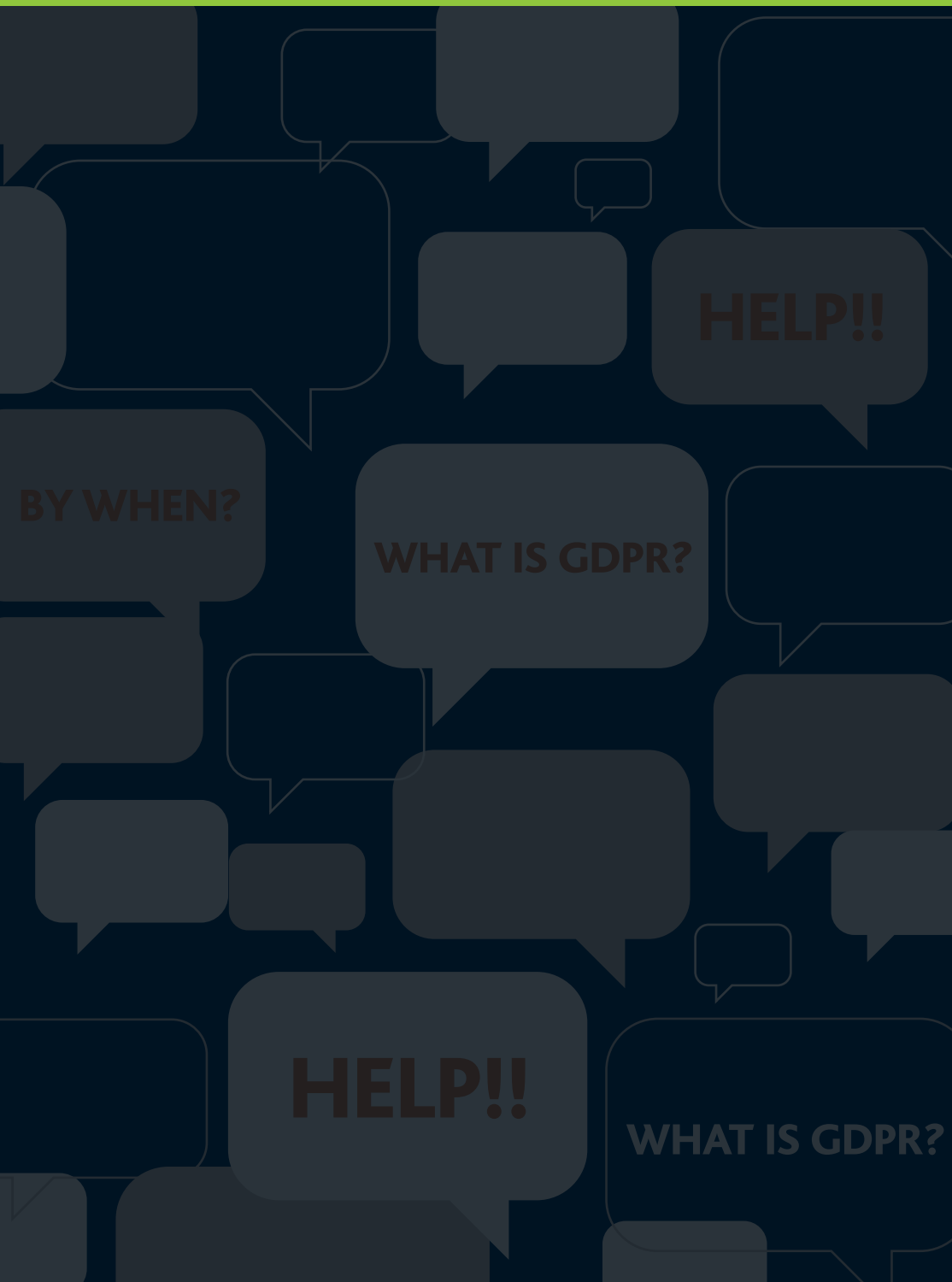
DISCOVER GDPR

T: 01708 86 55 44 *E:* sales@mailingguy.co.uk


HELP!!
BY WHEN?
WHAT IS GDPR?
HELP!!
WHAT IS GDPR?

CONTENTS

The information in this booklet is for guidance only and not suitable for all companies or situations. All companies MUST fully research into GDPR. For further information please contact ICO (Information Commissioner's Office).

All information is believed to be correct at time of print. Feb 2017

INTRODUCTION

WHY YOU NEED TO BE AWARE OF GDPR

The new General Data Protection Regulation (GDPR) comes into effect from the 25th of May, 2018. Yet, a shocking...

62% **OF BUSINESSES IN THE UK DON'T UNDERSTAND WHAT IT MEANS!**

GDPR gives everyone more control over their personal data. Any business that collects customer data needs to ensure that explicit consent has been given and that all relevant information is communicated in plain, no nonsense terms.

As a business owner, you need to review your data collection policies to make sure that they comply with the new regulations. If you don't, you could be hit with a fine of up to £20 million.

It's not all doom and gloom though.

This Book will tell you all you need to know about GDPR and how to prepare your business.

If you need more information, check out the Information Commissioner's Office's detailed guidance at https://ico.org.uk.

NEW RULES AND WHAT THEY MEAN

Before we get going, you need to understand what GDPR actually is.

What data does GDPR refer to?

What rights do customers have?

And what do you need to do to be ready for 25th of May?

THE DATA YOU KEEP

WHY YOU NEED TO BE AWARE OF GDPR

GDPR applies to any personal data you store about your clients. That means any data you keep that can be used to identify a particular individual, including; name, ID number, location data, or computer IP address.

If you're keeping any personal details, even if you just use tracking on your web-site, you need to think about how you're going to store that information securely.

THE RIGHT TO BE INFORMED

Whatever data you gather, individuals need to be kept updated. They need to know what personal information you're storing and what you're going to do with it. All communication with your clients on this subject must be straightforward and free of charge to access.

WHAT DOES THIS MEAN FOR ME?

In one of our previous eBooks, we advised asking customers and prospective customers for their contact details so that you can follow up with them later. Under GDPR, this can still be a valuable tactic, but you may need to review how you go about asking for those details.

- Consider what data you collect now
  - do you need it all?
- Consider how you're storing this information
  - is it secure?

CONSENT AND LEGITIMATE INTEREST

Under the new regulations, collecting and using data can only be considered legal if it falls under one of the lawful bases for processing. Before you collect any data, you need to be able to identify which one you are working under.

CONSENT

One lawful basis for processing is gaining the **"consent of the data subject"**. Consent is a very important element of GDPR because it puts the consumer in control of their own data.

Below are the forms of consent that you must collect for various marketing approaches.

METHOD OF COMMUNICATION	INDIVIDUAL CONSUMERS (plus sole traders and partnerships)	B2B (companies and corporate bodies)
Live calls	Screen against the Telephone Preference Service (TPS) Must be an option to opt out	Screen against the Corporate Telephone Preference Service (CTPS). Must be an option to opt out
Recorded calls	Consumer must have given caller specific consent to make recorded marketing calls.	Consumer must have given caller specific consent to make recorded marketing calls.
Emails or Texts	Consumer must have given sender specific consent to send marketing emails/texts. Or a soft opt-in is given (i.e. subject is a customer or has shown significant interest in the business) and there is an option to opt out	Can email or text corporate bodies Good practice to offer opt out options Individual employees can opt out
Mail	Name and address obtained fairly Must be an option to opt out	Can mail corporate bodies Individual employees can opt out

Another lawful basis for processing is if there is 'legitimate interest'. That is, if processing data is...

"Necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject".

In other words, you can store data as long as you can argue that what you need it for is beneficial to both you and the data subjects. You can head here for more specific examples of legitimate interest but, for now, here are a few reasons you might store data;

COLLECTING AND STORING DATA

- Direct mail purposes when you can show that your customers will benefit too - **such as an offer.**
- If you already have a relevant relationship, such as if the subject is a client.
- If you are expected to process a person's data **- like public authorities.**
- To be sure that people who've specifically asked not to receive direct mail don't get sent any by mistake.
- To personalise a web user's experience, perhaps by showcasing other items that they may be interested in.

CHANGES TO CONSENT

If you were ever unsure of what counts as solid consent, don't worry. Under GDPR guidelines, the definition of consent has been clarified to give everyone a much more conclusive understanding of what's acceptable.

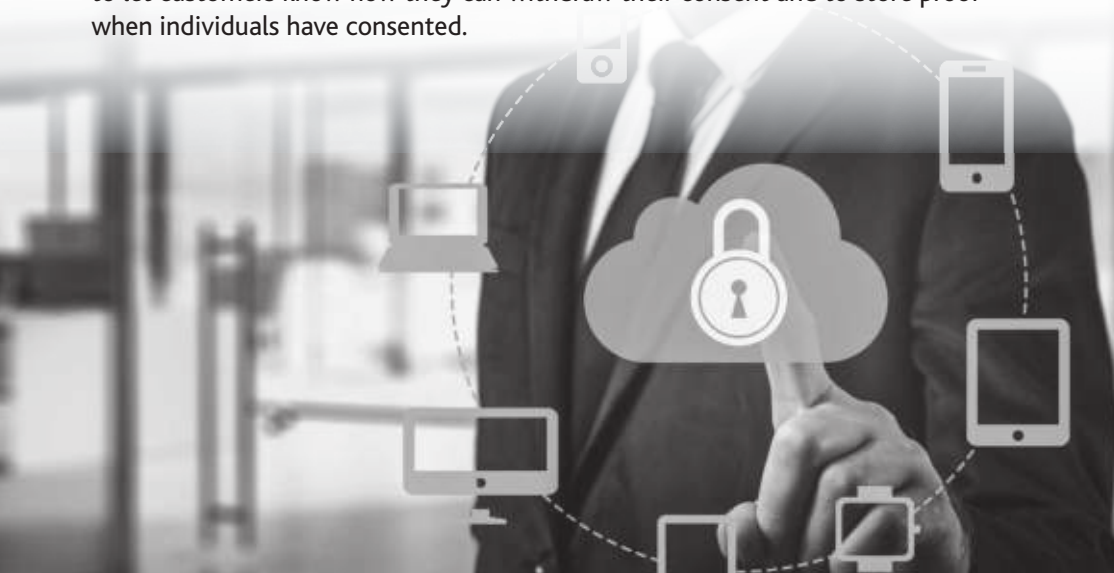
OPEN AND CLOSE

Consent means giving people control over their data. It must be clearly laid out, and there must be a way for individuals to opt out. You must also keep consent under review by making sure you refresh the terms with any updates.

TRANSPARENT COMMUNICATION

GDPR is very keen on transparency. Consumers should know exactly how their data is going to be used and they must be told in clear, easily understood language. There shouldn't be any rotten tricks like pre-ticked boxes or confusing terms like "Tick this box if you do NOT want to receive emails from us".

In addition, GDPR addresses the issue of most people not reading the terms and conditions. Therefore, to make sure they get read, consent boxes should be kept away from any other terms and conditions. Businesses also have a responsibility to let customers know how they can withdraw their consent and to store proof when individuals have consented.



WHAT DOES THIS MEAN FOR ME?

With all these changes, you need to make sure that you are giving your customers a fully informed and genuine choice over whether to share their data with you.

- A must - Take away all pre-ticked boxes.
- Use terminology that ALL people can understand without having to have a degree.
- Make it easy for people to withdraw their data.
- Keep your consent box away from the other terms and conditions. Keep a record of when and how you gain consent from individuals, specific examples of legitimate interest but, for now, here are a few reasons you might store data;

OPPORTUNITY:
This is all rather complicated and your customers may be overwhelmed by the whole thing. You can use this to position yourself as an expert and offer them a valuable service.

THE RIGHT TO OBJECT

As we mentioned before, part of giving true consent involves being able to withdraw your consent later. So, if a customer contacts you to say that they no longer want to share their data with you, you need to respect that choice and act on it right away, no questions asked..

If you're storing personal data...

- **for direct mail purposes**, you must stop as soon as you receive an objection – there are no exemptions or grounds to refuse.
- **for a legitimate interest**, you must stop unless you can demonstrate your legitimate grounds for processing their data, or you are processing their data for the performance of a legal task.

Communication is key. Customers **MUST** be made aware that they can refuse at "**the first point of communication**" and it should be stated in your privacy statement (see here for some fantastic examples of privacy statements **https://ico.org.uk/media/for-organisations/documents/1625136/good-and-bad-examples-of-privacy-notices.pdf**). Plus, a business cannot do anything to obstruct this right – they must be willing to deal with an objection at any time and cannot charge the customer for the privilege.

WHAT DOES THIS MEAN FOR ME?

In order to comply with the new regulations, you have to be open with your clients from the beginning.

- Clearly assert within your privacy statement that customers have the right to object.
- Confirm that customers have this right within your first communication with them.
- If someone exercises their right to object, cease to process their data immediately.

THE RIGHT TO ERASURE

It makes sense that, after a customer requests that you stop using their data, you must also respect their right to erasure.

Erasure refers to "the deletion or removal of personal data where there is no compelling reason for its continued processing." There are, however, other reasons why you might need to delete a customer's data from your system...

THE RIGHT TO BE INFORMED

- When processing their data is no longer necessary for the original purpose.
- When data has been unlawfully processed.
- When you must comply with a legal obligation to delete their data.
- When there is no overriding legitimate interest to continue processing their data.
- If you provide an online service for children under 16 who cannot give consent for themselves due to their age.

WHAT DOES THIS MEAN FOR ME?

If someone's data needs to be deleted, you need to be ready. Now's the time to assess what protocols you have in place and make sure that they're up to the job.

- Tidy up your data and make sure nobody is stored more than once.
- Review your data's security – who has access? Is the password encrypted?
- Set up a protocol, if you haven't one already, on how to delete a person's data.

THE RIGHT TO RECTIFICATION

For those customers who don't want you to delete their data, it's only fair that they can, at least, make sure you have the correct information. That's why GDPR gives consumers the right to rectification. That is, the right to correct their personal data if it is inaccurate or incomplete.

WHAT DOES THIS MEAN FOR ME?

You and your database must be ready to respond to any requests you receive about correcting personal data.

- Tidy up your database so that it's easier to find and correct things.
- When a request is made, update your own system immediately.
- Notify any third parties with whom you have shared the information.

DOCUMENTATION

GDPR doesn't just give guidelines on how to gather data, it also requires businesses to keep internal records of all their data processing activities.

If your company employs more than 250 employees, you must maintain an internal record of all data processing activities. For companies employing fewer than 250 employees, however, you need only record activities relating to high risk processing, such as;

- Processing that could lead to a risk to an individual's rights and freedoms. For example, if you record someone's ethnicity, you could be putting them at risk of unlawful discrimination.
- Processing special categories of data (e.g. genetic data, see here for a full list of special categories **https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/**) or data relating to criminal convictions and offences.

WHAT DOES THIS MEAN FOR ME?

Now, when it comes to making a record, you can't just write anything down. Like everything in GDPR, there is a defined structure to adhere to. You need to include...

- Name and details of your organisation (and, where applicable, of other controllers, your representative and data protection officer).
- Purposes of collecting, using, and storing data.
- Description of who you've obtained data from and why. Who you share your data with.
- Retention schedules (i.e. how long the data will be stored for and how it will be deleted if needs be).
- Description of your security measures.

WAYS TO MARKET AND THINGS TO REMEMBER

Now that you understand more about GDPR, here are a few things to remember and ways to market yourself.

Remember no matter how you market complying with GDPR is a MUST.

DIRECT MAIL

INCREASING DEMAND

While email marketing has become more restricted, direct mail remains a viable marketing option.

As it becomes more difficult for marketers to make effective use of online marketing channels, we predict that many will turn to direct marketing as a solution.

Under GDPR, companies can still contact people via post, as long as they can create a reasonable argument for legitimate interest. An example could be if people have purchased you in the past or visited your past event and expressed an interest in their services before. So, we expect to see a significant increase in sales for flyers and leaflets when GDPR becomes effective.

CURRENT EMAIL DATABASES

So, it's clear that you **MUST** gain consent moving forward, but what's to be done about your current email marketing list?

Being able to contact customers after a purchase is a fantastic way for you to check in and make sure they were satisfied with their order. It also allows you to quickly promote more products they might be interested in. Unfortunately, this will no longer be possible if the customer hasn't actively expressed an interest in your business, once GDPR comes into play any contacts on your email database that you have not obtained a **DOUBLE** opt-in from you can no longer email.

WHAT HAPPENS IF I DO HAVE CONSENT FROM MY CUSTOMERS?

Good news! If you've been proactive enough to have a thorough consent protocol in place, there's no reason for you to stop using that data. As long as you can prove that you have your customers' recent consent to email them, you can carry on emailing them.

WHAT HAPPENS IF I DON'T HAVE CONSENT FROM MY CUSTOMERS?

If you don't have a system in place to gain explicit consent from your customers, act now as once GDPR comes into play you must stop emailing them. Acting now is the only way for you to carry on communicating through email, it also has several other benefits;

- Your customer relations will improve as customers see you as a trustworthy company.
- You can deliver more relevant, targeted emails to people you know are actually interested.
- You should see higher click-through and open rates thanks to your refined marketing list.

It would be a smart idea to try and get this in place sooner rather than later to avoid a mad rush in May. While you still have people's contact details, why not send out a re-engagement email or an email specifically asking people if they'd like to opt-in or not? If they do opt in, you can keep their details in your database even after GDPR comes in.

TELEMARKETING

THE KEY THINGS TO REMEMBER ARE...

- Telemarketing lists need to be checked against your own unsubscribe list and the Telephone Preference Service (TPS) – or the Corporate Telephone Preference Service (CTPS) if you deal with businesses.
- Customers **MUST** be given the chance to opt out. This simply means asking them at the beginning and end of the phone call if they are happy to have this conversation and to receive further contact.
- Proof of consent must be saved which means you should record phone calls. These recordings then need to be stored as securely as all other personal data because of the content from the rest of the call.
- If phone calls can't be recorded, it needs to be clear that every effort possible has been made. The date and time of every conversation should be documented, along with their name and whether they consented to be called back.

Unit 2 Thurrock Trade Park, Oliver Road, Grays, Essex RM20 3ED