You Hold

You should document what personal data you hold, where it came from and who you are sharing it with. You may need to organise an information audit across the organisation or within particular business areas.

Individual's 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.

RIGHTS FOR INDIVIDUALS

The GDPR includes the following rights:

- the right to be informed;
- the right of access;
- the right to rectification;
- the right to erasure;
- the right to restrict processing;
- the right to data portability;
- the right to object; and
- the right not to be subject to automated decision-making including profiling.

Communicating Private Information

You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.

When you collect personal data you currently have to give people certain information, such as your identity and how you intend to use their information. This is usually done through a privacy notice. Under the GDPR there are some additional things you will have to tell people. For example, you will need to explain your lawful basis for processing the data, your data retention periods and that individuals have a right to complain to the ICO if they think there is a problem with the way you are handling their data.

SUBJECT ACCESS REQUIREMENTS

You should update your procedures and plan how you will handle requests to take account of the rules:

- In most cases you will not be able to charge for complying with a request.
- You will have a month to comply, rather than the current 40 days.
- You can refuse or charge for requests that are manifestly unfounded or excessive.
- If you refuse a request, you must tell the individual why and that they have the right to complain to the supervisory authority and to a judicial remedy.

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.

Consent

You should review how you seek, record and manage consent and whether you need to make any changes.

Data Breaches

You should make sure you have the right procedures in place to detect, report and investigate any instances of personal data breach.

Data Protection Officers

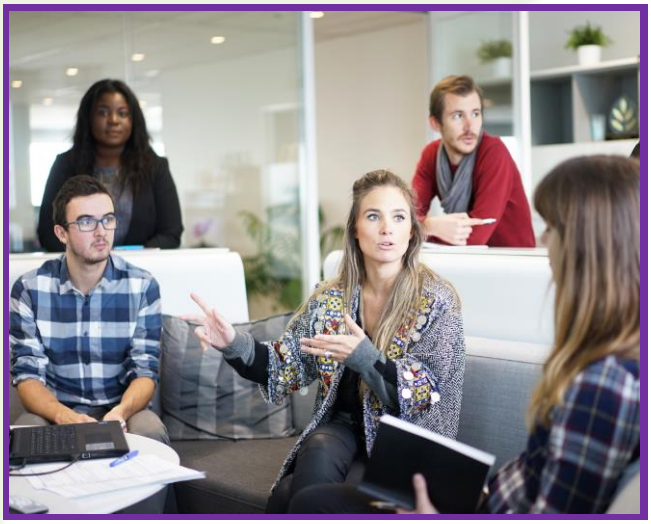
You should designate someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements.

PROTECTING CHILDREN'S PERSONAL DATA?

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. For the first time, the GDPR will bring in special protection for children's personal data, particularly in the context of commercial internet services such as social networking.

DATA PROTECTION IMPACT ASSESSMENTS

It has always been good practice to adopt a privacy by design approach and to carry out a Privacy Impact Assessment (PIA) as part of this. However, the GDPR makes privacy by design an express legal requirement, under the term 'data protection by design and by default'. It also makes PIAs – referred to as 'Data Protection Impact Assessments' or DPIAs – mandatory in certain circumstances.



Thank you for reading!

Got a question or want to know more? Let's Talk!

Call: 0114 360 1233 **Email:** info@trivolution.co.uk

Trivolution Ltd, Unit 5 Dinnington Business Centre, Sheffield, S25 3QX