GDPR Overview

General Data Protection Regulation

ClickReach's guide to upcoming changes

In May 2018, what we now know as the Data Protection Act (DPA) will be changing. In a bid to strengthen and modernise data protection legislation, the EU commission will instate the General Data Protection Regulation (GDPR).

With less than two years of transition time in a quickly evolving digital world, the time to prepare, get informed and act **is now**.

01376 653168 admin@clickreach.com www.clickreach.com

The GDPR Basics:

Currently, the DPA, in conjunction with the Privacy and Electronic Communications Regulations (PECR) govern how personal data is handled. There are clear rules and guidelines specifically relating to direct marketing calls, emails, texts and tracking via cookies (to name a few). Both sets of guidelines overlap to ensure personal data is handled appropriately across a range of media.

Until now, legislation only applied to controllers, however, the new GDPR will shift the responsibility for compliance across controllers and processors. In a four year-long process, the EU have amalgamated and updated the key principles in the current framework to generate a single legal framework that applies to all EU members. **Non-compliance will result** in **heavy penalties**.

Does this change affect my business?

The GDPR applies to any business that collects, stores and uses personal data. This may include:

- Customer information
- Data in a CRM system
- Use of direct and/or electronic marketing
- Use of B2B marketing data

The above applies, so what should I do?

Start by generating a **full audit trail** and document your data from origin to destination, including third party sharing. Ensure you are confident that you know where your data comes from, what type of personal data your business holds, and that you currently hold **all necessary consent**.

So, what about existing data?

If your existing data is not GDPR compliant, remove it. This may apply to data of unknown origin, or with unproven consent.

And new data?

All new data gathered must be GDPR compliant, and that you can evidence how. See the GDPR basics on the following page for more information.

I'm compliant, so how can I prove it?

Keep audit trails detailing your sources, enquiries, communications via your sales team and any accompanying information confirming consent.

01376 653168 admin@clickreach.com www.clickreach.com

GDPR in a Nutshell

Accountability and Transparency

Under the new regulations, data controllers will need to continually maintain **demonstrable evidence of compliance** and be able to produce it when required. As a result, privacy policies and statements will almost certainly require adjustment to ensure optimum transparency surrounding data processing. How an individual's data may be used and processed should be explained in a 'clear and understandable way'.

Consent

Key issues surrounding consent are the individual's right to object and the controller's obligation to gain consent specific to each data processing activity. Consent must be **"freely given, specific, informed and unambiguous and given by means of a statement or clear, affirmative action."** Where personal data is processed for direct marketing, the data subject will have a right to object. In addition, the GDPR reinforces that consent is not freely given if the subject has no free choice or is unable to withdraw without negative impact. It should be as easy to withdraw consent as it is to give it.

Right to Be Forgotten

Provided there are no legitimate grounds for controllers to retain data, individuals now have the right to request it is deleted. Furthermore, controllers must make reasonable effort to ensure third parties are informed of the individual's request.

Subject Access Request

Individuals have the right to request access to their data at no cost, within one month. Individuals may also request that data gathered about them is narrowed down.

Data Portability

Individuals can request that their data be provided in a useable format for direct transfer to another controller.

Reporting Breaches

It is mandatory for companies and organisations to notify the supervisory authority in the event of a breach within 72 hours. Subjects must be contacted in the event of a high risk breach to implement appropriate measures.

Fines

Breaches of the new legislation will incur heavy sanctions, with fines of up to 4% of annual turnover, up to 20 million Euros. With a tiered penalty system exceeding its predecessor, the GDPR's increased fines reflect a step up in data handling legislation.

01376 653168 admin@clickreach.com www.clickreach.com

Key Players: Roles and Responsibilities

Data Protection Officers (DPOs)

Certain organisations, particularly those with processing operations which require large scale monitoring and public authorities, will be required to appoint a DPO. This individual may be already employed or under a service contract and have sufficient expert knowledge dependent on the company's processing activities.

The One Stop Shop

Conceptualised to address the centralisation of the DPA framework, the idea behind creating a 'One Stop Shop' across all EU countries has faced criticism for being over simplified. However, the concept has translated to a regime whereby local and urgent cases will be handled by designated Lead Authorities.

New European Data Protection Board

An independent EDPB will issue opinions and guidance on cases, ensuring consistent application of the GDPR and reporting to the Commission. Integral to the consistency and success of the 'One Stop Shop' model, the EDPB will replace the current Article 29 Working Party. It will comprise of senior representation from the national Data Protection Authorities and the European Data Protection Supervisor.

Get GDPR Ready

Review

Review your business privacy statements to ensure they are GDPR compliant.

Monitor

Create and maintain detailed audit trails of where your data has come from.

Analyse

Examine any data used in the last 12 months and remove any non-GDPR compliant information.

Get private

Embed privacy into any new processes to pre-empt the upcoming changes.

Lockdown

Prepare for data security breaches by generating water-tight policies and company-wide awareness of notification time frames and requirements.