b2bmarketing.net

Getting to grips with the GDPR: A B2B marketer's guide

B2B Marketing

Insight · Development · Training · Events



Contents

Introduction 4

Section 1 5

The basics of the GDPR

1.1 What is it? 5
1.2 When does it come into force? 5
1.3 What does this mean? 6
1.4 What is 'personal data'? 7
1.5 The six principles of the GDPR 8
1.6 What are the potential implications of failing to comply? 9
1.7 Brexit and beyond 10
1.8 The benefits and opportunities of the GDPR 11

Section 2 14

Legal grounds

2.1 The six legal grounds 14
2.2 Direct marketing as a legitimate interest 14

Section 3 15

Consent

3.1 What does consent mean under the GDPR? 15
3.2 Oral consent 17
3.3 The duration of consent 17
3.4 Proving consent 17
3.5 What does this mean in practice 18
3.6 How to gain consent 22

Section 4 27

Individual rights

4.1 What rights do individuals have? 27
4.2 The right to be informed 27
4.3 The right of access 29
4.4 The right to rectification 29
4.5 The right to erasure 29
4.6 The right to restrict processing 30
4.7 The right to data portability 30
4.8 The right to object 30
4.9 Automated individual decision-taking, including profiling, rights 31

Getting to grips with the GDPR © **B2B Marketing 2017**

Contents

Section 5 33

Security and data breaches 33

Section 6 35

Penalties and enforcement 35

Section 7 36

Data protection officers 36

Section 8 37

SMEs 37

Section 9 38

Useful resources 38

Section 10 39

Timeline 39

Section 11 40

GDPR glossary 40

Getting to grips with the GDPR © **B2B Marketing 2017**

Introduction

GDPR. Just four little letters that could spell a whole heap of trouble for marketers.

This new piece of EU data protection law – the General Data Protection Regulation – represents a huge shake up to the way businesses are required to collect, process and secure the personal data of the individuals they do business with. And this revolution will be here soon. It's all change on 25 May 2018, with no transition period – and the potential is business-crippling fines if your organisation is found to be non-compliant.

But even at 261-pages long, containing 99 articles, the official text of the GDPR still doesn't tell marketers, and even regulators, exactly what they'll need to do to be compliant the day after the law comes into force.

In this guide we've set out to provide an overview of the regulation, and its potential implications, condensing the key areas B2B marketers need to be aware of, distilling the advice that is out there, and providing some practical action to consider in preparation – with the caveat that even with fewer than 12 months to go until it is enacted there is still much interpretation and advice to be provided by regulators.

Indeed, it's likely that much around the GDPR will remain unclear until enforcement cases come before the regulator, or possibly before a judge in the courts. But this is no reason for inaction or delay, as organisations need to act now to be ready in time to meet the deadline.

This guide will help you understand:

- What the GDPR is and its six principles
- The obligations it imposes
- The potential implications of non-compliance
- The opportunities the GDPR presents for marketers
- Practical steps you can take to prepare
- Checklists of actions that need to be completed on the path to compliance
- Useful resources and checklists you can access
- A timeline with suggested milestones for action.

Please note: while we have tried to present a comprehensive overview of the key elements of the GDPR, this document is intended to provide a general guide to the subject. Those seeking legal advice should contact a specialist with regard to their specific circumstances.

Section 1
The basics of the GDPR

1.1 What is it?

The GDPR is European legislation designed to harmonise data protection law across the EU. The intention was not to make marketers' lives more difficult (although it may seem that way), but to improve the rights of consumers with regard to their personal data and how it's protected.

It imposes new regulations for organisations to protect consumers around data control, access and security, in addition to tougher enforcement for breaches of the rules. The EU hopes the regulation will clarify obligations, make them more consistent across Europe and improve trust among consumers in the way their data is handled. The EU claims simplified rules for businesses will save €2.3 billion a year.

The GDPR was adopted by the European Council in April 2016, and member states have two years to implement its provisions. In the UK, the GDPR will replace the Data Protection Act.



1.2 When does it come into force?

As it's a regulation, the GDPR will come into force across all EU member states on the same day – 25 May 2018. There will be no transition or 'grandfathering' period, so all businesses must be compliant with the new regime as soon as it comes into force on that date.

1.3 What does this mean?

All marketers are likely to be affected by the new rules, so will need to prepare. The biggest shake-up for marketers will be around how personal data can be used for marketing purposes, and how that data is stored and protected, and strengthening the rights of data subjects. Organisations will need to understand what's required of them, so they're ready to comply with the rules by the deadline in May 2018.

In the UK, the Information Commissioner's Office (ICO) will be responsible for its regulation and ensuring GDPR compliance. Elizabeth Denham, the information commissioner, has spoken of the need for organisations to change their ethos on data protection – to move away from a box-ticking mentality and build a "culture of privacy" within organisations – beyond compliance and toward a commitment to managing data sensitively and ethically.

The principles of the GDPR (see 1.5) are similar to those contained within the Data Protection Act, which the GDPR will replace. Compliance with the DPA will give you a firm foundation, but you'll still need to adapt your approach.

"There's a lot in the GDPR you'll recognise from the current law, but make no mistake, this one's a game-changer for everyone."

Elizabeth Denham, information commissioner

1.4 What is 'personal data'?

'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Article 4.1

In essence, the GDPR's definition of personal data covers any information that could relate to an identifiable, living being. In practice this could cover names, email addresses, phone numbers etc.

"It's certainly true that accountability cannot be bolted on: it needs to be a part of the company's overall systems approach to how it manages and processes personal data. But this shift in approach is what is needed. It is what consumers expect."

Elizabeth Denham, information commissioner

Getting to grips with the GDPR © **B2B Marketing 2017**

1.5 The six principles of the GDPR

The GDPR is underpinned by six principles (much like the DPA was by its own eight principles) set out in Article 5. In summary, these are that personal data should be:

1. Processed lawfully, fairly and in a transparent manner in relation to individuals.

2. Collected for specified, explicit and legitimate purposes and not processed beyond those.

3. Adequate, relevant and limited to what's necessary in relation to the purposes for which they are processed;

4. Accurate and, where necessary, kept up to date.

5. 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.

6. Processed in a manner that ensures appropriate security of the personal data.

In addition, the GDPR states the data controller (the person or organisation who determines how the data is processed) is responsible for, and needs to be able to demonstrate, compliance with all these principles.

This concept of accountability is a key precept of the GDPR. The information commissioner has said: "This is about more than legislative box-ticking… accountability is at the centre of all of this: of getting it right today, getting it right in May 2018, and getting it right beyond that." She wants companies to understand the risks they create for others when they use data, and to mitigate those. To build what she describes as "a culture of privacy that pervades the entire organistion".

1.6 What are the potential implications of failing to comply?

A major change introduced by the GDPR is the potential sanction if your organisation fails to comply with the law.

If an organisation breaches the GDPR, fines could reach €20 million or up to 4% of global annual turnover of the previous year, whichever is highest. While there are a number of factors the domestic regulator – in the UK, the ICO – will take into account, these fines justify their potential status as "company killers" as one lawyer dubbed them. The previous maximum fine under the DPA was £500,000.

Analysis carried out by information security consultancy NCC Group found if the GDPR rules had applied to the fines issued by the ICO against UK companies in 2016, the total sanction would have been £69 million, rather than £880,500.

And it's not only regulatory action organisations will need to worry about under the GDPR. The regulation introduced allows for consumers to claim compensation from data controllers or processors who infringe the regulation for the damage they have suffered.

› See Section 6: Enforcement and penalties

"GDPR isn't just about financial penalties, but this analysis is a reminder that there will be significant commercial impacts for organisations that fall foul of the regulations."

Roger Rawlinson, MD of NCC Group's assurance division

1.7 Brexit and beyond

What does all this matter when the UK is in the process of leaving the EU? A survey by Crown Records Management in April suggested almost a quarter of firms had given up preparing for the GDPR due to the UK's decision to quit the EU.

The GDPR will come into force before the date Britain will leave the EU. And even once it does, it's likely the regulation will remain in place for some time – if not forever – before it's replaced by new domestic legislation. The UK government has confirmed it will apply.

One suggestion is an adequacy agreement (such as the Privacy Shield which safeguards data moving between the US and EU) be put in place between the UK and EU once Britain does leave the EU. It's hoped there will be greater certainty around this before the UK departs.

"We will be members of the EU in 2018 and therefore it would be expected and quite normal for us to opt into the GDPR and then look later at how best we might be able to help British business with data protection while maintaining high levels of protection for members of the public."

Karen Bradley, secretary of state for culture, media and sport

1.8 The benefits and opportunities of the GDPR

Amid the scary warnings of huge fines, and fears you'll be unable to use much of your carefully collected data after 25 May next year, it's important to remember the GDPR does present a number of opportunities for B2B marketers.

- **Databases will be leaner, and email marketing more targeted.** Under the GDPR individuals will need to opt in to your marketing, and you'll need to be able to prove they have done so. This will probably mean the loss of much of your database, but if they're not engaging, how much will that matter? A list of individuals who have opted in to your communications should be much more engaged, resulting in higher click-through, open and engagement rates in your email campaigns.

- **Accountability could provide a competitive advantage.** The information commissioner has stated that those organisations that can prove they handle customer data sensitively and respect an individual's privacy will have a competitive advantage over those who are not.

- **It will raise the profile of marketing within the organisation.** If marketing steps up to the challenge presented by GDPR and takes the lead in developing the culture of privacy demanded by the information commissioner, it should highlight the importance of marketing among senior leaders and increase the credibility of the function.

"We believe there is a real opportunity for organisations to present themselves on the basis of how they respect the privacy of individuals and over time this can play more of a role in consumer choice."

Elizabeth Denham, information commissioner

Checklist

General steps: What to do now

- **Carry out an information audit.** Look at how your organisation collects and uses information. Where is data collected and stored? Who is able to access this data? What security measures do you currently have in place?
- **Raise awareness within your organisation.** Most employees will have some connection to personal data the organisation holds and processes. Ensure they understand changes are coming, and the potential impact this could have on the business – and the potential penalties. Make sure senior management is engaged in the process, and establish cross-functional teams to tackle the challenges.
- **Review your privacy policies and statements.** Look at what you currently tell users about how you use their data, and assess how far this goes to complying with the GDPR.
- **Assess your policies and procedures.** Do you have formal guidance in place on what to do if an individual wants to know what information you hold on them, or if you had a security breach? Understanding the current situation will give you a foundation to put in place the required documentation.
- **Get in touch with your technology providers.** Compliance with the GDPR may require changes and amendments to your systems, with regard to how data is stored or secured. Contact your suppliers to understand what steps they're taking to become GDPR-compliant and support they're offering their clients.
- **Find out whether you will need to appoint a data protection officer (DPO).** In certain circumstances, organisations will need to appoint a DPO (see section 7).
- **Look out for updated guidance.** The ICO and Article 29 Working Party will continue to produce advice and guidance on how to interpret and implement GDPR's many provisions, so keep an eye out for updates.
- **Be careful.** There are already rogue organisations offering spurious certifications for GDPR compliance officers or similarly unnecessary training. The huge scope and nature of the GDPR means you'll likely need some help to prepare, but look closely at what's being offered to ensure you're not ripped off.

Getting to grips with the GDPR © **B2B Marketing 2017**



How to raise internal awareness

Andy Grant, MD at Bowan Arrow and vice chair of the DMA's responsible marketing committee, offers the following tips on the best way to communicate the GDPR to an internal audience

In the workplace keep it simple, it's a regulation that needs attention, awareness and action. To communicate effectively, use simple language to highlight the important top-line GDPR items. Highlight who it affects and how within the business and nominate a single point of contact for all internal GDPR-related questions and actions.

1. **Staff training.** This requires a two-step approach. First, a basic GDPR overview and impact illustration for all employees, included as part of everyone's KPIs. Secondly, make comprehensive training available for all staff that handle business-related data. It's their responsibility to comply with the GPDR.

2. **Conduct a data audit and amnesty.** For many businesses, this is something that's been on the to-do list but never been a priority. Now it's time it became reality. By offering an internal amnesty, the business can understand the extent of data being held and, therefore, deal with it appropriately.

3. **Adopt a business-wide GDPR compliant data policy.** Take guidance from the DMA, attend webinars and read their blogs, articles and guides. Find policy templates to adopt into your business.

Section 2
Legal grounds

2.1 The six legal grounds

Under the GDPR there are six legal grounds through which you can process personal data, all of which are equally valid and will allow your organisation to meet the first principle of the GDPR – that data is processed lawfully.

These six are:

- The data subject has given consent (see section 3)
- It's necessary for the performance of a contract
- It's necessary for the controller to comply with a legal obligation
- It's necessary to protect the vital interest of the data subject or other natural person
- It's necessary to perform a task in the public interest
- It's necessary for the purposes of the legitimate interest pursued by the controller or third party except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data.

You'll need to make clear to data subjects which legal ground you're using for the basis of processing data and explain why in your privacy notice. The key action is to work out which of these legal grounds you intend to use to lawfully process data.

2.2 Direct marketing as a legitimate interest

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

The positive news? Direct marketing is specifically referred to as a legitimate interest in the GDPR. For a legitimate interest to exist, the GDPR says there should be a "relevant and appropriate" relationship between data controller and subject. And it should be assessed whether the individual would "reasonably" expect their data to be processed at the time and context in which the data is collected.

It also says the use of legitimate interest must be a balance between the company's interest and the rights of the individual. Would a customer expect a business to use their personal data to promote its products and services (providing they hadn't already opted out of messaging)? To what extent would this impinge on the fundamental rights of the customer, such as the right to privacy? In addition, depending on how compelling the message to the customer is, there'll be a difference between marketing an event they've attended previously, and an unsolicited product ad they've never heard of.

One interpretation of this legitimate interest is that it allows you to collect and use personal data for marketing purposes, as long as you've already got their consent. This means it doesn't leave you free to carry out direct marketing without consent. It's also unlikely that if you fail to gain consent from an individual, you'll be able to fall back on a claim of legitimate interest as a method of lawful processing.

This is an area likely to remain unclear until the ICO or Article 29 Working Party provide greater clarity.

Section 3
Consent

3.1 What does consent mean under the 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

A change in the way individuals allow companies to use their data is one of the fundamental differences between the GDPR and current data protection legislation – and one that's likely to affect marketers the most – in that the GDPR requires a much higher standard for consent.

The idea of opt-out consent is dead – "failure to opt-out is not consent," says the ICO. Under the GDPR you'll only be able to send marketing communications to customers if they've opted in to receive them (that's the clear affirmative act set out by the regulation). Not only this, but you'll have to be able to prove an individual has done so, placing the burden on the data controller or processor. Individuals also have the right to withdraw their consent at any time (see section 4).

If you pursue this consent legal ground, rather than the legitimate interest route, you'll need it no matter how you're contacting people; be it email, telephone, SMS or direct mail.

The ICO is yet to publish its formal guidance on consent following its consultation in March, but the consultation itself gives an idea of the regulator's intent. That consent is freely given, specific and informed and unambiguous are its key components.



Freely given

This means individuals have a genuine choice and control, and withholding or withdrawing consent will not be detrimental. It also means consent cannot be bundled up, for example having to consent to marketing messages as a condition of sale.

Specific and informed

According to the ICO, when seeking consent you must cover:

- The data controller's identity, as well as name any third parties who may rely on the consent to process the data.
- The purposes and activity of the processing. Why you want the data and what you'll do with it. As a minimum it should cover how exactly the data will be used. It's worth spelling out in your privacy policy exactly what marketing messages mean to your organisation (returning to the principle of consent being clear and unambiguous).
- The right to withdraw consent, and how an individual can do so.

Unambiguous

It must be clear that the individual has given their consent, and you're able to prove this. A tick box (but not one that is pre-ticked, as that's prohibited) is not the only way to achieve this. The ICO suggests alternatives you could use:

- Signing a consent statement
- Oral confirmation (see section 3.2)
- A binary choice presented with equal prominence (yes or no options, for example)
- Switching technical settings away from default
- Saying yes to a clear oral consent request.

Even if you use these options, you'll still need to be able prove that it was the specific individual that was actually giving you their consent (as opposed to someone just pretending to be them).

In preparation for GDPR a number of organisations have chosen to deploy a double opt-in process for consent. When the affirmative action has been submitted, the individual receives an email asking them to confirm they're the individual in question, and they're consenting.

Some organisations are going a step further, providing what amounts to a 'consent receipt' for the individual once they've provided the affirmative action and double opted-in. This specifies who they are, what they've signed up to, how their data will be processed, the date, how long the consent is valid and naming the data controller.

3.2 Oral consent

While the ICO highlighted oral statement as a valid unambiguous statement, how could you prove it? Take the example of meeting someone at a trade show, who tells you they'd like to receive emails from you and gives you their address.

It's unlikely you'll need a recording of the conversation, but the ICO recommends you do include a copy of the script used at the time with your records.

Another method is to have a structured process in place for staff to follow at events, for example. If a person is interested, you could ask the individual to sign a form which complies with the principles of freely given, specific and informed, and unambiguous consent.

3.3 The duration of consent

Neither the GDPR nor the ICO have said how long consent should last for, saying only that it will depend on context. The ICO does say it will degrade over time, implying it does not last forever.

You'll need to consider the scope of the original consent and expectations of the individual. The ICO's recommendation is to refresh consent every two years.

3.4 Proving consent

Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

Article 7.1

As mentioned, a key aspect of consent is how you will be able to prove you have it if required. According to the ICO, a good record will include:

- **Who consented**
- **When they consented:** a copy of a dated document, online timestamp, or a note of the oral conversation.
- **What they were told at the time:** a copy of the document or data capture form as well as the privacy policy (with the version number and date recorded).
- **How they consented:** a copy of the complete data capture form, with timestamp.
- **If consent has been withdrawn:** and if so, when.

This may mean you'll need to make changes to your record management or CRM systems to be able to capture this information.

3.5 What does this mean in practice?

The GDPR says: "The request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form using clear and plain language."

The ICO says this means keeping it separate from your wider terms and conditions, adopting a simple style, using clear, non-technical language, keeping the request concise and specific and avoiding vague or blanket wording.

In terms of ensuring individuals are informed, the specifics can be contained within your privacy policy. This will allow you to go into the level of detail required by the GDPR, which is greater than the DPA currently.

What needs to be included in your privacy policy

The ICO has published a comprehensive list of the information required to be in the privacy policy under the GDPR.



Information to be provided	Data obtained directly from the data subject	Data not obtained directly from the data subject
Identity and contact details of the data controller and, where applicable, the controller's representative and data protection officer	✓	✓
Purpose of the processing and lawful basis for the processing	✓	✓
The legitimate interests of the controller or third party, where applicable	✓	✓
Categories of personal data	X	✓
Any recipient or categories of recipients of the personal data	✓	✓
Details of transfers to third country and safeguards	✓	✓
Retention period, or criteria used to determine the retention period	✓	✓
The existence of each data subject's rights	✓	✓
The right to withdraw consent at any time, where relevant	✓	✓
The right to lodge a complaint with a supervisory authority	✓	✓
The source the personal data originates from, and whether it came from publicly accessible sources	X	✓
Whether the provision of personal data is part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data	✓	X
The existence of automated decision-making, including profiling and information about how decisions are made, the significance and the consequences	✓	✓

To summarise in layman's terms, this broadly means setting out:

- Who we are
- What we'll do with your data
- How we look after it
- Why we need it
- How long we need it for
- What your rights are.

Remember, you'll need to strike a balance in your privacy notice between it being both sufficiently comprehensive to inform the individual (with all the information included above), and sufficiently clear that the individual can understand it. When considering this, try to move away from the idea of the privacy notice as something intended to protect the company, and towards informing the individual about how their data will be processed.

Of course, this doesn't necessarily have to only be a written notice. *The Guardian* newspaper produced a short video to explain all the above (bit.ly/b2bguardiandata). Instant messaging service provider Slack has a clear, well-presented privacy policy that you could use for inspiration at slack.com/privacy-policy.

Preference centres

The ICO has suggested the implementation of preference centres or privacy dashboards to offer "ongoing choice and control" over consent to individuals. This is particularly important when it comes to withdrawing consent. Opting-out by reply is not sufficient, the ICO says where feasible withdrawal should be made possible by the same method as opting-in.

An example of a business presenting its credentials as a competitive advantage is email firm Dotmailer. It has set up a 'trust center' on its website to bring together all its information on how it processes and secures data, along with a list of its accreditations, links to contacts and its preference centre.

Preference centre best practice

As we've mentioned, the ICO is recommending the introduction of preference centres to make it as easy for individuals to opt out of your communication as it is to opt in. Ideally, your preference centre should cover three options – opt in, opt out and updating a data subject's data.

The intention of the preference centre should be to hand control of the data back to the individual, in line with the principles of the GDPR. You'll want to:

- Let the data subject understand what exactly they provided consent for (this should be a reminder from when they originally gave consent).
- Explain how their data will be used and processed (also in the privacy policy).
- Allow them to control and manage the frequency and volume of communication they receive.

The primary attribute of a great preference centre is simplicity. You'll want to offer plenty of options for the individuals, but this must be balanced by making it user-friendly. There's no point giving the user 50 different combinations of channel, format and frequency to choose from, as they'll end up overwhelmed and not in control. In pursuit of this user-friendly experience, don't be afraid to borrow from the B2C world for examples.

Remember, you should only be collecting the data you need for processing, so try to resist the calls to collect superfluous information that may be useful for segmentation or research but does not impact the data processing. Under the GDPR, individuals also need to understand how you intend to use their data. Make sure links to your privacy policy (where this should be explained) are clear and prominent.

Here are some other tips:

- **Give it a personality.** This should, of course, reflect your brand and tone of voice. Many brands take a light-hearted approach. It's unlikely your subscribers will feel guilty about clicking the unsubscribe link, so don't make it sound like a big deal.
- **Stick to the point.** The subscriber will have come to your preference centre to opt in or out of your messages. Don't bombard them with other information such as sales messages, promotions or customer surveys.
- **Show you care.** It's a fact, people will unsubscribe from your emails, there's no point getting too hung up about it. Having said that, it's worth trying to see if you can keep them engaged. Perhaps they just want to change their email address or change which emails they receive. Which leads us to…
- **Offer alternatives.** Control and choice are the key options. Give them the opportunity to choose the type of content (marketing, sales, promotions), channel (email, SMS, DM), format (HTML, plain text) and frequency (how often they should be contacted) of messages they want to receive.
- **Offer a resubscribe option.** If they just want a break from your emails, make sure they have the opportunity to opt back in to your communications.
- **Gather feedback.** It's good to learn why people are choosing to unsubscribe. A quick, multiple choice option should give you some feedback, which hopefully you can use to improve your CX.

There are two other key things to consider. First, make sure the preference centre is kept updated to provide the ongoing choice and control demanded. Second, make sure the preference centre is promoted. Individuals need to know where they can manage their options. Include a link in all your emails, and make the language you use simple. While we marketers understand what a preference centre is, would your customers?

3.6 How to gain consent

If you're going to email your existing database to ask for their provable consent, it'll need to be done before 25 May 2018. As once GDPR comes into force you won't have their consent to email them to ask for it.

Just emailing your existing audience is unlikely to be that effective on its own at driving people to opt in. A more effective way of getting your audience to opt in to your marketing communications is to offer the individual something to gain their consent – a piece of content such as a whitepaper or ebook, for example – to be added to a marketing database.

However, you (may not be entitled to) can't make the download contingent on the individual signing up to your marketing list – this could mean their consent would not be freely given, invalidating it for use.



Running a re-engagement campaign

If you can't prove you have the consent of those individuals on your email database, you face a race against time before 25 May 2018 to start building an opt-in database. You'll want to contact those in your current email database now to re-engage them and earn their permission to continue to contact them post-GDPR implementation.

In addition, under the GDPR consent has an expiration date so re-engagement will be a tactic you'll need to build into your schedule, or you'll suffer a huge amount of list churn and a constant battle to engage new subscribers as existing ones drop off your database.

In any re-engagement email, there are four key points to get across:

- **How you got their details.** Why is the individual receiving this email? Where did their data come from?
- **Why you're contacting them.** How long has it been since they engaged with one of your emails? Why are you trying to re-engage with them?
- **What you'll be sending them in the future.** What sort of messages – sales, promotions, marketing, events – have they signed up for?
- **How they can manage their consent.** This is where to point them to your preference centre so they can choose and control what they receive.

The subject line in a re-engagement campaign is even more crucial than usual. "We've missed you", "Come back" or "It's been a while…?" are commonly used to invite individuals to click.

You should try and make your re-engagement emails as human as possible. Inject them with personality – this is essentially a last chance to re-connect with the individual, so be bold in your approach, but be prepared to accept them saying no. It's always preferable for the email to come from a real person (or at least, appear as if it has), if only to make the re-engagement plea sound more credible.

Another common tactic to drive re-engagement is to offer something in return, such as discounts on products or services. But make sure these aren't a condition of offering consent, as this may not meet the test that consent has been freely given by the individual.

Try to stick to a single CTA. If they've not been engaging with you, you don't want to turn them off instantly with a lot of irrelevant information. Stick to driving them to consent or re-engage.

But remember – it's no good starting your re-engagement campaign until you have the systems and processes in place to record and collect the consent permissions. If you're re-engaging them as part of building a GDPR-compliant database, you'll need to ensure your preference centre is equipped to handle a double opt-in process.

Other re-engagement options

Rebuilding a database doesn't have to end with email. You could also consider the following as part of a re-engagement campaign.

- **Website pop-overs/overlays/lightboxes.** These can feel intrusive, but that's often why they're effective. It's finding the right balance that's key – the interruption needs to be useful. Keep the design simple, and make the call-to-action clear. Because of the need under GDPR to demonstrate consent is both specific and informed, there should be a link to your privacy policy if you're collecting data on a double opt-in basis using these tactics.

- **Thank you pages.** Once individuals have completed an action on your website, such as downloading a whitepaper, use the thank you page as an opportunity to gain their consent. You need to be careful not to overwhelm the individual with options, so again keep it simple and prioritise the call to action you want them to take.

- **Retargeting emails.** Use retargeting to focus on those not opening your emails, or the individuals who haven't yet given you the consent permissions that you need. Your marketing automation system should be able to do this

Ultimately, any re-engagement campaign will benefit from the more information you have about why individuals are not engaging with your emails. Are there too many? Are they too frequent? Are they irrelevant? Understanding this will leave you in a better place to work out which approach to take when trying to re-engage with subscribers.



Hold it!

Having read all this, there's still a possibility that some of the GDPR provisions around consent might not apply to B2B marketing after all. The GDPR itself makes no distinction between B2B and B2C marketing.

Currently, B2B marketing emails and texts are permitted to existing customers on a soft opt-in basis, under the Privacy and Electronic Communications Regulation (PECR). However, the EU is currently revising its ePrivacy directive (which informs PECR in the UK), into a new regulation called the (frustratingly similar) Regulation on Privacy and Electronic Communications.

A leaked version of the regulation brought it into line with the GDPR, only allowing direct marketing by email to those who had given their prior consent. But the latest draft, published in January 2017 and awaiting approval by the European Parliament and the Council of Ministers, maintains the soft opt-in approach for B2B. Pending approval, this new regulation should come into effect on the same day as the GDPR, 25 May 2018.

This leaves B2B marketers in a bit of a quandary. You could take a gamble, and bank on the B2B marketing exemption making its way through the EU's legislative sausage factory and coming out the other side in one piece. But if the worse happens, and it doesn't make it, you'll have very little time to get compliant.

In addition, adopting this 'wait and see' approach is hardly in line with the ICO's desire for organisations to develop a culture of privacy and putting customers first when it comes to their data.



Checklist

Consent: What to do now

- Review your current data and understand your current consent provisions. Could you prove you have consent from these individuals? If not, you won't be able to use this data post-GDPR. You'll need to build up a new database, but don't worry as there's still time.
- Revise both your privacy policy and data capture forms to bring them into line with the information required by the GDPR, so consent can be freely given, specific, informed and unambiguous. Would they pass the clear and plain language test?
- Examine your record management or CRM systems to ensure they can capture all the information required so you are able to prove consent if required. Speak to your tech providers to find out how they can assist with this.
- Establish a preference centre or privacy dashboard so you can meet the ICO's recommendation of offering "ongoing choice and control" to individuals around consent. Ensure it enables a double opt-in process.
- Start planning a strategy to build a new database of individuals with provable consent. This should be a combination of contacting your current database, and developing content that will make users want to opt in.
- Come up with a definition on how long consent should last for your organisation's marketing communications, and ensure your data management systems can handle this by providing reminders to refresh consent or removing data subjects when they lapse.
- Prepare your team for alternatives to mass marketing, such as email. The concern around GDPR's potential impact reflects the reliance we have come to place on email marketing. Now is the time to think of other potential channels to reach your audience, and to learn strategies so they can cope in a post-GDPR world.

Getting to grips with the GDPR © **B2B Marketing 2017**

Section 4
Individual rights



4.1 What rights do individuals have?

The GDPR introduces and strengthens a number of rights for individuals with regards to their data, some of which will impact the way marketing handles customer data. These are:

- 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
- Rights in relation to automated decision-making and profiling.

4.2 The right to be informed

As mentioned previously, this is the right that sets out information you should supply with regards to how you collect and use personal data. The ICO has provided a comprehensive list of this information necessary to meet this. This needs to be provided at the time data is obtained from the subject, or within one month for data not obtained directly from the subject.

Information to be provided	Data obtained directly from the data subject	Data not obtained directly from the data subject
Identity and contact details of the controller (and where applicable, the controller's representative) and the data protection officer	✓	✓
Purpose of the processing and the legal basis for the processing	✓	✓
The legitimate interests of the controller or third party, where applicable	✓	✓
Categories of personal data	✓	✓
Any recipient or categories of recipients of the personal data	✓	✓
Details of transfers to third country and safeguards	✓	✓
Retention period or criteria used to determine the retention period	✓	✓
The existence of each's data subject's rights	✓	✓
The right to withdraw consent at any time, where relevant	✓	✓
The right to lodge a complaint with a supervisory authority	✓	✓
The source the personal data originates from, and whether it came from publicly accessible sources	×	✓
Whether the provision of personal data is part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data	✓	✓
The existence of automated decision-making, including profiling and information about how decisions are made, the significance and the consequences.	✓	✓

Source: https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/individuals-rights/the-right-to-be-informed/

4.3 The right of access

Individuals will be able to request from organisations whether personal data is being processed by the data controller; the purpose of the processing; the categories of personal data; to whom the data has been disclosed and how long it will be stored.

Companies will be obliged to provide a copy of the data in question. Where previously under the DPA they could charge £10, this now has to be provided to subjects for free.

The information should be provided "without undue delay" and "at the latest" within one month of the request. This compares with the 40 days currently under the DPA.

There are a few restrictions on this, including where requests are "manifestly unfounded" or "excessive". For these, the organisation can either charge a fee in line with the administrative cost, or refuse to respond. If they refuse to respond, it must be explained to the individual why and they must be notified of their right to complain to the supervisory authority (the ICO) and to a judicial remedy within a month.

4.4 The right to rectification

If personal data is inaccurate or incomplete, individuals are entitled to have this changed within a month (this can be extended by a further two months when a request is considered complex).

4.5 The right to erasure

This is alternatively referred to as the "right to be forgotten". It allows individuals to have their data erased when:

- It's no longer necessary for the purpose it was processed.
- The individual withdraws their consent (or there's no other legal ground for processing).
- Data has been unlawfully processed.
- In compliance with a legal obligation.

Talk with your technology provider to learn what your database system is capable of – as some won't let you completely delete records without leaving some kind of electronic trace.



4.6 The right to restrict processing

This is an individual's right to suppression of their data (under the DPA this was known as 'blocking'). It applies when:

- An individual contests the accuracy of their data, and should be restricted until it has been verified.
- An individual objects to processing, and you're considering the request.
- An individual does not want data to be erased when processing has been unlawful and would prefer it to be restricted.
- The organisation no longer needs the data, but the individual requires the data to defend or exercise a legal claim.

You'll need to review whether or not your data management system will allow you to (temporarily) suppress users' personal data.

4.7 The right to data portability

This allows individuals to obtain their personal data, and then reuse it across different services. This only applies when an individual had provided personal data to a data controller, the processing is based on consent or for the performance of a contract, and the processing is carried out automatically.

Data controllers must provide the data in a structured, commonly used and machine readable form (the ICO suggests a CSV file as an open format), and for free, within one month.

4.8 The right to object

If you use the legitimate interest of direct marketing to process data, individuals have the right to object. The organisation will have to stop processing the data – there are no exemptions or grounds to refuse. The right to object must be clear in the company's privacy notice and at the time of the first communication with the individual.

4.9 Automated individual decision-making, including profiling, rights

The GDPR is set up to protect individuals against potentially harmful decisions being made with regard to data without human intervention. Individuals have the right not to be subject to a decision when it produces a legal effect (declining a credit card, for instance), and this is based on automated processing. Individuals must be able to obtain human intervention, be able to express their point of view and obtain an explanation of the decision and be able to challenge it.

When it comes to profiling, this is defined as automated processing intended to evaluate certain aspects of the individual to analyse or predict aspects, such as work performance, personal preferences or behaviour.

The ICO says you'll need to:

- Ensure processing is fair and transparent by providing meaningful information about the logic involved.
- Use appropriate mathematical or statistical procedures.
- Implement appropriate technical and organisational measures to minimise the risk of errors and correct inaccuracies.
- Secure personal data in a way proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects.

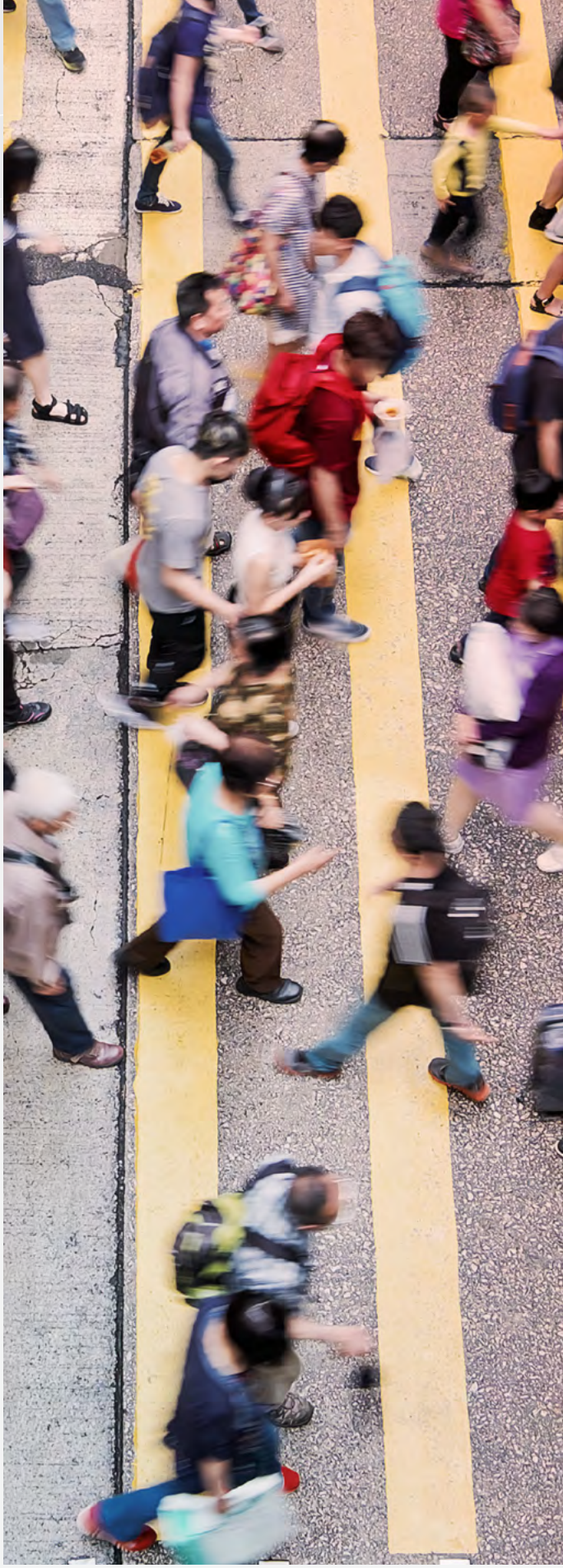
There will be further guidance from the Article 29 Working Party on profiling later this year.



Checklist

Individual rights: What to do now

- Make sure your privacy policies cover all the information necessary to ensure compliance with the right to information.
- Put practical policies and plans in place to respond to potential requests for the rights of access, erasure, rectification, restrict processing, data portability and to object.
- Assess whether your organisation carries out automated processing and/or profiling, and if this needs to be adapted to comply with the GDPR.



Section 5
Security and data breaches

You might think data security is the responsibility of the IT function – and according to one survey of CMOs in financial services the figure that do is as high as 96%. But the most common cause of cyber security breaches is human error, and due to the very short period that companies have to notify authorities of a data security breach under the GDPR, all employees need to be aware of what to do if the worst happens.

The GDPR introduces an obligation on organisations that should a breach of personal data take place – which could include the loss, alteration, unauthorised disclosure of or access to personal data – and there is a risk to the rights and freedoms of individuals, the data controller must notify the supervisory authority within 72 hours. If they don't, the fine could be up to €10 million or 2% of global turnover.

The notification to the authority should contain:

- The nature of the breach, the categories and number of individuals affected, as well as the categories and number of data records affected.
- The name and contact details of the data protection officer or contact for more information.
- The likely consequences of the breach.
- The measures taken to address the breach, and mitigate its potential impact.

The ICO expects businesses to have internal processes in place to facilitate decision-making about how and when to notify the authorities. Guidance on these is expected from the Article 29 Working Party this year.

The data subject also has to be made aware of the breach if it's "high risk" (high risk has not been defined by the GDPR or ICO). The notification should detail the nature of the breach, and what individuals can do to mitigate its potential impact. The mitigation factors need to be communicated to the individual "as soon as reasonably feasible", in cooperation with the supervisory authority and other potential authorities, such as law enforcement.

Checklist

Data breaches: What to do now

- Review security policies and procedures around storage of personal data in your organisation.
- Locate where personal data is being stored – is it in one place or on multiple legacy systems? Review access privileges and rights.
- Liaise with IT to identify potential security weaknesses around personal data. Understand how these can be plugged and secured.
- Speak to your technology provider(s). What security measures do they have in place, and are they sufficient to provide the protection required by the GDPR?
- Develop an organisation-wide incident response policy and procedures document.
- Make sure the incident response policy is tested regularly. It's no good to come up with a policy and then leave it to gather dust on a shelf. Train staff what to do in the event of a breach.



Section 6
Penalties and enforcement

We've already mentioned the potential crippling nature of the fines for failing to comply under the GDPR. A survey by law firm Irwin Mitchell found 17% of firms said the maximum fine of €20 million of 4% of annual turnover would force their company out of business.

Fines are not the only penalties regulators can impose. The GDPR also allows for warnings, reprimands or temporary suspensions of data processing. It's unlikely a maximum fine will apply in every case. The GDPR outlines the criteria that will be applied when the ICO is considering a sanction. These are:

- The nature, gravity and duration of the infringement
- Whether the infringement was intentional or negligent
- The data controller's steps to mitigate any potential damage
- How the regulator found out about the non-compliance
- Adherence to a particular code of conduct.

It would be dangerous to attempt to predict the approach of the ICO (or supervisory authority of any of the other member states for that matter) to enforcement once the GDPR comes into force.

Some experts believe the focus will be on large organisations early to get some big name victories under the belt. Others believe the focus will be on smaller businesses who won't have an army of lawyers to fight the numerous interpretations of the legislation.

The GDPR does allow the regulator to take a proactive approach to enforcement – ordering controllers or processors to provide information it requests, carrying out audits, reviewing certifications, and so on.

One thing that's certain is that regulators across Europe are likely to take an extremely dim view of those organisations who have made no effort to prepare to comply with GDPR. A number of marketers appear to be counting on the ICO letting first-time offenders off with a slap on the wrist once the legislation comes into force. This is a misguided approach, and not one to be recommended.

This is where the accountability concept will be key. You'll be in a far stronger position if hauled in front of the regulator if you can provide evidence of why you have come to the decisions you have come to in terms of attempting to comply, than if you show up empty-handed.

Much will also depend on the public awareness of the GDPR (which given how limited the business awareness is at the moment may take some time to take hold). The EU is promising an EU-wide campaign so citizens of members states are aware of their rights, and make a complaint to the regulator.

Section 7
Data protection officers



Some organisations will need to appoint a data protection officer under GDPR. These are:

- Public authorities
- If they carry out large-scale systematic monitoring of individuals, or
- If they carry out large-scale processing of 'special' categories of data (such as biometric data).

The DPO needs to:

- Report to the highest level of management in the organisation
- Operate independently (although, they can be an existing member of staff)
- Have adequate resources to enable them to meet GDPR obligations.

The DPO's role is to inform and advise the organisation about GDPR and data protection compliance, to monitor the organisations' efforts and to act as the point of contact for supervisory authorities and individuals. While they don't need professional qualifications, it's expected they will have some professional experience and knowledge of data protection law.

Section 8
SMEs

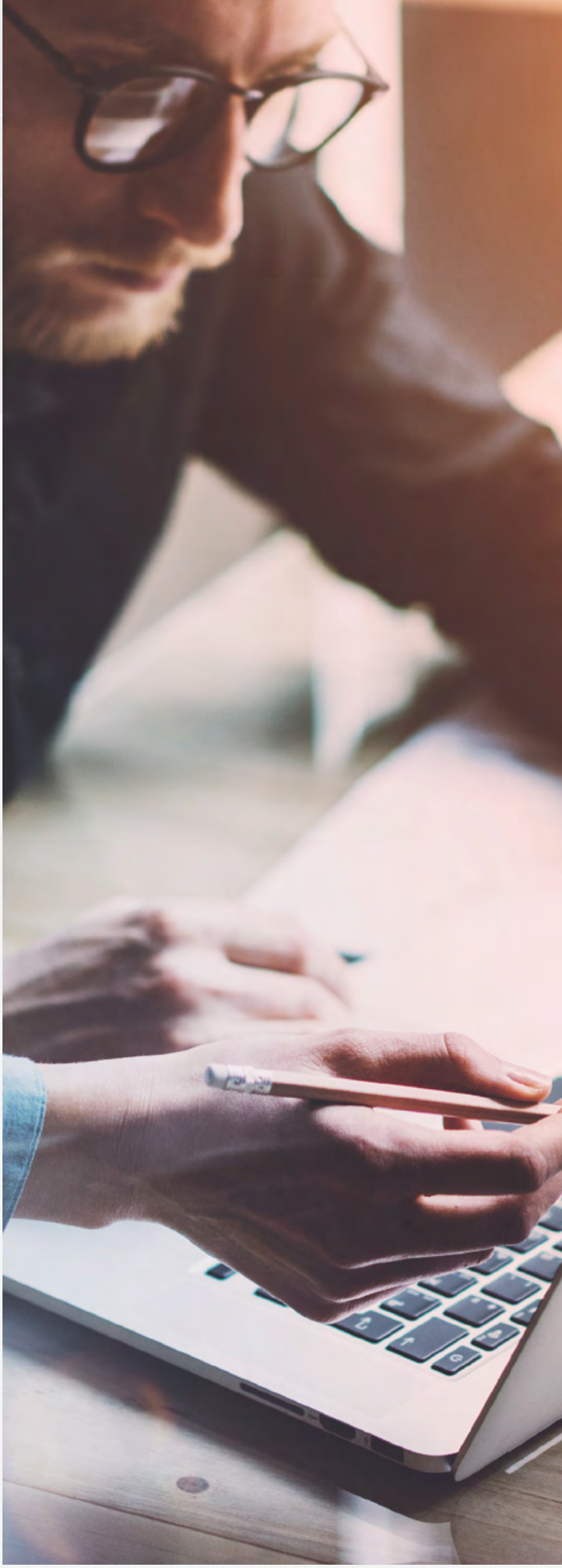
"When it comes to data protection, small businesses tend to be less well prepared. They have less to invest in getting it right. They don't have compliance teams or data protection officers. But small organisations often process a lot of personal data, and the reputation and liability risks are just as real."

Elizabeth Denham, information commissioner

The EU has tried to mitigate the impact of the GDPR on small businesses, additionally claiming the reform will cut costs and red tape for businesses.

This means:

- SMEs will not have to appoint a data protection officer, apart from where the organisation's core business requires regular and systematic monitoring of data subjects on a large scale, or process special categories of data (such as racial or religious information).
- SMEs will not have to keep records of processing activities, unless this is not occasional or likely to result in a risk for the rights and freedoms of data subjects.
- SMEs will not have to report all data breaches to individuals, unless the breaches represent a high risk to rights and freedoms.



Section 9
Useful resources

We have tried to be as comprehensive as possible in the creation of this guide, but acknowledge we have really only just scratched the surface of the GDPR's potential impact. A number of organisations have created free checklists for organisations to use to assess their readiness and weaknesses. As compliance with the GDPR is currently a moving target, it's equally important to keep on top of updates from the ICO and the Article 29 Working Party.

Checklists

ICO: Getting ready for GDPR

https://ico.org.uk/for-organisations/improve-your-practices/data-protection-self-assessment/getting-ready-for-the-gdpr

DMA advice: GDPR checklist

https://dma.org.uk/article/dma-advice-gdpr-checklist

Law firm Fieldfisher has developed a GDPR app for Apple devices, with its own checklist and countdown clock

https://itunes.apple.com/gb/app/gdpr-the-complete-guide/id1239256607?mt=8%20

DQM GRC: GDPR self-assessment (requires registration)

http://www.dqmgrc.com/gdpr-self-assessment

Other resources

Article 29 Working Party updates

http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

ICO consultations updates

https://ico.org.uk/about-the-ico/consultations/

Section 10
Timeline

Really, there's only one concrete date in the GDPR you need to worry about – 25 May 2018, the date it enters into force.

But there's plenty of work to get on with between now and then, so here are a few milestones you can work to as a guide – bearing in mind different organisations will be at different stages of the journey and will depend on circumstances. Don't forget to make use of the various checklists on offer from the likes of the ICO that can help to track your progress.

September 2017

By now you should have:

- Completed your information audit, and have an understanding of where your data is located and stored.
- Reviewed your data security and storage policies and procedures.
- Started the process of raising awareness of GDPR and its implications internally, and established a GDPR taskforce or appointed someone to take the lead on co-ordinating compliance.
- Spoken with your technology providers and third-parties who process or interact with your data to understand what they're doing with regards to GDPR compliance.
- Decided upon which legal ground(s) you intend to use to process data.
- Ensure members of the marketing team understand the implications of the post-GDPR landscape, to enable them to think of alternatives to email or SMS marketing.

November 2017

By now you should have:

- Reviewed your privacy policies and statements, and begun the task of making them GDPR compliant.
- Drawn up policies and procedures on how staff should handle data rights requests and potential security breaches.
- Put in place systems to record consent (if that's the legal ground you intend to use for processing), and implemented a preference centre or privacy dashboard, to enable you to begin the process of re-engaging your database to seek their permission to contact them after 25 May 2018.
- For email-centric marketing strategies, looked into potential alternative ways of contacting that audience (events or direct mail, for example) after 25 May 2018.

February 2018

By now you should have:

- Trained staff in the policies and procedures to deal with data requests or breaches so they're clear on what to do.
- Begun to re-engage your subscribers to build a database that has provable consent that individuals have opted in to receive messages from you.

May 2018

By now you should have:

- Put in place all systems and processes needed to become GDPR compliant.
- Completed your initial database re-engagement activity, with a final push warning those who do not confirm their consent will not receive any further communication.

Section 11
GDPR glossary

A guide to some of the most frequently used terms in the GDPR lexicon.

Article 29 Working Party

Set up in 1996, this group is made up of a representative from the data protection supervisory body of each EU member state, the European Data Protection Supervisor and the European Commission. The group provides guidance on the interpretation of data protection law.

Data processing

Under the GDPR, processing refers to any operation performed on personal data, including collection, recording, organisation, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Data controller

The organisation or individual that determines the purpose and manner of data processing.

Data processor

An organisation or individual that processes data on behalf of a data controller. One change under GDPR is that data processors can now be held liable by the regulator or individuals for a failure to comply.

Data subject

This is a living individual who the personal data is about.

Information Commissioner's Office

The UK's supervisory authority (see below) is the Information Commissioner's Office, an independent body established to uphold information rights. The current information commissioner is Elizabeth Denham.

Supervisory authority

As the GDPR is a regulation rather than a directive, it has binding legal force as opposed to being transposed into domestic law. Each member state appoints a supervisory authority to oversee compliance to the GDPR. In the UK this is the Information Commissioner's Office (ICO).

Acknowledgements

Thank you to the following experts who have helped to inform the development of this guide.

Jo Bance, head of global marketing, SQS

Sue Daley, head of cloud, data, analytics and AI, TechUK

Chris Evans, consultant, Druces

Andy Grant, MD, Bowan Arrow

Evgeny Grigorenko, head of public affairs, Europe, Kaspersky Lab

Richard Jones, business development, Foregenix

James Milligan, solicitor, DMA

Simon Moss, head of marketing, Communigator

James Mullock, partner, Bird & Bird

Oliver Pinson-Roxburgh, EMEA director of solutions architecture, Alert Logic

Zach Thornton, external affairs manager, DMA

Claire Trévien, head of content marketing, Passle

Tom Wright, head of content, Incisive Media



About B2B Marketing

Established more than 12 years ago, we are the number one go-to resource for B2B marketers across the globe.

Through our content hub and professional development services – including events, training and networking – B2B Marketing users are empowered with the tools, insight and inspiration they need.

Our promise to you

Things change fast in B2B. Just staying on top of the changes can be a full-time job. So, we do that job for you.

With our subscriber content, training and events we guarantee you'll:

- Put your best-ever strategies in place
- Lock down the multiple skills, tools and insights you need
- Find real-world inspiration for rolling out some outstanding marketing initiatives
- Make the progress you've always wanted in putting marketing at the top table of your business.

How we help you, your team and your business to grow and succeed

- Free online member content, including guides, toolkits, interviews and case studies from experts and inspirational leaders in B2B
- Premium, subscriber-only content, including industry research, benchmarking and analysis, expert strategy and tactical guides and a *B2B Marketing* magazine subscription
- Four, flagship UK-based, annual events for B2B marketers and leaders: Ignite; The Conference; InTech; and the B2B Marketing Awards
- Bespoke training for marketing teams (UK only)
- More than 40 one-day open training courses and workshops each year (UK only)
- Leaders networking, through the B2B Marketing Leaders programme and Leaders Forum (UK only).

First step

- Choose a 12-month subscription to all our Premium subscriber content – for just £399/$499
- Go to b2bmarketing.net/unlock to find out more about the benefits of subscribing.
- Or call our client services team on +44 (0)207 014 4920.

B2B Marketing

Insight · Development · Training · Events

b2bmarketing.net

B2B Marketing

Insight · Development · Training · Events

Contact us

B2B Marketing
Clover House
147–149 Farringdon Road
London
EC1R 3HN

Tel: +44 (0)20 7014 4920
info@b2bmarketing.net
b2bmarketing.net