Clear's guide to GDPR

GDPR is the EU's new regulation for the protection of personal data. It takes over from two policies that were set out in 1998 and 2003. Obviously technology has moved on massively since then, and so has the way we collect, process and manage data.

Let's take the example of mobile phones

The Nokia 3310 (released in 2000) could hold 1KB of data. Fast forward to 2015, and the iPhone X can hold 256GB, that's 268,000,000 times the amount of data!

So, as painful as it may be to get your head around, the regulations surrounding data are definitely overdue an overhaul!

We've put together this guide to give you a heads up on the basics of GDPR and provide you with 6 key things you need to be thinking about when starting to prepare for GDPR.

General Data Protection Regulation

Contents

For more information, get in touch

01743 344 911 **hello@cleardesign.co.uk** **cleardesign.co.uk**

clear

The basics

What's it all about?

- GDPR replaces the Data Protection Act of 1998 (DPA) and Privacy and Electronic Communications Regulations 2003 (PECR)
- It is concerned with the way personal data is acquired, stored and secured
- GDPR is already law, but becomes enforceable on May 25th, 2018
- Fines are up to £20 million or 4% of turnover (whichever is greater)
- Current advice is that Brexit won't affect GDPR (aka we still have to comply)

If you haven't already, now is the time to act to make sure you're compliant by the deadline of **May 25th, 2018**.

What counts as personal data anyway?

- Name
- Email address
- Mobile phone number
- Bank account details
- Address
- Credit card number
- Driver/passport number
- Genetic or biometric data

For more information, get in touch

01743 344 911 hello@cleardesign.co.uk cleardesign.co.uk

clear

Principles

GDPR says that personal data must be...

1

Processed lawfully, fairly and transparently.

2

Collected for specific, explicit and legitimate purposes. Further processing must not occur outside the original reason for collection.

3

Only collected for the purpose specified – no unnecessary data should be acquired.

4

Accurate and kept up to date.

5

Kept in an identifiable format for as little time as possible for the purpose specified.

6

Processed securely to protect against loss, destruction or damage.

For more information, get in touch

01743 344 911 **hello@cleardesign.co.uk** **cleardesign.co.uk**

clear

Data Processing & Consent

Data Processing

You need to document your reason for processing personal data (and make sure it's lawful).

Lawful reasons include:

- They have consented (more on this below)
- It's necessary to fulfill a contract with the data subject
- You have a legal obligation
- Processing protects the interests of the data subject

Consent

In GDPR, consent must be informed and unambiguous – the user has to clearly opt in (gone are the days of pre-ticked tick boxes).

Opt-Ins must be separate from T&Cs and be specific in terms of what will be done with the data.

You will also need to provide simple ways for the user to withdraw consent.

The rules are different for B2B vs B2C data though:

- **B2C or named B2B data (e.g. bob@apple.com):** You need explicit consent to use data at the point of data collection. If someone consents, there needs to be the option for them to be forgotten at any point.
- **B2B:** For a publicly available email address, consent is not required although there must be a legitimate reason for contact, and they must be given the option to unsubscribe.

For more information, get in touch

01743 344 911 hello@cleardesign.co.uk cleardesign.co.uk

Individual's rights

The right to be informed

You need to tell the data subject how you will use their data at the point of data collection. You also need to have an overall privacy statement on how you handle data (for example a Privacy Policy on your website)

The right of access

Individuals must be able to confirm with an organisation if their data is being processed, and be given access to their personal data if requested.

The right to rectification

Individuals must be able to have their data updated if it's incorrect or incomplete.

The right to erasure

Individuals data must be removed from your database if requested.

The right to restrict processing

Individuals can allow you to store their data, but can request that it is not processed any further.

The right to data portability

This relates to the individual being able to contact you and requesting all of the data you hold on them to transfer to another organisation. This data must be provided in a simple and commonly used format.

The right to object

Individuals can object to processing even for legitimate interests, direct marketing and processing for research/statistics.

Rights in relation to automated decision making and profiling.

This relates to automatic processes that are completed without human intervention that may have detrimental effects on the individual. You need to ensure that individuals are able to challenge the decision and obtain human intervention.

For more information, get in touch

01743 344 911 hello@cleardesign.co.uk cleardesign.co.uk

Where do I start?

So we've established that GDPR is coming, and we have no choice as businesses but to act. We know it's a daunting task, but here are 6 key steps to get you on your way to being GDPR compliant....

Assign a Data Protection Officer

All businesses, no matter how big or small, are subject to GDPR. It's important to have one person, or a team of people in charge of GDPR. For smaller companies, this can form part of someone's role, but for bigger organisations you may require one or more people dedicated solely to Data Protection.

Data Protection Impact Assessment

You need to consider the different areas of your business and how they collect, process and store data, including third party software such as email marketing software. A data protection impact assessment (DPIA) can help you collate this into one document, so you can consider your next steps. There are many templates for this available online.

Privacy Policy

Make sure your website's Privacy Policy is up to date – it needs to include how you collect, process and store personal data.

Online Forms

If you collect data via online forms, make sure there is a statement below the form on how you will use the data. If you're using the data for marketing purposes, make sure there is a clear tick box for the user to opt in.

Unsubscribe Options

You must make it clear that individuals can unsubscribe from marketing at any time. This should be included in your privacy policy, and also in any marketing such as email newsletters, direct mail etc.

Record Consent

You must keep a record of when and how you got consent from individuals, and what they were told.

Remember – this data must be kept in an encrypted, secure file.

For more information, get in touch

01743 344 911 **hello@cleardesign.co.uk** **cleardesign.co.uk**

clear

Clear's Guide to GDPR

(Version 1) – 01/11/2017

This information is our interpretation of the regulations and guidance currently available on GDPR. This resource is not to be taken as legal advice and Clear cannot be held accountable for the legal validity of this resource.

Sources:

http://www.thedrum.com/opinion/2017/10/31/8-tips-help-you-prepare-the-gdpr

http://www.smartinsights.com/advice/gdpr-briefing/

https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/

https://www.wired.com/video/2016/08/nokia-3310-vs-iphone-6s/

For more information, get in touch

01743 344 911 hello@cleardesign.co.uk cleardesign.co.uk