The Marketing Pod's Guide to...

GDPR

Q. What is GDPR?

A. 'Game changing' data protection rules you shouldn't ignore

New legislation around data protection is coming, and it's something every business and marketer needs to be aware of. At a time when data, digital communications, and information systems underpin our everyday lives, the General Data Protection Regulation (GDPR) will make a real difference to the way you can collect, store and share customer data – and failure to comply could mean hefty fines.

It's time to act

Despite the increased responsibility about to be placed on businesses and the increased threat of enforcement action for those who fail to take appropriate action, it's not always easy to understand exactly what businesses should be doing to ensure compliance. That's not to say that you can afford to wait for clarification; the compliance deadline comes without a transition period and the new regulation has been described as a 'game changer for everyone' by the UK Information Commissioner Elizabeth Denham.
Our advice would be: act now.

With that in mind, we've created this easy to use guide. It covers what we believe are the key changes brought about by GDPR for businesses who use data for marketing purposes.

While it's difficult for anyone to answer the many questions still surrounding GDPR and how it will be interpreted or enforced in practice, we hope to offer a helpful starting point on the path to compliance.

Our advice would be: act now.

GDPR – A quick look at the basics

Name: General Data Protection Regulation

Compliance deadline: 25th May 2018

Areas affected: All EU member states must comply from the same date. The government has confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR.

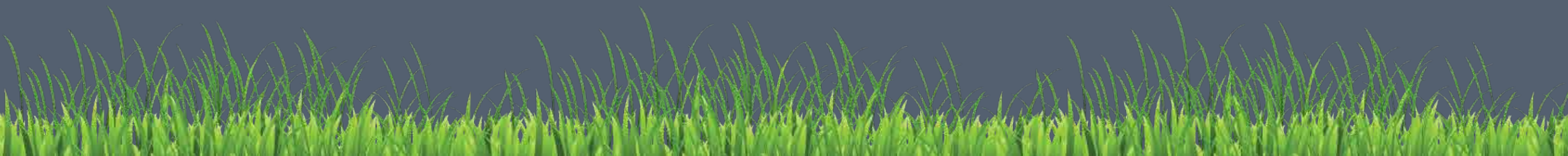
Transition period: none

Aim: Protection of consumer rights (GDPR replaces the Data Protection Act)

Effect: Tighter controls around data control, access and security – with much harsher penalties for non-compliance.

Business affected: All. Business of all sizes are affected by GDPR, although SMEs (less than 250 employees) who only hold small amounts of customer data and use it carefully and infrequently, will have a lighter burden to bear. These organisations will still need to implement high security standards - but when it comes to processing data, they'll only be caught by the regulation if the processing carried out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data.

How this will be interpreted by legislators remains to be seen.



Controllers and processors: Affected businesses will either fall into the category of data controller or data processor (or both). The controller says how and why personal data is processed and the processor acts on the controller's behalf. If you are a processor, the GDPR requires you to maintain records of personal data and processing activities. The GDPR will therefore mean new obligations and new liabilities in the case of a breach. If you are a controller, the GDPR places obligations on you to ensure your contracts with processors are compliant.

Penalties under GDPR? Failure to comply with the GDPR will lead to weightier punishments. Under current rules, the UK's Information Commissioner's Office (ICO) can fine up to £500,000 for a breach but the GDPR will raise this to €20 million or 4 per cent of annual turnover. In addition, individuals can sue you for compensation to recover both material damage and non-material damage, like distress.

B2B marketing and GDPR

No distinction is made between B2C and B2B activities under the GDPR. At the moment, B2B businesses can rely on the 'soft opt-in' permitted under the Privacy and Electronic Communications Regulation (PECR). However, the EU is in the process of revising the directive which informed this UK legislation. The new Regulation on Privacy and Electronic Communications will replace the EU ePrivacy Directive and is intended to come into force on the same day as GDPR. It is currently unclear whether it will maintain the approach of the PECR, or bring B2B regulations into line with GDPR. Either way, B2B businesses would do well to start getting their data processes ship shape – and those who start preparing for the worst will be in a better position next year, if the soft opt-in is whipped away from them.

5 things you need to know about GDPR?

So, what's changed? If your business is already doing a good job of complies under the requirements of the Data Protection Act (DPA), or comply with international data security standards such as ISO 27001 or PCI-DSS, you have a strong foundation for meeting your obligations under GDPR. However, the most important thing to recognise about the new GDPR is that it is much more than a revised version of the DPA. Its reach is wider, it introduces brand new concepts - such as the right to be 'forgotten' - and when it comes to enforcement, its status as a Regulation (rather than a Directive) gives it the immediate full force of EU Law.

1 Asking for consent

Here's a closer look at what we believe are the five most important changes brought about by GDPR.

> Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement."
>
> **Recital 32**

Perhaps the most significant change for businesses and marketers is the new requirement for explicit and unambiguous consent. Under this new stricter test, businesses will be required to gain consent for each separate processing activity and will need to provide clear information on how data will be used, along with more granular options for customers to choose from when providing consent, to give them maximum control on how their data is used once they've handed it over.

In addition, documents requesting consent must be clear and easily identifiable by the customer; separate from other written documents or agreements. The easy option of 'bundled' consent will no longer be available to marketers, nor will businesses be able to offer products or services for which customer requests can only be processed once consent is given – rendering consent forced as opposed to 'freely given'. Silent consent is a thing of the past and inactivity as consent is also no longer acceptable.

Action: Data cleansing and re-engagement

If you need to contact your existing database to gain consent that meets the GDPR test, do so before next year's May deadline, as you won't have permission to do so afterwards! It might be worth considering a re-engagement campaign – but make sure you've got GDPR compliant systems in place to handle the data you collect first (see point 5).

When updating your data collection comms, check that your consent requests are kept separate from other terms and conditions. Use plain English, avoid technical descriptions and keep your request specific and concise.

Signed statements are fine, binary choices with equal prominence given to 'yes' and 'no' are also OK. While tick boxes agreeing to data collection or processing will still be commonplace after May 2018, they will certainly always need to start off blank, requiring action for positive consent.

Need help planning a re-engagement campaign?
We can help!

Rethinking your privacy statement

The GDPR requirement for informed consent can be covered by a clear, comprehensive yet concise privacy statement. You will need to tell customers the following things in a way you'll be sure they understand:

- Who you are (and who any third parties with data access are)
- How you will use their data eg. to tailor marketing comms around their preferences
- How you will keep their data secure
- Why you need their data and how long you will keep it
- What their rights are. This is REALLY important and must include details about their right to access and revoking consent.

2 Providing the option to revoke consent

Under the new regulation, providing customers with easy ways to revoke their consent is as important as ensuring that you have obtained consent fairly. Put simply, you must make it at least as easy for customers to revoke consent or 'opt out' of your database as it was for them sign up and allow you to hold or process their data. In practice, this is likely to require organisations to provide for consent to be withdrawn through the same media (e.g. website, email, text) as it was obtained. The customer's right to withdraw consent - and the method by which they can do so - should also be covered clearly and concisely in your privacy statement.

Action: The right to be forgotten

As well as updating your comms and carefully reviewing the options you provide to customers who may want to opt out of your database, it's important to check your system capabilities well in advance of next May's deadline, to be sure you have the technical ability to remain compliant.

This is because, under GDPR, every individual has the right to request complete removal of their data from a database when it is no longer being used for the purpose for which it was given or where it has been processed unlawfully. A customer's right to object to the use of their data for direct marketing purposes is an absolute one, unmitigated by legal or national security related issues.

Once requested, their removal from your database needs to take place quickly and completely. You may need to talk to your technology provider to find out what the technical limitations of your database systems are, as some don't allow for complete removal of records without leaving a trace.

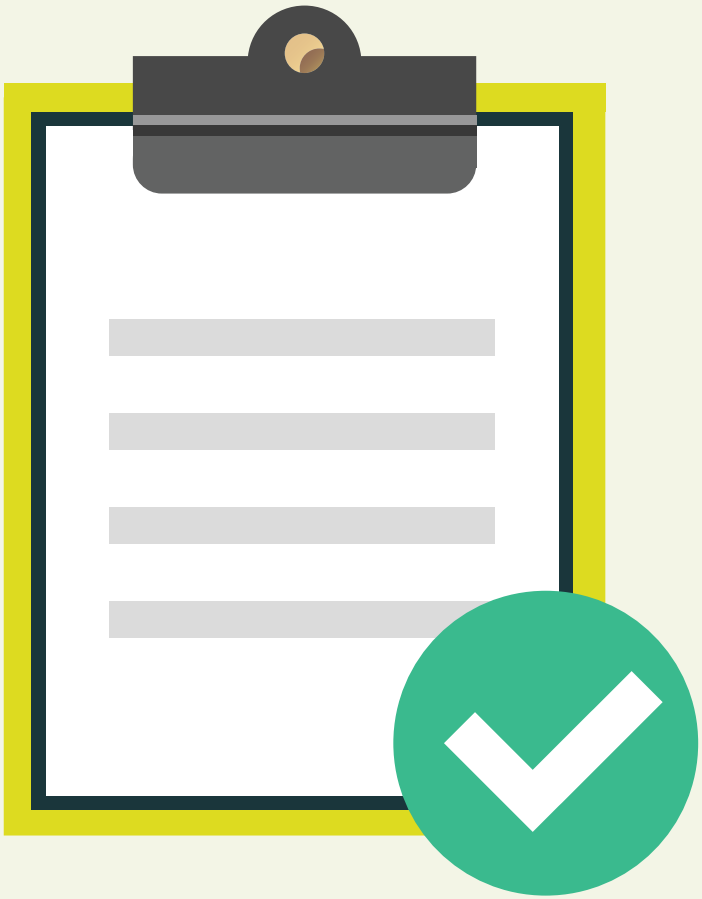
3 No nonsense transparency

The requirement for transparency runs through all sections of the GDPR. It's a special concern of the legislation and businesses would therefore be wise to integrate transparency across all business communications. The new GDPR combines and rationalises the various transparency obligations which currently exist across the EU. There is an extensive list of information which data processors are required to give before they obtain consent, and if your processing requirement is for 'legitimate business activity' then it's vital to clearly and concisely define that activity. In practice, this means you'll need to lay out the how, why, where, when and what. Again, it's possible that your privacy statement that will do most of the hard work here, so getting this document right, flagging it up at all the right moments, and making it really easy to access is essential.

Action:

Creation of new, user friendly customer documents is important, but in many cases 'one size fits all' comms simply won't cut it. GDPR demands integrated and tailored communication that prioritises customer control over their data. Think about whether your organisation will need to tailor comms to different customer groups and how to make information easy to access and understand for those groups.

The challenge is a big one: there's a long list of information to provide and a requirement that you do it in a clear and concise fashion. Might a video or other, less traditional approach work for your audience? If you use digital processes, check the timing of communications and flow of information, to be sure that your customer is receiving the right information at the right time.



4 A broader definition of personal data and sensitive data

As with the Data Protection Act (DPA), GDPR applies to 'personal data'. Under a newly concise definition, this translates as: 'any information relating to an identified or identifiable natural person'.

The effect of this shorter definition is actually to broaden the meaning of 'personal data' so that it reflects advancements in technology and changes the way businesses collect information. For instance, ambiguity about online identifiers such as IP addresses, cookie IDs and location data has been cleared up by the more expansive definition.

It's also important to recognise that both manual and automated personal data systems are caught by the new data processing rules, which apply wherever data is accessible or searchable according to specific criteria. The definition of what constitutes 'sensitive' personal data – and therefore requires stronger justification for processing - is broadly the same as in the DPA but with some small changes. For example, the wording specifically covers genetic data and biometric data whenever it is processed to uniquely identify an individual.

Action: Reassessing data and introducing 'pseudonymisation'

Now is the time to review and reassess the data you hold against this new expanded definition of 'personal data'. It may also be the time to consider whether statistical analysis, customer profiling or campaign planning could work equally well with a pseudonymisation process in place. Whilst pseudonymisation is a bit of a mouthful to say, it could help you streamline your data handling, as using this technique serves to relax some of the stringent processing rules imposed by GDPR eg. it may allow you to use data for a slightly different reason than that declared when collecting it.

Pseudonymisation also helps you to boost security and protect your customers from data breaches. It is incentivised by GDPR and included as an example of a technique which may satisfy requirements for organisations to implement 'privacy by design and by default' – a concept at the very core of GDPR.

What is 'privacy by design?'

Privacy by design is an approach to projects that promotes privacy and data protection compliance from the start. Unfortunately, these issues are often bolted on as an after-thought or ignored altogether.

ico.co.uk

What is 'privacy by default?'

Privacy by Default simply means that the strictest privacy settings automatically apply once a customer acquires a new product or service. In other words, no manual change to the privacy settings should be required on the part of the user. There is also a temporal element to this principle, as personal information must by default only be kept for the amount of time necessary to provide the product or service.'

eudataprotectionregulation.com

5 The importance of accountability

Under GDPR, it's not enough to have consent; you must be able to prove that you have consent. Nor is it enough to process data compliantly; you must be able to prove that you do so. There will be a new burden on businesses to equip themselves with the systems they will need to handle data in a way that creates a trail and makes them accountable. There must be structures and processes in place to record data processing activities, as well as processes for all relevant team members to follow when they need to handle and refresh data and consent. For many businesses, this may mean an investment in technology, for others it may mean time spent on retraining the entire team.

Action: Be prepared to demonstrate compliance

When it comes to GDPR, an informed and educated team will be as important as the right tech. Start now, by looking at your internal policies and organising staff training sessions, internal audits and reviews of HR policies. Think about ways in which you can minimise the data that you hold and pseudonymise it wherever possible. Businesses with more than 250 employees will need to appoint a data protection officer if they don't already have one. Your data protection officer will have responsibility for ensuring that relevant documentation on data processing is maintained.

Perhaps most importantly, subject your data security measures to close scrutiny, and think about how a policy of continual improvement could be implemented in your organisation.

Accountability and keeping track

Under GDPR, businesses who process data will need to record the following things:

- Name and details of your organisation (and where applicable, of other controllers, your representative and data protection officer).
- Purposes of any data processing that takes place.
- Description of the categories of individuals and categories of personal data processed.
- Categories of recipients of personal data.
- Details of transfers to third countries, including documentation of the transfer mechanism safeguards in place.
- Data retention schedules.
- A full description of technical and organisational security measures.

And finally...

The benefits of building a culture of privacy

Although many businesses will be worried about the additional burdens of GDPR, there is also an interesting commercial opportunity here for those who embrace it. Yes, businesses will need to work harder to get people to opt in- but those who do say 'yes' – and make an informed choice to do so - are much more likely to engage with any communications from you in the future. When it comes to leads, think quality over quantity; when it comes to documentation, create a privacy statement that your customers will find as compelling as a good content piece; when it comes to getting a return on your GDPR investment, turn the new regulations to your advantage by letting customers know how much you care about their data and what you are doing to protect it. Make security and transparency core to your brand messaging. In today's digital world, it's something your customers will care about – whatever your sector.

When it comes to creating a culture of privacy throughout your organisation, board buy-in will be essential – but don't forget about the rest of the team. It will be an easier journey with everyone on board.

What can we help with?

Planning re-engagement campaigns, compelling customer comms...

Useful resources:

GDPR full text, neatly arranged: https://gdpr-info.eu/

Getting ready for GDPR checklist: https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/getting-ready-for-the-gdpr/

THE MARKETING POD®

The Marketing Pod
Ideas HQ, Unit 1-3 Umberslade Business Centre,
Pound House Lane, Solihull, B94 5DF

Email: hello@themarketingpod.co.uk | Call: 01564 742 848