GDPR

Applying the General Data Protection Regulation to your business

mediaburst

Contents

Introduction

GDPR is is now the law, and it's important, so we've put this guide together to help you comply.

The General Data Protection Regulation (GDPR) is the biggest change to data protection law for almost twenty years.

25th May 2018

The GDPR came in to effect on 25th May 2018 and the government have confirmed that the UK's decision to leave the EU will not affect implementation of the GDPR. A failure to meet GDPR regulations will result in possible fines being issued by the Information Commissioners Office (ICO).

The ICO can take action to change the behaviour of organisations and individuals that collect, use and keep personal information. This includes criminal prosecution, non-criminal enforcement and audit.

You must ensure everyone in your organisation knows that the law has changed and the impact of GDPR, so why not forward this guide around the office?

What is GDPR?

The purpose of GDPR is to provide more privacy to EU citizens by updating the existing data protection act to reflect today's digital world.

The new law does this by regulating the use of all personal data. The term 'personal data' has been expanded to include all online identifiers such as a cookie, IP address, location or an advertising ID.

Information commissioner Elizabeth Denham has said:

"If your organisation can't demonstrate that good data protection is a cornerstone of your business policy and practices, you're leaving your organisation open to enforcement action that can damage both public reputation and bank balance.

She continues:

"But there's a carrot here as well as a stick: get data protection right, and you can see a real business benefit."

Here are the 12 steps the ICO have advised all companies and individuals prioritise:

1

Awareness

You should make sure that the decision makers and key people in your organisation are aware that the law has changed to the GDPR. They need to appreciate the impact this will 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 with privacy information

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

4

Individuals' rights

You should check your procedures to ensure they cover all the rights individuals have, including how you 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 if they don't meet the GDPR standard.

8

Children

You should think 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 Protection Impact Assessments

You should familiarise yourself now with the ICO's code of practice on Privacy Impact Assessments as well as the latest guidance from the Article 20 Working Party, 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 (ie you carry out cross-border processing), you should determine your lead data protection supervisory authority. Article 29 Working Party guidelines will help you.

Who does it apply to?

GDPR applies to you if you host your site, run your business or have customers based in the EU or are based in the EU yourself.

It applies to both controllers and processors. The definitions are mostly the same as under the DPA. The controller says how and why personal data is processed and the processor acts on the controller's behalf.

Processors

The GDPR places specific legal obligations on processors. As a processor you will have significantly more legal liability if you are responsible for a breach. These obligations for processors are a new requirement under the GDPR.

Controllers

As a controller, you are not dismissed of your obligations where a processor is involved. The GDPR places obligations on you to ensure your contracts with processors comply with the GDPR.

Exempt activities

The GDPR does not apply to certain activities including processing covered by the Law Enforcement Directive, processing for national security purposes and processing carried out by individuals purely for personal/household activities.

What information does the GDPR apply to?

Personal data

The GDPR's definition of personal data is more detailed than the DPA's. Information such as an online identifier like an IP address can be personal data. These new rules reflect changes in technology and the way organisations collect information about people.

Most organisations will see little difference as if you hold information that falls within the scope of the DPA such as customer lists, HR records or contact details it will also fall within the scope of the GDPR.

The GDPR covers both automated personal data and manual filing systems where personal data is accessible according to specific criteria. This is wider than the DPA's definition and could include chronologically ordered sets of manual records containing personal data.

Personal data that has been disguised such as encoded can fall within the scope of the GDPR depending on how difficult it is to recognise the original data or individual.

Sensitive personal data

The GDPR refers to sensitive personal data as "special categories of personal data". These categories are broadly the same as those in the DPA, but there are some small changes.

Personal data relating to criminal convictions and offences are not included, but similar safeguards apply to its processing.

What are the consequences of not complying?

The potential consequences for not complying with the GDPR are massive:

The EU is able to fine organisations up to €20m or 4% of annual turnover ... whichever is greater.

For more information about GDPR, you can look at the ICO's guidelines and overview or get in touch with us.

mediaburst

Have questions?

Speak to our friendly support team for help
with setting up your brand new account:

hello@mediaburst.co.uk | 0161 359 3100

We're here to help you get all the information you need.

http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf

https://ico.org.uk/for-organisations/data-protection-reform/

http://www.marketingfile.com/knowledge/Guides/What-is-GDPR
https://dma.org.uk/article/all-about-the-gdpr

www.mediaburst.co.uk

Mediaburst, Studio 18, 18 Hilton Street, Manchester M1 1FR United Kingdom