Getting ready for the

GDPR

Introduction

The General Data Protection Regulation (GDPR) is the result of four years of work by the EU to bring legislation up-to-date and in line with the ways that data is now used.

The GDPR will have implications to all businesses that process the data of EU citizens. With this in mind, we've put together this document to help marketers get a better understanding of the forthcoming changes, and how to prepare for them.

The Digital Single Market

The GDPR owes its existence to the European Union's 'Digital Single Market Strategy', published back in May 2015.

Due to various legal or administrative restrictions between states, and the associated complexities these often bring, only 7% of small and medium-sized businesses in the EU trade across borders.

The idea of the Digital Single Market is to try and remove barriers by standardising and simplifying regulations, and it is hoped that this will help businesses to take full advantage of the European market as a whole.

In order to protect consumers as part of the new Digital Single Market, the GDPR was created to give individuals better protection and control of their personal data.

The increased confidence and trust in digital goods and services will create a more successful digital economy.

When do the changes come into effect?

The GDPR was adopted in April 2016, but isn't going to be enforceable until the 25th of May 2018. As we'll have had two years to get up to speed, there isn't going to be any kind of grace period, so you'll need to make sure you're ready in time.

Who does it affect?

The GDPR applies to any company based in the EU, but additionally any organisation that is processing the data of EU citizens.

That means that regardless of whether you're a data controller or processor, and regardless of where you're based or where the processing is taking place, you'll need to comply with the GDPR if it relates to EU citizens.

What happens if you don't comply?

€20 million OR **4% annual global turnover**

WHICHEVER IS HIGHER

Failure to comply with the GDPR can result in unprecedented financial penalties. These can be as high as 20 Million Euros or 4% of your company's global annual turnover, whichever is highest in each case.

Getting ready for GDPR

12 STEPS

The ICO have published a 12 step guide you can follow to prepare for the GDPR. This guide includes a summary of the key points and resources that will be of use to you when preparing your own business for GDPR compliance.

1

Awareness

Initially, making sure everyone at your business is aware of the upcoming changes will be key, along with the impact this will have on any data you hold.

Hopefully you won't need to make too many changes, but by giving everyone in your organisation time to review everything that is necessary, you can avoid a last minute rush.

2

Information you hold

Conduct an audit on all of the personal data you hold, whether it's about your customers or your staff.

The kind of details you'll want to consider are:

- What kinds of data you hold
- What consent each individual gave (or didn't give)
- Where you obtained it
- How long ago it was obtained
- How and where it is stored and used

Once this is established, you'll be in a much better position to review your compliance and any steps that you may need to take as a result.

3 Communicating privacy information

You should review your current privacy notices and ensure these are all in line with the new regulations.

Make sure you're telling individuals who you are, how you intend to use their data, and anyone it will be shared with. For more information on how to structure this, the ICO have published details which are linked to below.

Privacy notices, transparency and control overview

Privacy notices, transparency and control

4 Individuals' rights

The GDPR includes the following rights for individuals:

- 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
- the right not to be subject to automated decision making including profiling

You'll need to review your processes and practices to ensure that you can accommodate individuals rights.

For example, a recipient can request all of the personal information you hold on them to be erased, so carefully consider how you'd facilitate this.

Individuals rights - ICO

5 Subject access requests

As with the current Data Protection Act, an individual is entitled to contact you requesting any personal data you hold on them, what you're doing with it and who you share it with. The GDPR strengthens this, for example specifying that you have 30 days to comply and that you're not allowed to charge for these types of requests, unless the request is deemed excessive. You should update your procedures and plan how you will handle these requests, especially if they start appearing in large numbers.

Subject access requests - ICO

Subject access requests code of practice - ICO

6 Lawful basis for processing personal data

Under the GDPR, you need to ensure that you have a lawful basis for processing any personal data. This should be documented and published within your privacy information.

For more information on this, the ICO have explained what constitutes lawful basis on their website:

Lawful processing: key areas to consider - ICO

7 Children

The GDPR includes specific protection for the personal data of children. If your organisation relies on consent to collect information about children, you will need to consider whether you need to put systems in place to verify individuals' ages, and to obtain parental or guardian consent for any data processing activity.

8 Consent

The GDPR sets new standards in terms of consent, and defines it very clearly:

'Consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her'

In practice, this means that:

- Asking for consent should be clear and unbundled. In other words, separate from any other terms and conditions, so individuals are clear what they are consenting to and given choice.
- You can't make consent a precondition of receiving a service, unless it is absolutely necessary to provide the service. For example, automatically being opted in to receive marketing emails just to access free wi-fi is now not allowed.
- Consent requires a positive opt-in. Pre-ticked consent boxes are specifically banned. This type of passive consent is no longer sufficient.
- Individuals need to know who the organisation is, and specifically name any third parties that the data will be shared with. Saying that you're consenting to be contacted by 'carefully selected third parties' is no longer sufficient. Transparency is key.
- Individuals should be easily able to withdraw their consent. Having an unsubscribe option behind a login page is no longer acceptable; it should be as simple and clear as possible.

Consent guidance - ICO

9 Data breaches

The GDPR requires all organisations to report certain types of data breach to the ICO, and in certain cases to individuals.

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

Security breach overview and guide - ICO

10 Data Protection by Design and Data Protection Impact Assessments

The GDPR makes data protection by design a legal requirement, so you'll need to ensure that you're considering this moving forward.

As part of this, the GDPR makes privacy impact assessments a requirement for any processing that is considered high risk.

Further details of this can be found below:

Protection impact assessment code of practice - ICO

11 Data Protection Officers

Under the GDPR, you are required to appoint a Data Protection Officer if you are:

- A public authority (except for courts acting in their judicial capacity)
- An organisation that carries out the regular and systematic monitoring of individuals on a large scale
- An organisation that carries out the large scale processing of special categories of data, such as health records, or information about criminal convictions.

Regardless of whether you're required to, it's probably a good idea to ensure you have someone who is responsible for compliance on an ongoing basis.

Guidelines on Data Protection Officers - Article 29 data protection working party

12 International

If your organisation processes data in more than one EU member state, you should establish who your lead data protection supervisory authority is.

Some guidelines to help you work out whether you're required to do this and how to proceed can be found below.

Guidelines for identifying a controller or processor's lead supervisory authority - Article 29 data protection working party

What are Pure360 doing to prepare for GDPR?

In many ways, the GDPR simply puts into law a lot of the best practice ideas and principles that we've all known are an effective way of increasing customer trust and engagement.

As a result, we believe the GDPR has the potential to revolutionise the email marketing landscape for the better, and we're committed to making sure our customers are able to make the most of this opportunity.

Along with everyone else, we're following the ICO's advice by conducting a full review of our processes, practices, platform and infrastructure, so that our customers will have the confidence that Pure360 are fully GDPR compliant by the time the GDPR comes into effect in 2018.

Suggested further reading

Preparing for the GDPR - ICO

Dma.org.uk/gdpr

What to expect and when - ICO

Note: Pure360 does not provide any legal or auditing advice, and while every effort has been made to ensure accuracy, the contents of this guide should be viewed for information purposes only. Pure360 strongly recommends everyone seek their own specific legal advice regarding the impact of the GDPR on their organisation.