



GDPR and text messaging

What you need to know



Contents page:

Introduction	pg.3
GDPR, you ready?	pg.4
The Basics of GDPR	pg.5
What is meant by 'processing personal data'?	pg.6
What is meant by having a 'lawful basis' for data processing?.....	pg.7
Sending texts after GDPR	pg8
Identifying the most appropriate lawful basis	pg.9
Customers and legitimate interests	pg.10
Prospects and ex-customers - gaining consent	pg.11
Gaining consent from your existing database contacts	pg.12
Understanding the role of privacy policies	pg.14
Updating your privacy policy	pg.15
Presenting your privacy policy	pg.16
GDPR and data processing - what are your responsibilities?	pg.18
Conclusion	pg.21

Introduction

We're increasingly being asked, "Will I still be able to send SMS to customers after the GDPR legislation comes into effect?" And, "Do I need to get my customers to explicitly opt-in to receiving text messages from me?"

The short answer is, yes, you can continue to text your customers, and no, you don't necessarily need to re-request their permission to do so, but it's essential that you familiarise yourself with the basics of the GDPR to ensure that you are compliant.

The GDPR (General Data Protection Regulation) is a European Union directive and regulation to which the UK will adhere; it replaces the UK Data Protection Act 1998 (DPA). It is designed to allow individuals to better control their personal data - meaning any data that can identify them, regardless of whether it is in a private, public or work context.

This newly instated regulation comes into effect as of May 2018, so what does it all mean? In this eBook we'll explain by looking at the following:

- ▶ The basics of GDPR
- ▶ The meaning of 'processing personal data'
- ▶ Identifying the appropriate lawful basis for communicating with your customers
- ▶ Updating your privacy policy - why it's necessary and how to do it.

It is important to note that while we have checked our sources and are confident in our interpretation, this eBook does not constitute legal advice.

GDPR, you ready?

The EU General Data Protection Regulation (GDPR) is one of the most important changes to happen in data privacy regulation in 20 years. Many businesses have spent several months preparing for this, but many more are unsure about how it affects them. We hope to make explicit the steps you must take, and provide a simple framework for doing so.



The basics of GDPR

The General Data Protection Regulation, or GDPR, came into effect on 25th May 2018 and replaced the previous legislation for data protection in every EU country – including the UK. It is designed to allow individuals to better control their personal data - meaning any data that can identify them, regardless of whether it is in a private, public or work context.

Key definitions under GDPR

Data controllers are the individuals or organisations who determine the purpose for which the data is going to be used (this is most likely to be your role). **Data processors** are the individuals or organisations who process the data (in sending your messages, Esendex is a data processor).

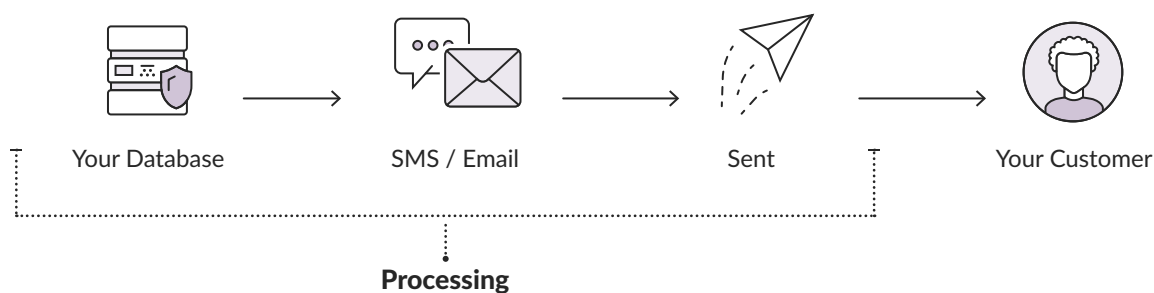
The new legislation puts the responsibility for protecting data subjects' rights on the shoulders of both the controller and the processor, resulting in significant fines for organisations that do not comply. Previously, data controllers were largely responsible for data integrity; the change in the law means that you as a data controller need to be sure that you are partnering with GDPR-compliant data processors.

To find out more about your responsibilities as a data controller, jump to '[GDPR & data processing - what are your responsibilities?](#)'.

What is meant by 'processing personal data'?

“Processing... means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data... it is difficult to think of anything an organisation might do with data that will not be processing.”¹

Your customer database and any SMS (or emails) that you send to the individuals within the database would be considered 'processing'.



What is meant by having a 'lawful basis' for data processing?

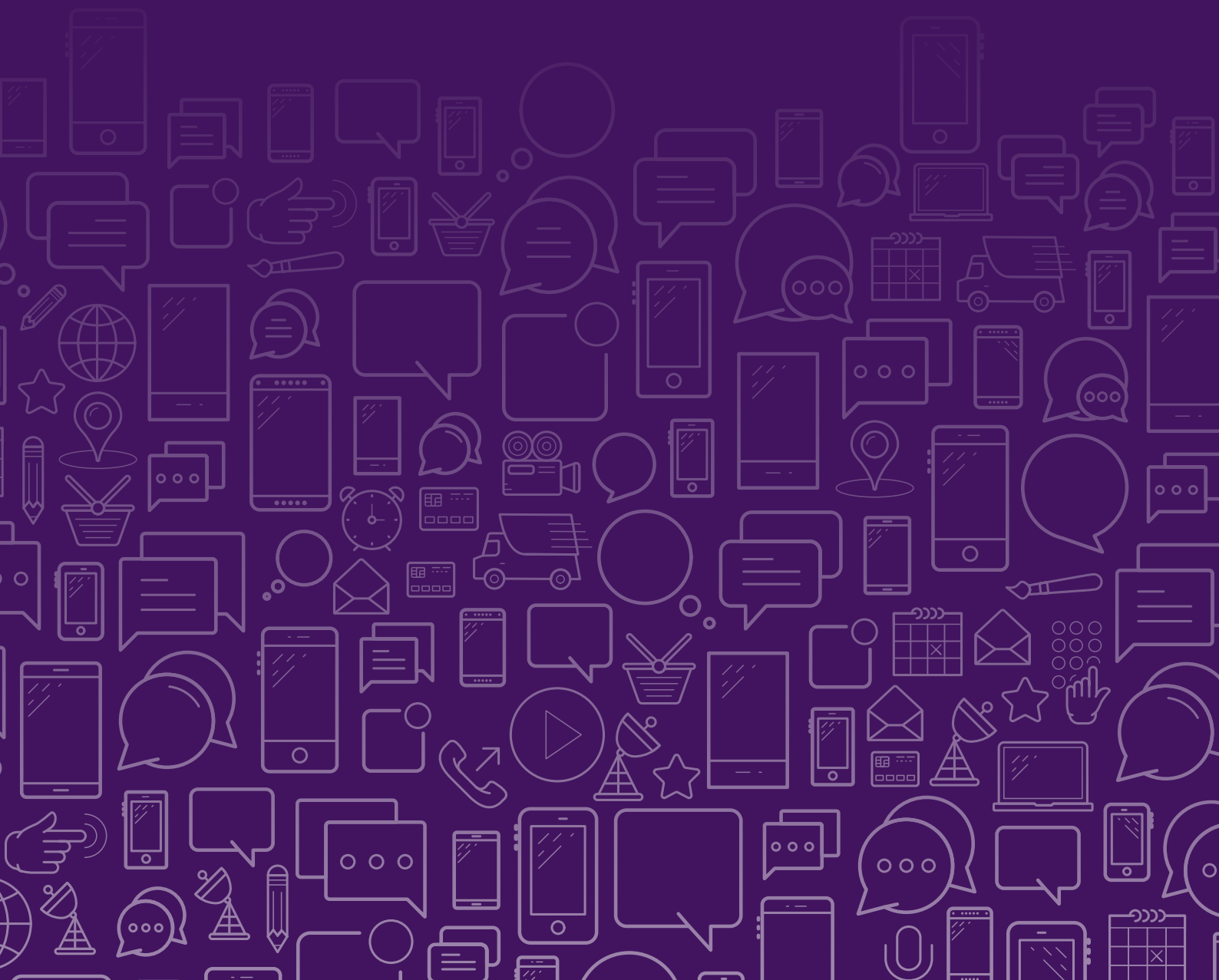
It is effectively the justification you have for processing data. There are six available lawful bases for processing, none of which is 'better' or more important than the others. The one getting all of the airtime is **gaining consent**, but – and this is a key takeaway – where your existing customers are concerned, it's probably not the most appropriate.

Defining prospects, customers and lapsed customers

- ▶ A **prospect** is someone who has provided you with their contact information, but hasn't (yet) taken the next steps of making a purchase, booking an appointment, or formally registering to utilise your services
- ▶ A **customer** is someone who has taken those next steps, 'taken those next steps, and has an active relationship with you
- ▶ A **lapsed customer** is someone who was a customer but isn't a customer any more. Exactly how you define a lapsed customer will vary from business to business, and industry to industry. For example, at Esendex, we take the view that a customer is officially 'lapsed' 12 months from the date of their last purchase – because in the nature of what we sell (principally **SMS**), it can take several months for the customer to utilise that service.

Sending texts after GDPR

There are six lawful bases for data processing, and your relationship with the individuals whose data you hold will determine which is the most appropriate. The following section both aims to help you identify your lawful basis (or bases), and how to ensure that you are meeting the requirements for compliant data processing.

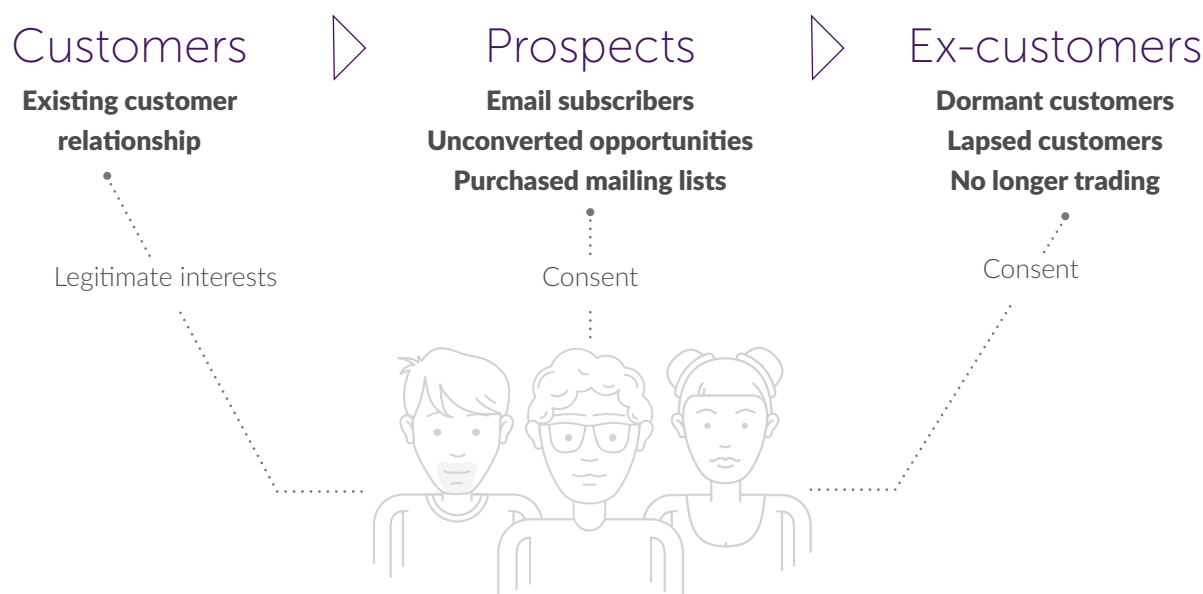


Identifying the most appropriate lawful basis

The six lawful bases are:

- ▶ Consent
- ▶ Contract
- ▶ Legal obligation
- ▶ Vital interests
- ▶ Public task
- ▶ Legitimate interests.

The two lawful bases for communication which we think most private companies' data processing activity will fall under are consent and legitimate interests.



Legitimate interests is the most flexible lawful basis for processing, covering you for using people's data in "ways they would reasonably expect and which have a minimal privacy impact, or where there is a compelling justification for the processing."¹

However, in the case of both prospects and lapsed customers, it is probable that gaining consent will be the most appropriate lawful basis for communicating with them, because legitimate interests are only valid when you can demonstrate an "existing customer relationship."

Customers and legitimate interests

Every act of processing - for example, sending an email newsletter to an existing customer – needs to stack up against three questions:

- 1 Do you have a legitimate interest for sending this message?** This can include your own need to cross-sell other products / services or promote wider use of an already purchased item, for example
- 2 Do you need to send the message in order to achieve those interests?** If you could reasonably achieve the same result through other, less intrusive means (such as unprompted visits to your website), legitimate interests do not apply.
- 3 Have you balanced the act of sending the message against the individual's interests, rights and freedoms?** This comes back to the early statement about reasonable expectations on their part.

These three steps make up the Legitimate Interests Assessment (LIA), which should be completed ahead of the GDPR coming into effect. There is a detailed explanation and a template for completing the LIA from the Data Protection Network [here](#).

Prospects and ex-customers - gaining consent

How you approach this now depends on how you have approached this in the past.

If you have always provided a tick box at the point at which you collected their data to say 'Yes! I would like to receive updates about products and services...', and allowed people to **actively opt-in** by ticking that box, then, assuming that they have had the opportunity to unsubscribe, you will simply need to be able to demonstrate that consent.

However, most businesses haven't done this: they've either rolled in consent with their normal terms and conditions of service; they've pre-ticked the consent box, or they've missed this step out altogether.

If this is you, don't panic.

Going forward, you need to have a tick box at the point of gathering data which invites individuals to opt-in to receive messages from you. This must be separate from other terms and conditions and not pre-ticked. *eConsultancy* lists some great examples of different retailers, media companies and charities getting this right.

Gaining consent from your existing database contacts

Before even considering this exercise, you need to ensure two things: firstly, that your prospects and lapsed customers haven't unsubscribed. You can't contact people who have unsubscribed.

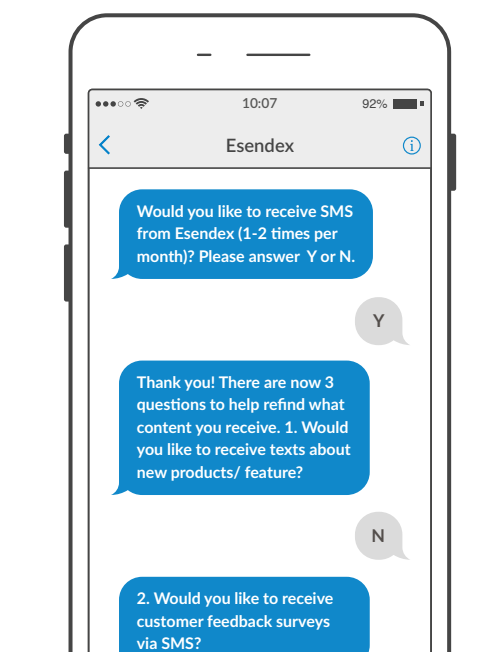
Secondly, that your original method of collecting the data was inline with *PECR's guidelines*. If you're unsure about this, it's probably better to err on the side of caution, and use a non-electronic means refreshing consent (*direct mail is not subject to the same rules as electronic mail*).

1 Email consent

Emailing your prospects and lapsed customers to ask them to confirm if they want to continue receive content from you going forward is quick, easy and cheap. However, if your email open rates aren't great to begin with, the amount of people who'll see this request will be limited. For some ideas we like this *re-engagement blog post from IMPACT* – or just check out your own inbox!

2 SMS Survey consent

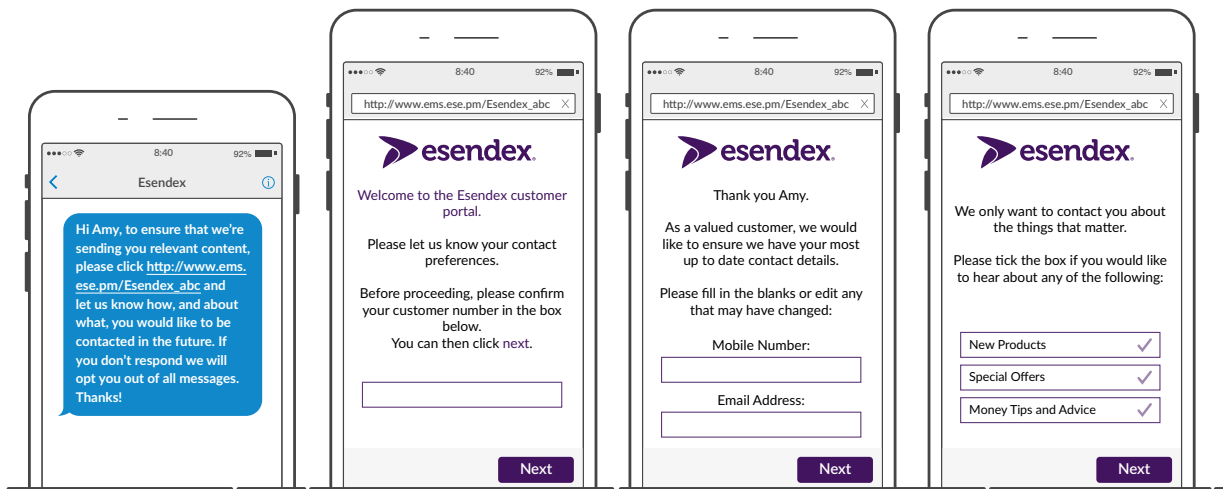
With a 95% open rate for text messages¹, an *SMS Survey* overcomes email's visibility challenges, and as you can see from the screenshot on the right, can replicate the functionality of a preference centre. However it's probably not best suited for email preferences, so would need to be combined with an email or direct mail campaign.



3

SMS + mobile-first preference centre

To overcome the limitations of an SMS Survey, try coupling a text message prompt with a mobile-first preference centre. Most preference centres are not designed with the mobile user in mind, and an unfriendly user experience here will result in fewer people completing the exercise. A service like a *Mobile Journey* delivers full preference centre-functionality, but puts the needs of the mobile user first, as our example shows.



At the point at which GDPR becomes effective, any prospect or lapsed customer who hasn't specifically opted in to receiving messages from you should be considered as having unsubscribed, and ultimately removed from your database.

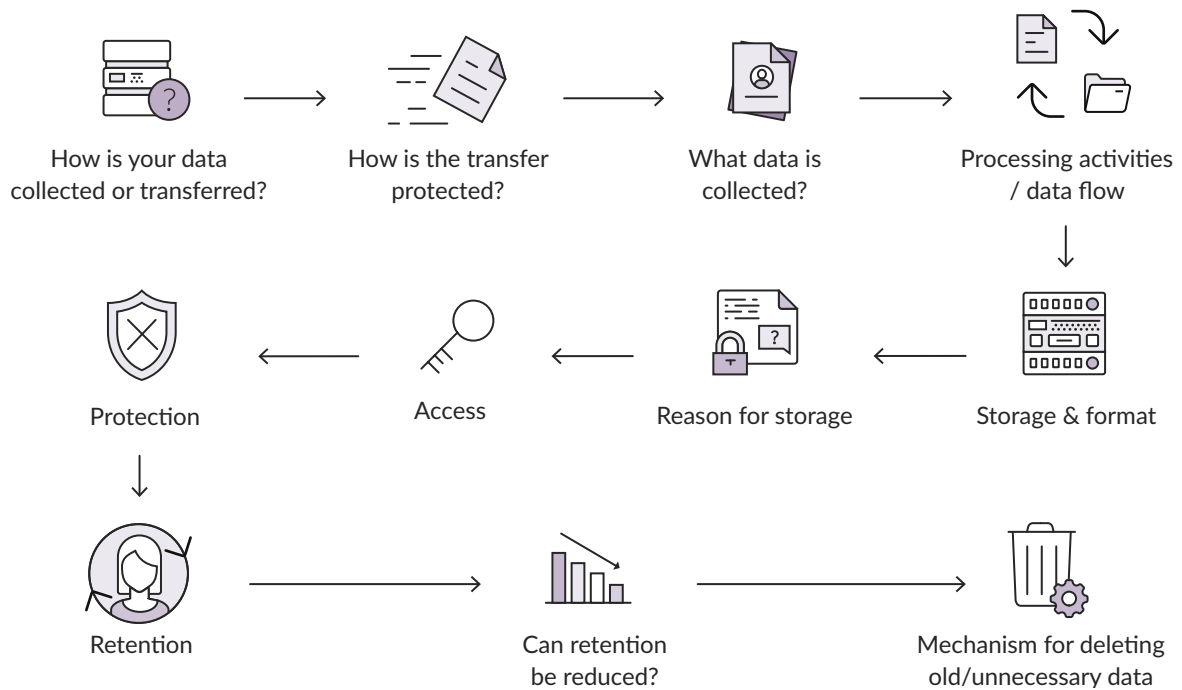
Yes, it's quite possible that your database will be reduced as a result of your GDPR preparations, but on the plus side, **the people that do opt-in will be more engaged** – and you're probably losing people who weren't that excited about hearing from you in the first place.

Understanding the role of privacy policies

It's estimated that the average person would spend 244 hours reading the privacy policies of every website they visited in a year. So, no one reads them. But under GDPR they gain greater importance as companies must now ensure that their privacy policy is provided to data subjects at the point of data collection. In this section we'll look at what needs to be included in your privacy policy, and where it needs to be displayed.



Updating your privacy policy



1

Get to know your data - map out how your information flows through your organisation, and how you process it

2

Conduct a privacy impact assessment to understand whether you actually need to carry out these processes

3

Write up your privacy policy which should address:

- ▶ Scope (type of information and to whom the policy applies)
- ▶ Policy statement (expected behaviours and consequences of non-compliance)
- ▶ Definition of personal information
- ▶ Protection standards
- ▶ Destruction standards
- ▶ Who to call for questions and concerns
- ▶ An effective date.

Presenting your privacy policy

There are numerous ways to present a privacy policy and it's important that it reflects your business. A generic statement that uses complicated vocabulary will not cut it. Channel 4 does this very well in their '*Viewers promise*' which uses a light tone and video to explain their intentions behind their data requests.

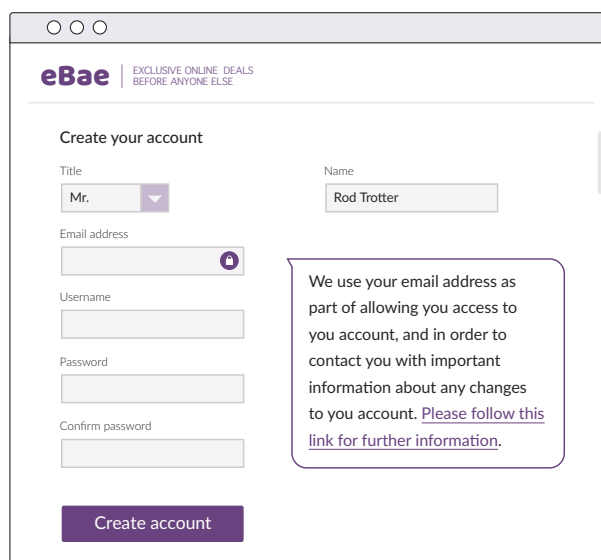
Messaging app *Telegram*, although longer than some privacy notices, is clear and easy to understand. By dividing their policy into four specific sections: Sharing data, Storing data, Deleting data and Payment information, users are able to quickly find the information they need.

The ICO focuses on two types of approach:

The 'just in time' approach

This example provides a quick explanation as to why this information is being requested at the point of collection.

When a user interacts with a data field, the reason you're collecting that information can be clearly presented alongside their submission. This is a simple option that most form building software can provide already.



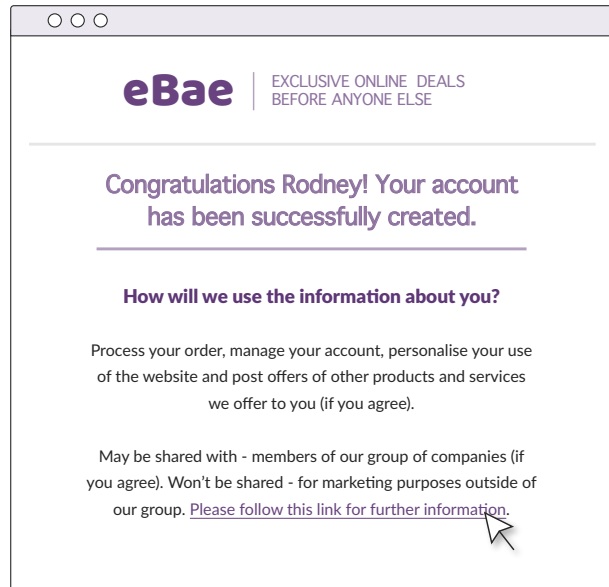
The screenshot shows a web browser window with the eBae logo and tagline 'EXCLUSIVE ONLINE DEALS BEFORE ANYONE ELSE'. The page title is 'Create your account'. The form includes fields for Title (dropdown menu with 'Mr.' selected), Name (text input with 'Rod Trotter'), Email address (text input with a lock icon), Username (text input), Password (text input), and Confirm password (text input). A purple 'Create account' button is at the bottom. A callout box on the right contains the text: 'We use your email address as part of allowing you access to you account, and in order to contact you with important information about any changes to you account. [Please follow this link for further information.](#)'

The 'layered' approach

This can help you provide the necessary information when space is limited.

With layers, you can continue to add more information as the customer clicks through – integrating with the customer journey.

It's always recommended, regardless of which style you choose to use, to direct the recipient to the full privacy policy, in all call-outs.



The screenshot shows a browser window with the eBae logo and the tagline "EXCLUSIVE ONLINE DEALS BEFORE ANYONE ELSE". The main heading reads "Congratulations Rodney! Your account has been successfully created." Below this, a section titled "How will we use the information about you?" lists the purposes: "Process your order, manage your account, personalise your use of the website and post offers of other products and services we offer to you (if you agree)." A second section states: "May be shared with - members of our group of companies (if you agree). Won't be shared - for marketing purposes outside of our group. Please follow this link for further information." A mouse cursor is pointing at the link.

GDPR and data processing - what are your responsibilities?

Data controllers define the purpose (why) and means (how) of the processing of personal data. You are almost certainly a data controller.

Data processors process personal data on behalf of the controller, following the controller's instructions. Data processors include the provider of your CRM / billing system, cloud hosting services, outsourced IT, and Esendex!



What are your responsibilities as a data controller?

The best place to start is to map your data processes, and identify all of the internal and external systems that touch personal data – from Google Analytics through to your tax adviser. This should provide you with a list of data processors.

As a data controller, you are responsible for appointing data processors who can provide sufficient guarantees that they've implemented technical and organisational measures that meet the requirements of the GDPR.

Some good questions to ask data processors are:

- 1.** Where is the data stored?
- 2.** What are the data flows?
- 3.** Who can access the data?
- 4.** Do you have a Data Protection Officer (DPO)?
- 5.** Do you inform me if you transfer data to any other processors, or a third country?
- 6.** Have you ever experienced a data breach?
- 7.** What controls do you have in place to reduce risk?
- 8.** Do you have security breach notifications in place?
- 9.** Can you provide a description of your security measures?
- 10.** What are your processes for deleting data should our agreement come to an end?

Once these questions are answered satisfactorily, you'll need a written contract when you directly employ a data processor, or if the data processor employs another processor. This should specify what processing activity they are permitted to undertake on your behalf, and commit them to compliance with GDPR. This type of contract is known as a **Data Processing Agreement**.

Check your existing contracts to ensure that they cover these two points, that you know the answers to the above questions, and that the responses are documented; if not, it's time to revisit them.

Data Processors

As a data processor, you need to ask yourself the same questions as the above list, and **ensure that you:**

- ▶ Have adequate information security in place
- ▶ Keep a record of all processing activities
- ▶ Have a process for notifying the controller of any data breaches, and assist the controller in managing the consequences
- ▶ Have appointed a Data Protection Officer if one is required (here is a *checklist* to determine if you need a DPO)
- ▶ Cooperate with the relevant authorities in the event of an enquiry
- ▶ Comply with EU data transfer rules and *data subjects' rights*
- ▶ Are able to delete or return all personal data at the request of the controller
- ▶ Advise the controller if the nature of their processing request is not compliant with GDPR.

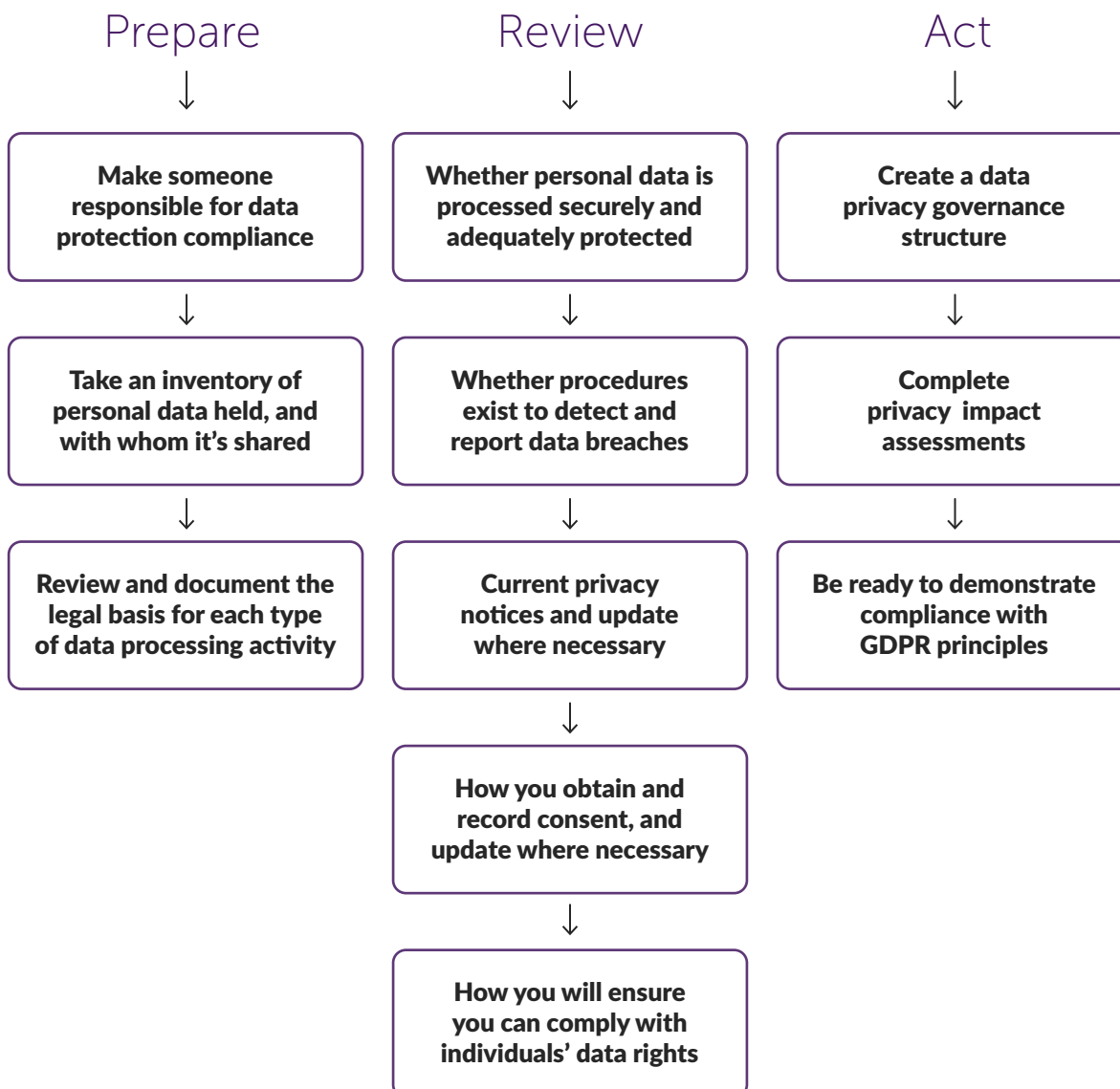
Conclusion

By the time you read this eBook, it's likely that the GDPR will be live and enforceable. Some readers will be reassured that they've taken the necessary steps for compliance, while others may not have started. If you're in the latter group, start now. Be proactive, even if a year has elapsed and you've not (yet!) experienced any challenges because of non-compliance.



Steps to compliance

Here's a summary of the steps you need to take:



About Esendex

Esendex is a mobile business communications provider helping thousands of customers worldwide.

We offer 1-2-1 account management to help you get the best out of your transactional and marketing campaigns, and have direct network connections to all of the major networks, meaning that your messages will be delivered quickly, securely and reliably.

To contact your account manager:

 Call **0345 356 5758**

 Visit www.esendex.co.uk where our agents are available on [LiveChat](#) (office hours only).



Designed and published by Esendex Ltd.

Esendex Limited 2018 | Registered company number: 04217280