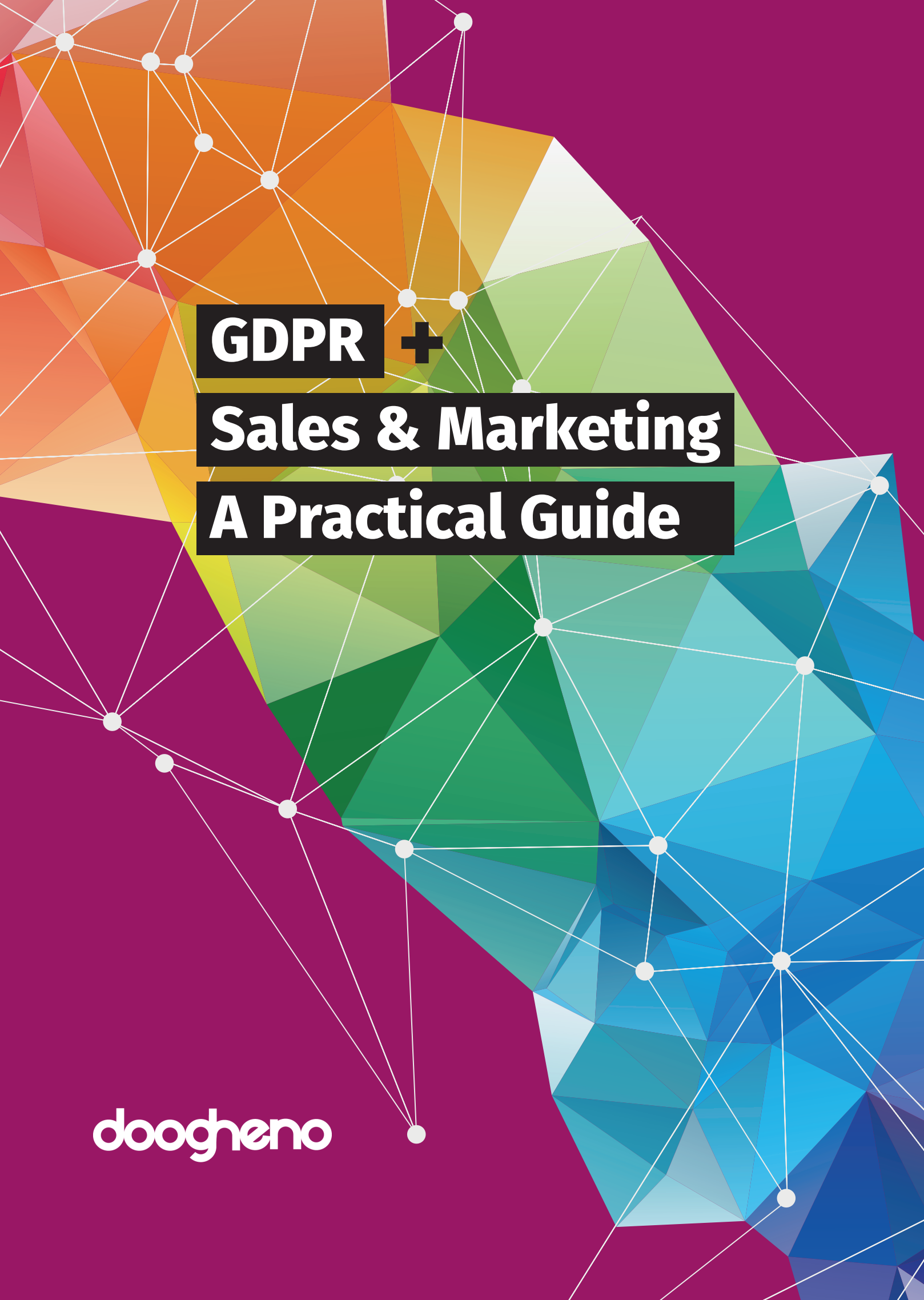

GDPR +
Sales & Marketing
A Practical Guide
doogheno

General Data Protection Regulation (GDPR) comes into effect on the 25th of May, 2018.

Your company should already be a long way down the line with its preparation. This paper is not intended for Data Controllers within an organisation or to advise you on how to ensure you are ready across your company for GDPR, it is intended as a reference source for the people handling data subject information within your sales and marketing departments.

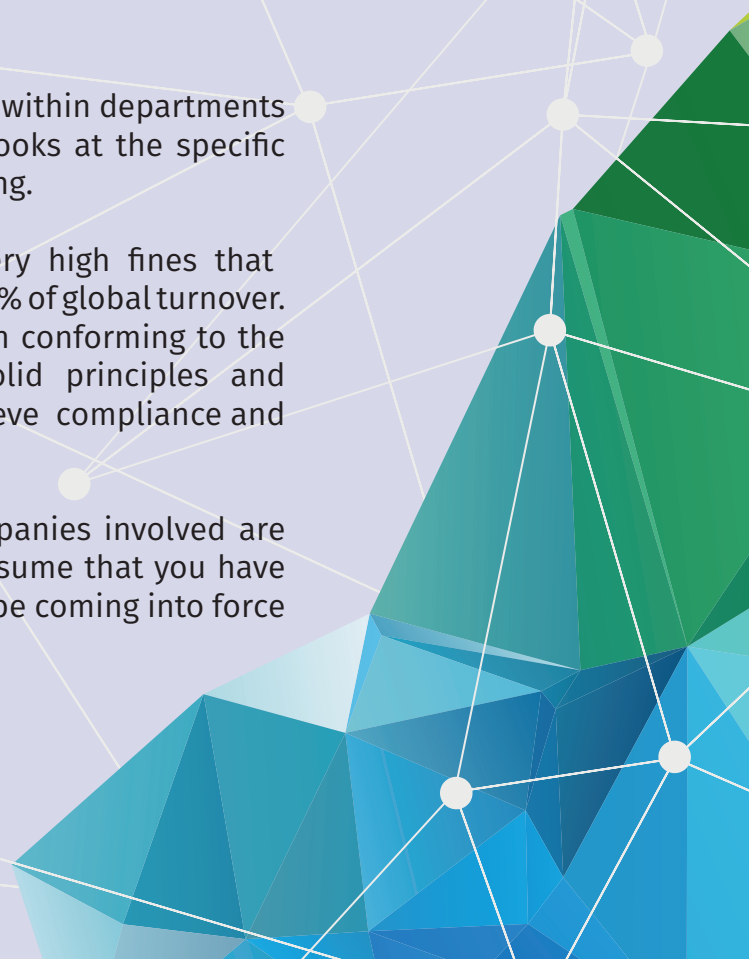
The introduction of GDPR will impact every area of business, sales and marketing in particular, as it brings with it a requirement for a new level of responsibility.

In preparing for compliance, companies have tended to focus on how they hold and store current data. They have not given much thought to the impact of GDPR on day to day operations.

New data collection and the use and storage of data within departments have tended to be overlooked. This short paper looks at the specific practical implications of GDPR on sales and marketing.

Every Information source on GDPR details the very high fines that accompany the new regulations, up to €20 million or 4% of global turnover. This alone should be enough to focus your mind on conforming to the regulations, and we believe that if you follow solid principles and best practice, your business will be able to achieve compliance and avoid incurring fines.

Throughout this paper, it is assumed that the companies involved are working in the B2B space within the UK. We also assume that you have already had a look at the GDPR regulations that will be coming into force in May.



What is your risk?

It is unlikely that your company will be picked for an audit, so for sales and marketing, the highest risks within your control are data breach, or being reported by an unhappy contact. Your Data Controller should inform you of what to do in the event of a data breach, and you should familiarise yourself with the process of immediately reporting a breach to them. Being prepared and efficiently handling requests from contacts, to opt out of future communications for example, will minimise risk. But this is not an excuse to be complacent, one complaint could be very disruptive to your business and lead to a damaging fine.

GDPR might feel frustrating but it is for the benefit of us all as it protects how our personal data is being held and used. It is good practice to treat every contact with the same security and diligence with which we'd expect our credit card company to treat our own personal data.

The Basics

The General Data Protections Regulation (GDPR) is a ruling intended to protect the data of citizens within the European Union. The GDPR is a move by The Council of the European Union, European Parliament, and European Commission to provide citizens with a greater level of control over their personal data. This applies to the UK and will not be affected by Brexit.

The basic principles are:

Lawfulness, fairness and transparency	Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject
Purpose limitation	Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
Data minimisation	Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
Accuracy	Personal data shall be accurate and, where necessary, kept up to date
Storage limitation	Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed
Integrity and confidentiality	Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures
Accountability	The controller shall be responsible for, and be able to demonstrate compliance with the GDPR

If you are new to GDPR we recommend that you read the Information Commissioners Office Guide ***https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/***

As we are looking at the specifics of job functions we are only working with the main points that you should be aware of. This guide is intended to enhance your knowledge and allow you to apply it to your job role.

Legitimate Interest

"...the processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest."

In most instances, Legitimate Interest will be used as legal grounds for marketing activity. But this does not give marketers carte blanche to continue the practices they have used previously.

GDPR requires the sending party to justify that a communication is in the legitimate interest of, and does not risk the privacy of, the individual concerned.

The following of a three-step process, a Legitimate Interest Assessment, is required. This assessment should be recorded and attached to the record in the CRM in case it is required at a later date.

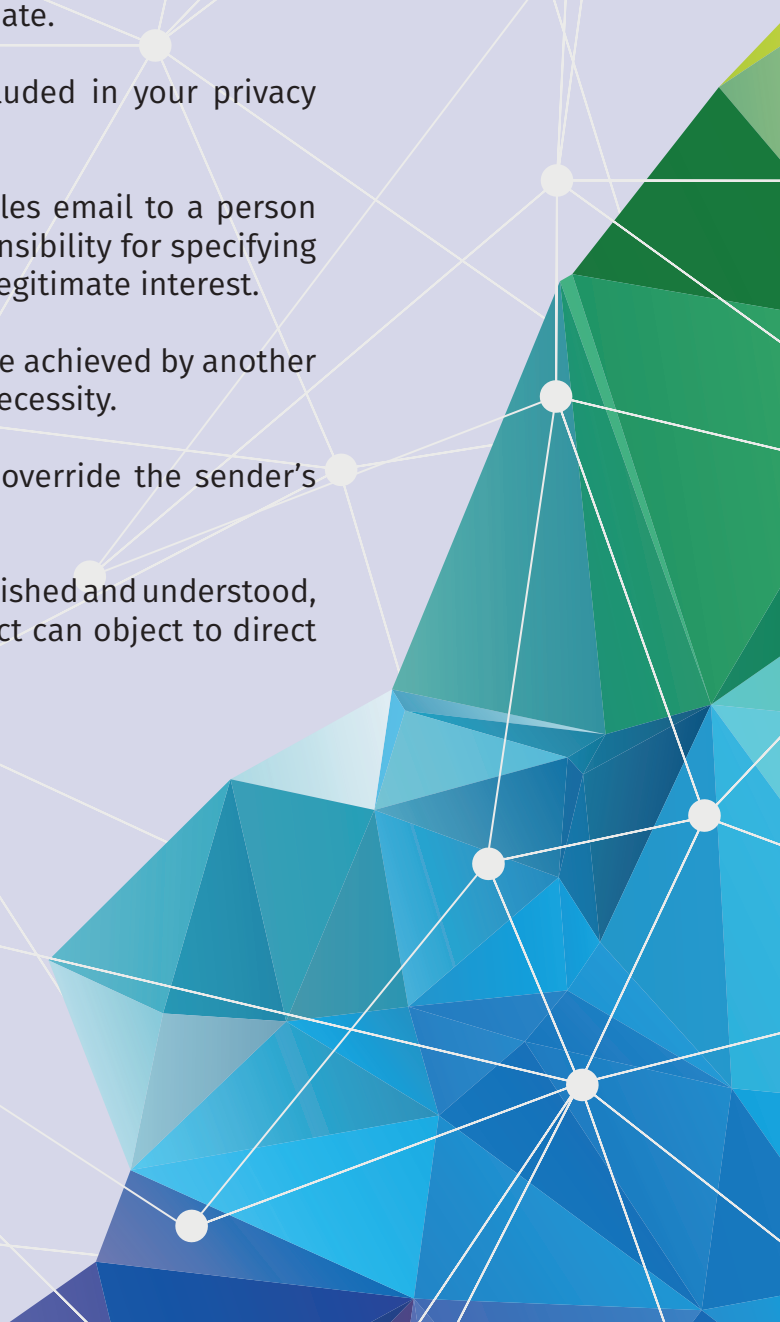
Details of your legitimate interests must be included in your privacy notice.

1. Identify a legitimate interest. Sending a sales email to a person within a company who has decision-making responsibility for specifying and purchasing services that you sell would be a legitimate interest.

2. Is it necessary? Could this communication be achieved by another means? The business objective could determine necessity.

3. Strike a balance. Do the recipient's rights override the sender's interests in sending the email?

Legitimate interest is already reasonably well established and understood, as it is the basis for unsubscribe links. Any contact can object to direct marketing and this principle still remains.



Data Profiling

Profiling is defined by more than just the collection of personal data; it is the use of that data to evaluate certain characteristics related to a contact. The purpose of profiling is to predict a contact's behaviour and make decisions based on that information. In the context of email marketing, it could relate to the choice of who to send a particular campaign to.

This might be based on the previous activity of that contact, or data subject. This could be based, for example, on their interaction with content as a part of an inbound campaign.

Profiling can be defined by three specific elements:

- It implies an automated form of processing;
- It is carried out on a contact's personal data
- The purpose of the profiling is to evaluate certain characteristics of a contact to predict their behaviour and take decisions regarding it.

Data profiling is permitted under GDPR but there are some requirements you need in order to safeguard the data profiling subject's rights.

The rights of profiling data subjects are:

- To be forgotten; to be informed; to have data deleted; and to have a copy of all the personal data you hold on request (within a month, free of charge)
- The right to data portability – for example enabling them to move to another provider supplied electronically in a commonly used format;
- The right to object;
- The right to halt; and
- Rights in relation to automated decision making and profiling.

Data Processing

Handling contact data for any reason within your company is classed as data processing. For example creating an email list is data processing. To comply with GDPR, data should be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing. A contact has the right to stop you processing their data.

By processing data you have legal responsibility as you are working for the data controller and handling personal details of your contact, the data subject.

You will not be held liable for data protection compliance, that falls on the data controller, but you must be aware of your role. Firstly you need to be authorised by your data controller to process the data and if you pass this work out to your colleagues, you need to inform your data controller and they too need written authorisation. You must carry out the processing in accordance to the data controllers instructions. You must maintain records of the data processed, take appropriate security measures and inform your data controller of any breaches.

Marketing

All marketers should be aware of GDPR, its importance, and its impact on their day to day actions. They also need to continue to comply with the Privacy and Electronic Communications Regulations 2003 (PECR). GDPR covers the use of personal data, PECR dictates how you can undertake certain types of marketing – specifically, electronic marketing messages such as email.

We assume throughout this guide that contacts are B2B and therefore Corporate Subscribers, a term which includes limited companies, limited liability partnerships, Scottish partnerships and some government bodies.

If a contact is a sole trader or in another type of partnership, they are considered an Individual Subscriber and need to be treated as such when it comes to communication. You will not be able to cold email these contacts under Legitimate Interest, but you can contact them if they have previously opted in, or if your proposed communication is relevant to an existing service they have with you.

Marketing and customer acquisition under GDPR will be harder. It will require more thought, more work, a change of emphasis within the marketing mix and in some instances a new approach.

Before we look at the details of GDPR preparation and compliance for marketers, we must consider tools such as marketing automation platforms and CRM. It is the marketer's responsibility to ensure that these tools are ready for GDPR.

The marketer should understand how a technology provider proposes to process and store a contact's data, in order to ensure that it is in line with GDPR compliance.

Understand the process whereby the provider reacts, responds to and resolves a data breach in compliance with the 'Data breach notification' legislation.

Understand the process of enabling data downloading and data deletion if requested by a contact.

Email Marketing

More on cold and opt-in emails

The fundamental principle of GDPR is to protect an individual contact's data. And there is a distinction between an individual and a business. The GDPR regulations leave it up to the individual countries within the EU to decide whether cold B2B email ('unsolicited commercial communications') should be opt-in or opt-out. So while GDPR is a pan-EU coverage, in the UK, PECR applies – The Privacy and Electronic Communications (EC Directive) Regulations 2003.

The UK Information Commissioner states:

You can email or text any corporate body (a company, Scottish partnership, limited liability partnership or government body).

However, it is good practice – and good business sense – to keep a 'do not email' list of any businesses that object or opt out, and screen any new marketing lists against that.

You may also need to consider data protection implications if you are emailing employees at a corporate body who have personal corporate email addresses (eg firstname.lastname@org.co.uk).

This means you are able to cold email business contacts but you must still apply the principles of GDPR.

A guiding principle with GDPR is only collect and hold data that is going to be used. So if you are only going to be emailing then do not hold postal addresses and phone numbers.

Do not collect data that you do not have a clear plan to use.

In marketing emails you should inform your contact that their personal data is being processed. This can be added as a disclaimer at the end of an email informing the recipient that you will be processing their data, an explanation of why you are processing the data, and instructions on how they can change the data process or request removal of their data from the list.

This disclaimer can be simple such as 'Based on my research I chose to contact you as I believe that our services are relevant to you and that you could benefit from them. I have processed your name and email to enable me to send this email. If you want any change to information that I have used to contact you please reply and let me know. If you want to be removed from my list please use the unsubscribe link.'

Cold Email

While you can still cold email businesses, you need to follow best practice. The consequences of not doing so are no longer just a terse email requesting you to stop, your actions could lead to a very large fine.

You need to ensure that you are sending relevant information to a contact that would genuinely benefit from knowing more about your company and you need to consider Legitimate Interest as well as complying to GDPR when handling their data.

You can no longer send out a generic email to a base and hope that someone replies. You must be highly targeted and disciplined and your research needs to be excellent.

If you are building cold lists you need to consider how long you hold that data. If the prospective contact has not responded or interacted with the communication it is reasonable to assume that they are not interested in the service. As such your company will have no reason to process that data and therefore you need to delete that data from your records. A thirty-day rule of thumb can be applied.

Your contacts data should be obtained in a legal and transparent way, you should be able to explain to the recipient where you got the data from and why you chose to process their data to enable the email to be sent. This should be detailed in the sent email.

Make sure you provide a mechanism for opting out of any further communication and the ability for them to change their personal data.

Opt-in Emails

To avoid risks of complaints arising from cold email you should build an opt-in list. This opt-in list needs to explicitly state what data you will be processing and what communications you will be sending. You cannot just add a person to the mailing list because you have an email enquiry from them, and you cannot send marketing messages to someone who signed up only to receive a monthly newsletter.

You can only process the data in the specified ways the data owner has agreed to, only for as long as they grant you their consent, and only until they express their wish to withdraw it.

Do not assume contacts on your database have opted in unless you can prove it.

When you collect contacts for your opt-in list any kind of data you ask for should be justified by the purpose for which you want to process it.

> Don't ask for a postal address if you want to send someone an e-book. If you wish to collect a phone number, state that it is because you will want to phone them.

Make sure your Terms and Conditions and Privacy Policy are updated. These need to be clear. Check with a sample of people to ensure that they are easy to understand.

And as with all data remember you do not own it, it belongs to the contact. You are not free to use it as you choose and you cannot transfer it to third parties.

Double optin is not a requirement under GDPR but it is good practice and therefore we recommend it.

Events

Opt-in consent requirements mean marketers will no longer be able to add event attendee lists automatically to campaigns.

You are required to show evidence for opt-in, such as an opt-in from your stand, or a follow-up email post-event before adding the contact.

Inbound

Content driven inbound marketing is an excellent way to attract new customers and to build your opt-in list.

On your landing pages, it is no longer good enough just to collect a prospect's contact details. You need to gain their specific consent to receive marketing information and for their data to be processed. This needs to be opt-in not a pre-ticked box. You should use a double opt-in which emails them after they complete the form, asking them to confirm opt-in.

You should link to your policy which will state why you are asking for the data, how you will use the data and give clear opt-in and opt-out rules.

If you use automation and email follow-up, remember that the contact may have only given consent to receive a specific piece of content so you cannot send them information on another subject just because they are on your database.

As with all data held you need to have a process for someone to be removed from the database, change any information that you may hold and receive a copy of the data that you hold on that contact.

Any data which was included under the current Data Protection Act is included and the EU has also further increased the scope so that IP addresses and online identifiers are included. The list includes:

- Name
- Address
- Phone number
- Email address
- Job title and place of work
- Cookies
- IP

Review your Cookie and IP opt-in – these have been established since the EU Cookie Law and include getting consent for cookie and IP tracking.

Sales

In many businesses, the line between sales and marketing is blurred, especially where there is no dedicated marketing resource. Salespeople are expected to spend a large part of their time prospecting for new business, and this prospecting is effectively marketing in its rawest form. It is direct contact from the salesperson to the potential prospect, usually in the form of a direct email or a cold call.

Salespeople are unlikely to overly concern themselves with GDPR compliance initially, but their actions do fall under the regulation and therefore they should be made aware of the potential consequences of their actions.

Cold Email

Cold email has been a mainstay of sales prospecting for 20 years. While salespeople will still be able to cold email under GDPR there are now more rules that they need to follow. The following guidance should ensure that your sales team remain on the right side of these rules.

All customer records should be kept centrally in a CRM, salespeople should not keep shadow copies in Excel with silos of uncontrolled and unencrypted data across the company.

The records should only contain fields for data that are in line with the information that is required to carry out the sales process. If there are existing contacts held within the CRM you must be able to identify and prove which contacts have opted in to receive contact about additional services and products. If contacts cannot be proved to have opted in they need to be treated with caution. Some companies, including pub chain Weatherspoon's, have opted to completely delete such data, in their case over 600,000 contacts were removed.

Often salespeople bring contact lists from previous roles and this practice has even been actively encouraged by new employers. Sharing databases of customer and prospect data, whether legitimately obtained or not, is strictly prohibited.

Using bought in lists, unless they can be shown to have opt-ins is also now prohibited.

But this does not mean the end of cold email. It just means that the spray and pray approach that is so often used by salespeople has to stop.

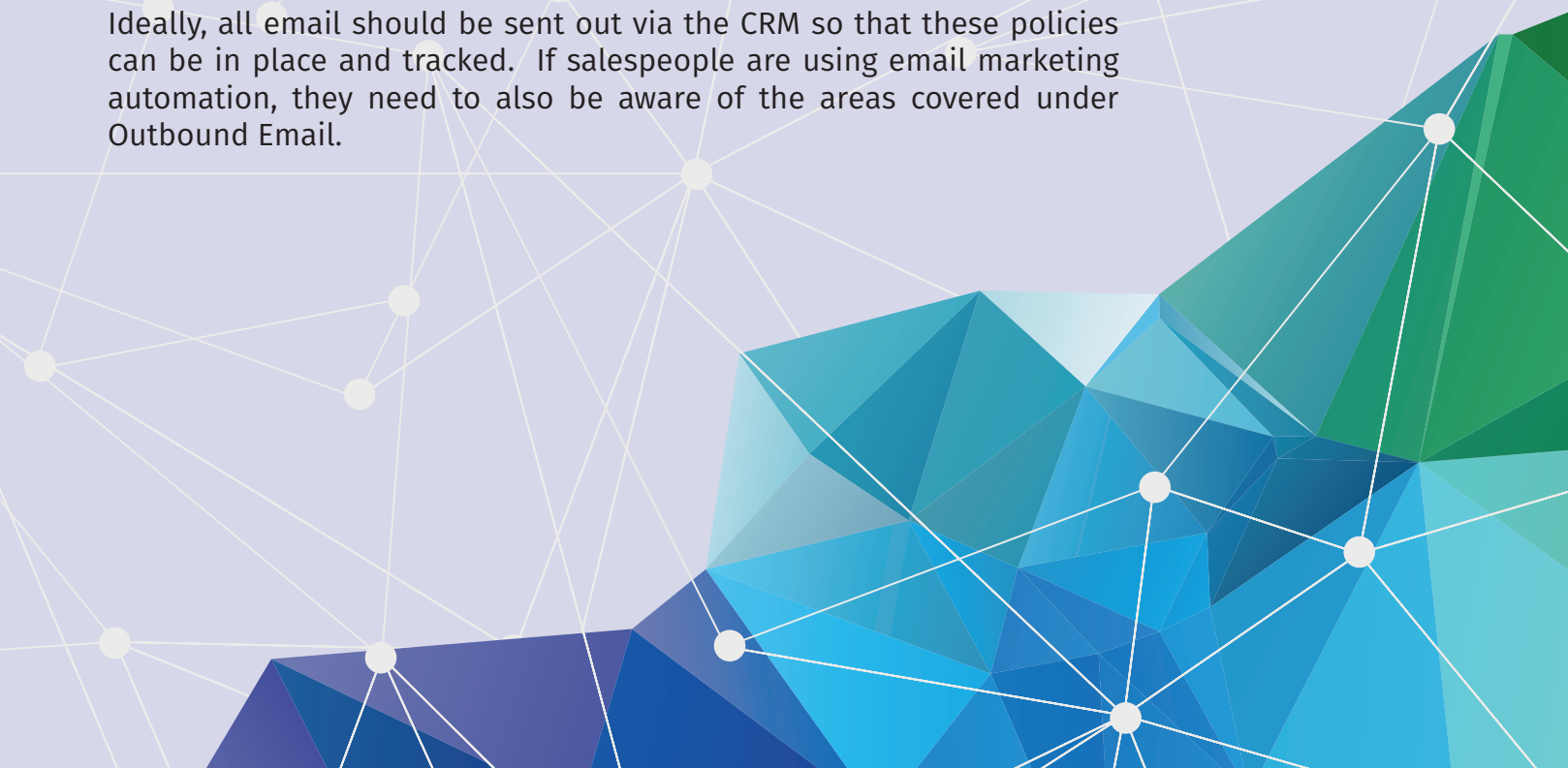
Cold email now has to be highly targeted. This will enable it to be used under GDPR and should also result in a higher response rate and a higher close rate. This approach requires extra work.

The initial stage of this extra work, is to prove Legitimate Interest. Can you prove that your services are relevant to a specific contact within a specific company? If you sell financial modelling software for manufacturing companies, then it would be reasonable to say that the Financial Director within a manufacturing firm would have a legitimate interest in your product. However, this could not be said of the Operations Director of the same company.

You need to carry out a Legitimate Interest Assessment (LIA) and this should be held in your CRM so it can be accessed if needed by the data controller. In this test you 1. Identify a Legitimate Interest, 2 Carry out a Necessity Test and 3 Carry out a Balancing Test. ***(For a detailed breakdown see the Data Protection Networks guide https://www.dpnetwork.org.uk/wp-content/uploads/2017/09/DPN-Guidance-A4-Publication.pdf)***

Make sure salespeople state why the contact has been sent the email. And make sure the recipient has the right to be forgotten and the right to assist in data deletion. This can be via an unsubscribe option or a simple statement saying that the contact can request to opt out and/or be deleted completely. Then ensure this happens before any additional communication is sent.

Ideally, all email should be sent out via the CRM so that these policies can be in place and tracked. If salespeople are using email marketing automation, they need to also be aware of the areas covered under Outbound Email.



Cold Calls

Unlike with email, there is no distinction between an individual subscriber and a corporate subscriber when it comes to cold calling, the rules apply to everyone.

If cold calls are automated, then you will have to both have and prove prior opt-in from contacts.

If you are making live calls, you will either need consent or numbers will need to be checked against the Telephone Preference Service (TPS) or the Corporate Telephone Preference Service (CTPS) and your own records in case they have previously requested to be removed or not to be called. If the numbers are not registered with TPS or CTPS, and there is no do-not-call request, then you may make the call to the contact.

As with all personal data, you will need to process this in line with GDPR. Like cold email, you will need to prove a legitimate interest.

Events

The collecting of business cards and contacts at events needs to be considered under GDPR. Someone passing you their business card does not automatically constitute consent to be put on a mailing list or receive cold email. You must ask for specific documented consent.

Recommendations

All direct marketing should now be highly targeted. This has always been best practice for marketing, but now it is a requirement. This is going to put an additional burden on marketing and sales teams. The marketing mix should be reviewed as cold outreach will no longer be an easy way to prospect for new customers and existing customers will not be as easy to upsell to.

Increase your focus on digital marketing through better on site and off site SEO, PPC and inbound marketing.

Utilise social media to the full.

Ramp up content driven inbound marketing.

Outsource email campaigns to a company who will manage delivery and compliance.

Automate LinkedIn for sales prospecting.

If you require assistance in these areas contact ***hey@doogheno.com***. Our team will answer your questions, give you guidance and explore how we can help you further.

About This Guide

This guide was written after extensive research of over 50 articles and courses and where practical, has third party legal clarification. While we believe the information that we have provided in this document to be correct at time of publication further clarification is being provided by the ICO weekly. You should carry out your own research and where appropriate obtain your own legal clarification of the GDPR regulations, ultimately it is your company that can be fined if you are non-compliant. This guide should be used to augment your existing GDPR readiness activities. It is important that your organisation take GDPR seriously and fully explore how it will impact all areas of your business.

About Doogheno

Doogheno growth marketing combines digital marketing best practice, content driven inbound marketing to inform and shape the conversation across all platforms, growth hacking to increase your close rate and solid sales principles updated for the way your customers buy today.

Doogheno has experience across the board of working with technology companies and aims to bridge the gap between sales and marketing so that you win more business and keep more customers. Many of our team have carried their own sales targets so know the value of great creative marketing. Doogheno isn't just about making things look good, it's about filling the sales funnel and driving sales through to a close. We are passionate about growing your business so we don't mince words, we don't bluff and guess, we work with you to achieve your strategic business goal.

Speak to us today about GDPR compliant marketing.

Hey@doogheno.com 020 7097 8567
24 Holborn Viaduct London EC1A 2BN

www.doogheno.com