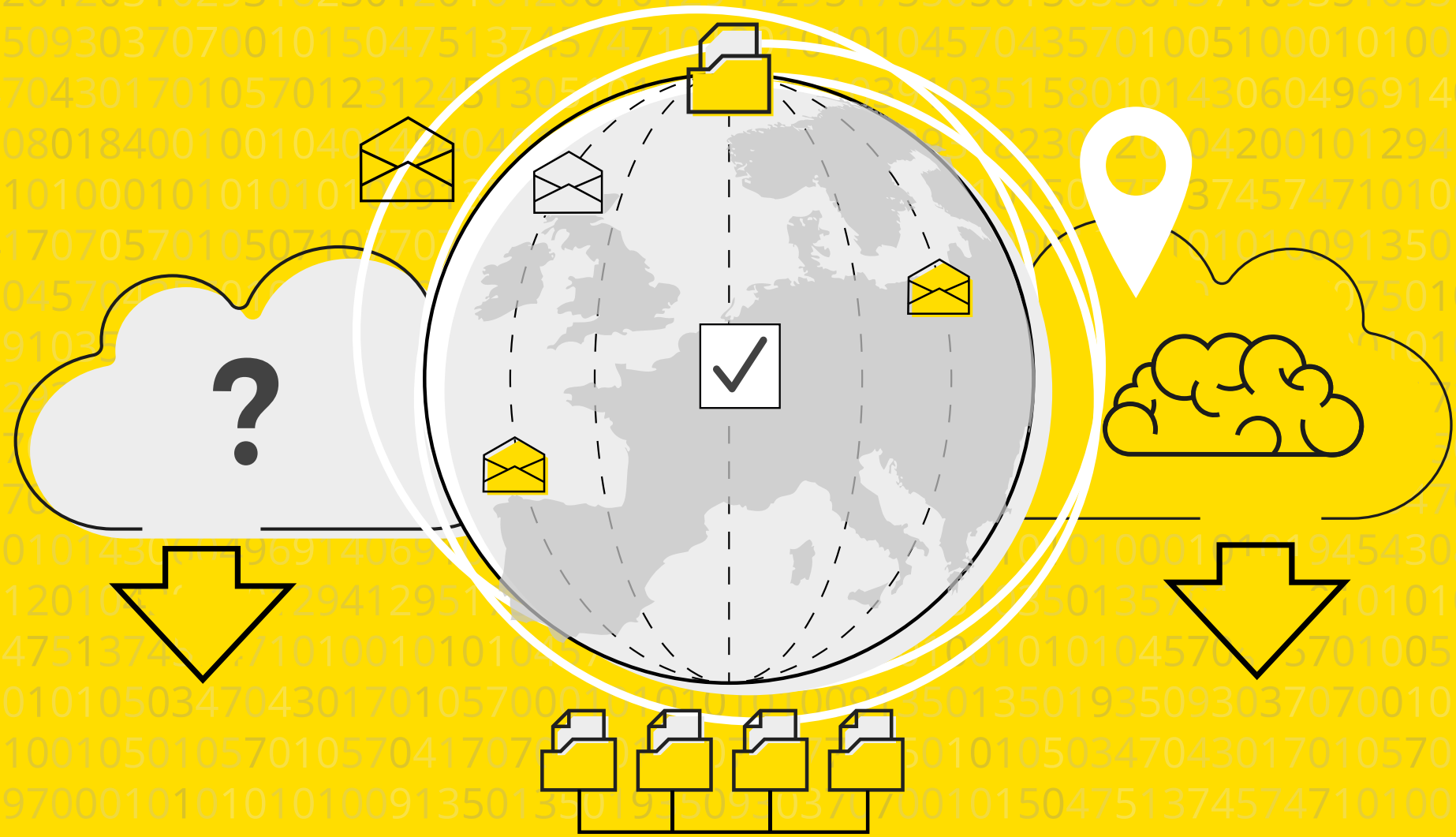
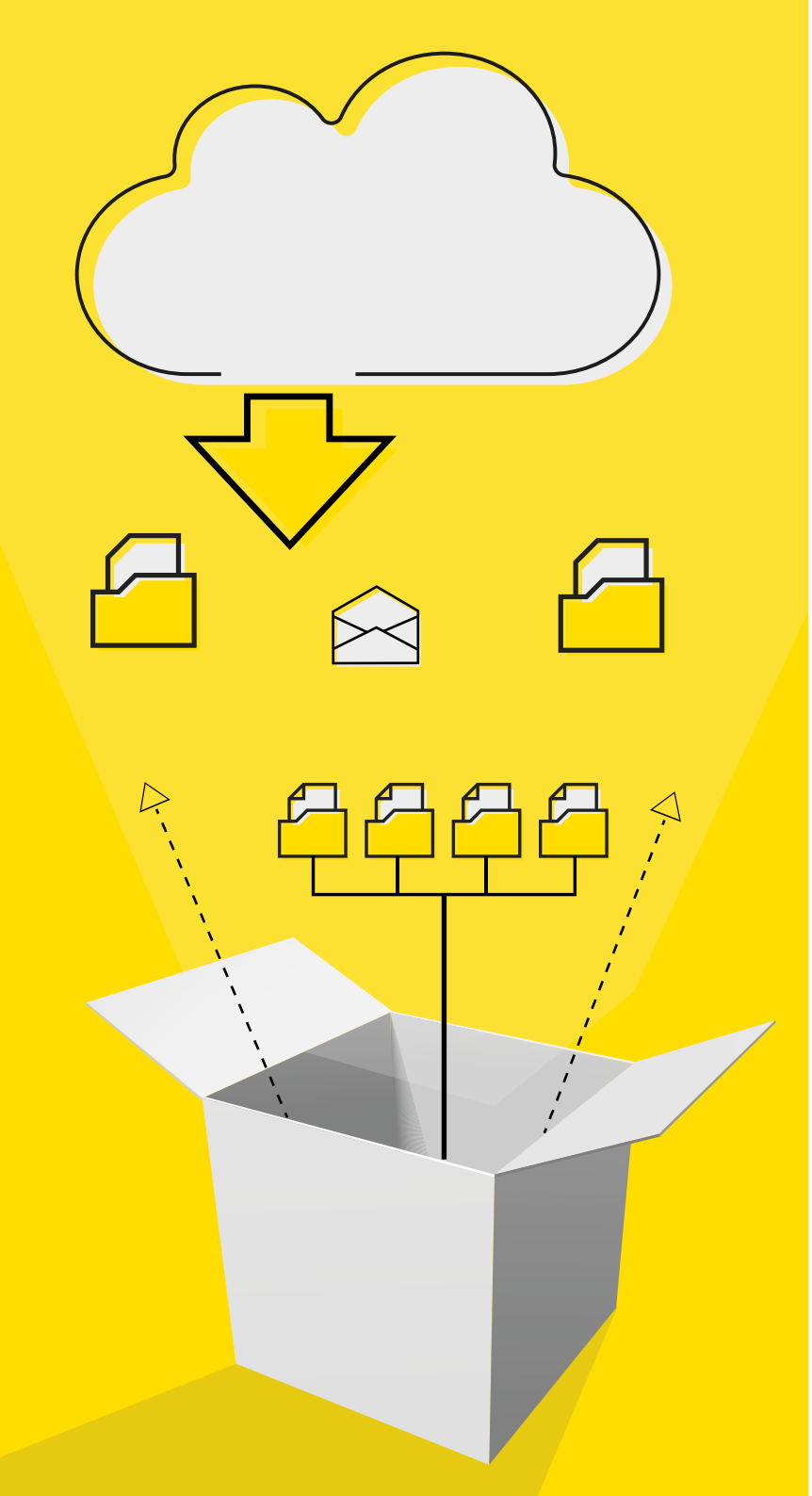


Your GDPR questions answered

The feefo guide

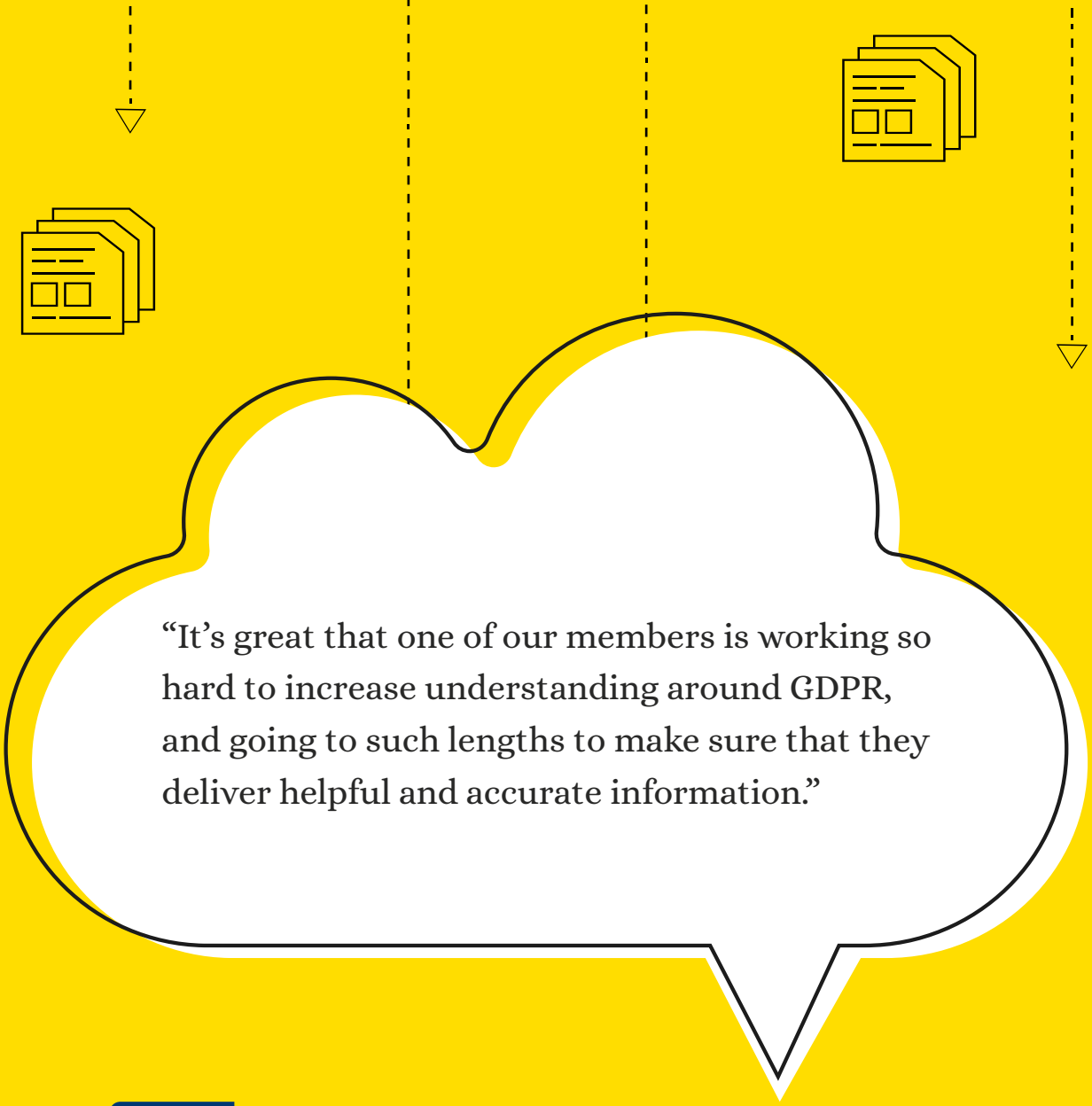


What's inside...

Introduction

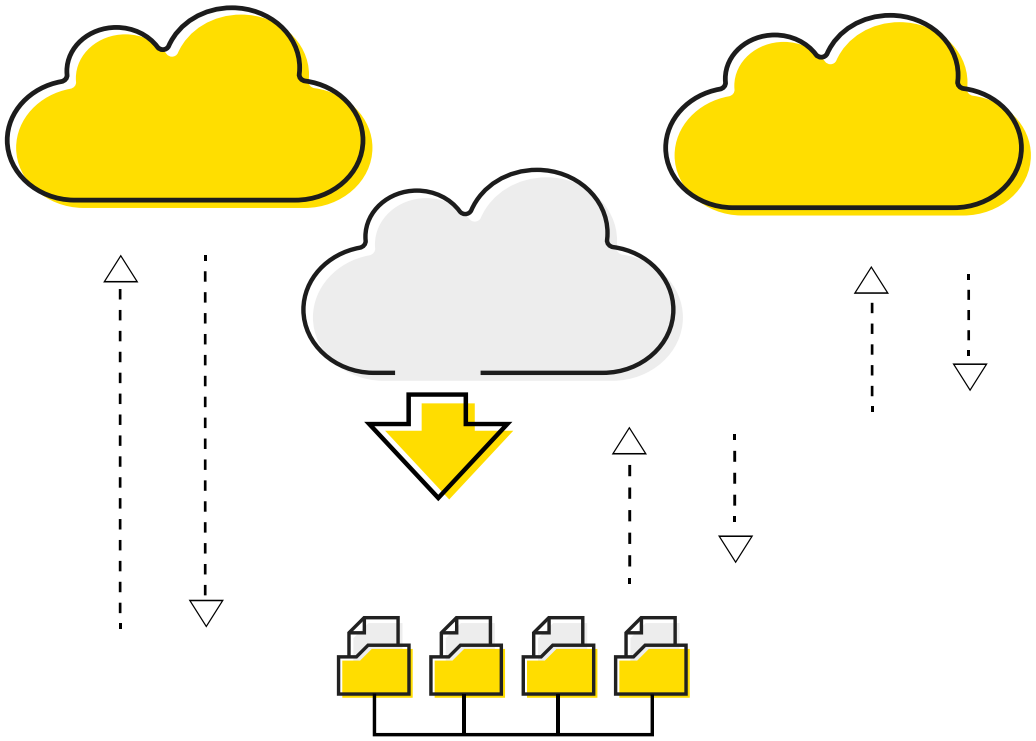
At Feefo, we're all about gaining valuable insight from customer feedback. After listening to the questions that our customers are asking about GDPR, we've come to the conclusion that finding straightforward answers isn't as easy as you'd think!

We've gathered together some of our most commonly asked questions, and done our best to answer them in plain English. This e-book by no means qualifies as a legal document and is no substitute for seeking help and advice from a legal professional. It should however, give you a better understanding of GDPR and a good idea of what you will need to do to comply with the new regulations.



"It's great that one of our members is working so hard to increase understanding around GDPR, and going to such lengths to make sure that they deliver helpful and accurate information."

John Mitchison, Director of Policy and Compliance, Direct Marketing Association (DMA)



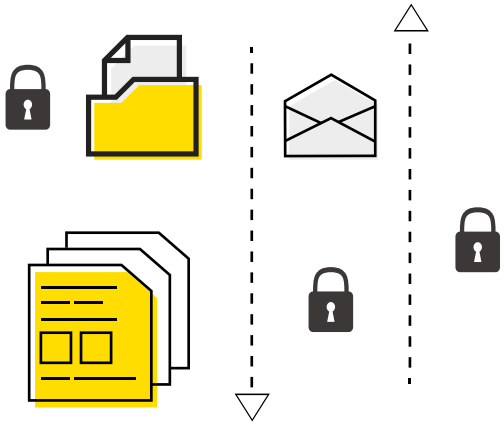
What is GDPR?

On the off-chance that all of this has somehow passed you by (it's not as unusual as you'd think!), the GDPR is an EU regulation, designed to update and align current data protection laws across the continent. The new regulation gives greater rights and protection to the individual when it comes to their personal data.

In order to meet the new standards, businesses and organisations may have to make some big changes to their existing practices and put new rules in place to make sure that they are fair and honest when it comes to collecting data in the future.

Before we get started

There are a few bits of terminology that you'll see cropping up time and time again. Here is a basic overview of some of the main offenders.



Remember, these are simple explanations of complicated terms. Make sure you get legal advice when putting together your plan.

feefo

Your questions answered...

What is a Data Controller?

A Data Controller is the person or persons that decide who to collect data from, and why and how that data will be used.

What is a Data Processor?

A Data Processor provides a service; they receive data from the Data Controller, process it and then generate output. The Data Processor doesn't take ownership of personal data or decide how or why the data is used, they merely act on behalf of the Data Controller. (Note: A Data Processor cannot be an employee of a Data Controller.)

What is the Right to Erasure ?

This is also sometimes referred to as The right to be forgotten. Individuals now have the right to request that their personal data be erased without delay. It may be necessary, however, for organisations to keep skeletal data in-house for legal reasons, or to make sure that they no longer market to that individual.

What is a Supervisory Authority?

This is the independent authority responsible for enforcing GDPR. Each nation within the EU will have its own supervisory body and the Information Commissioner's Office (ICO) will be responsible for the UK.

What is a Data Protection Officer?

A DPO is either an employee or somebody hired externally who is responsible for making sure that their organisation complies with the GDPR. They act as the main point of contact for data subjects and national supervisory authorities, such as the ICO.

What is Legitimate Interest?

Legitimate Interest is a legal ground for processing data that allows businesses to use direct marketing without consent in certain circumstances. Strict criteria have to be met by organisations that want to rely on LI and the individual still has the right to object.

Is GDPR a good thing?

The GDPR is all about respect, and respect is always a good thing. The new regulations encourage you to build a better relationship with your customers, clients or candidates based on transparency and trust.

You may stand to lose some tired consumers in the short term, but the long-term reality is that the right approach to data protection will allow you to grow a far more valuable database of engaged customers that will ultimately benefit your business.

Improve and enhance with deeper insights

It's important that we begin to recognise the true value of a customer's data. When a consumer grants a business or organisation access to their personal information, it is an investment, and like all investments they expect some return.

The contract of trust cannot be one-sided and enhancing every stage of the customer experience should become a priority, using the valuable insight we're entrusted with, to improve customer service, send relevant communications and tailor content to keep them engaged.

How to use customer data responsibly

Here are some rules of thumb when it comes to responsible practice. Adopting good data protection as a core value of your business will promote consumer confidence, build lasting relationships and create valuable advocates for your brand.

88% of consumers think transparency increases trust

63% of us are happy to share our personal data

Top tips to follow...

The customer comes first

We are all consumers. How would you want your data to be used? Data should be used to benefit the customer as well as your business.

Be diligent with data

Make security a priority, build confidence and use customer data wisely.

Respect privacy

Data belongs to the individual, not the business. Don't bombard customers or share without consent.

Meet customer expectations

Make sure you honour your promises and give them the service and information that convinced them to opt in.

Take responsibility, be accountable

Make a concerted effort to comply and change old habits for the better; monitor customer feedback and be quick to respond if there's an issue.

Be honest, fair and transparent

Let people know why and how you want to use their data. Make it interesting and relevant, so they want to be part of the conversation.

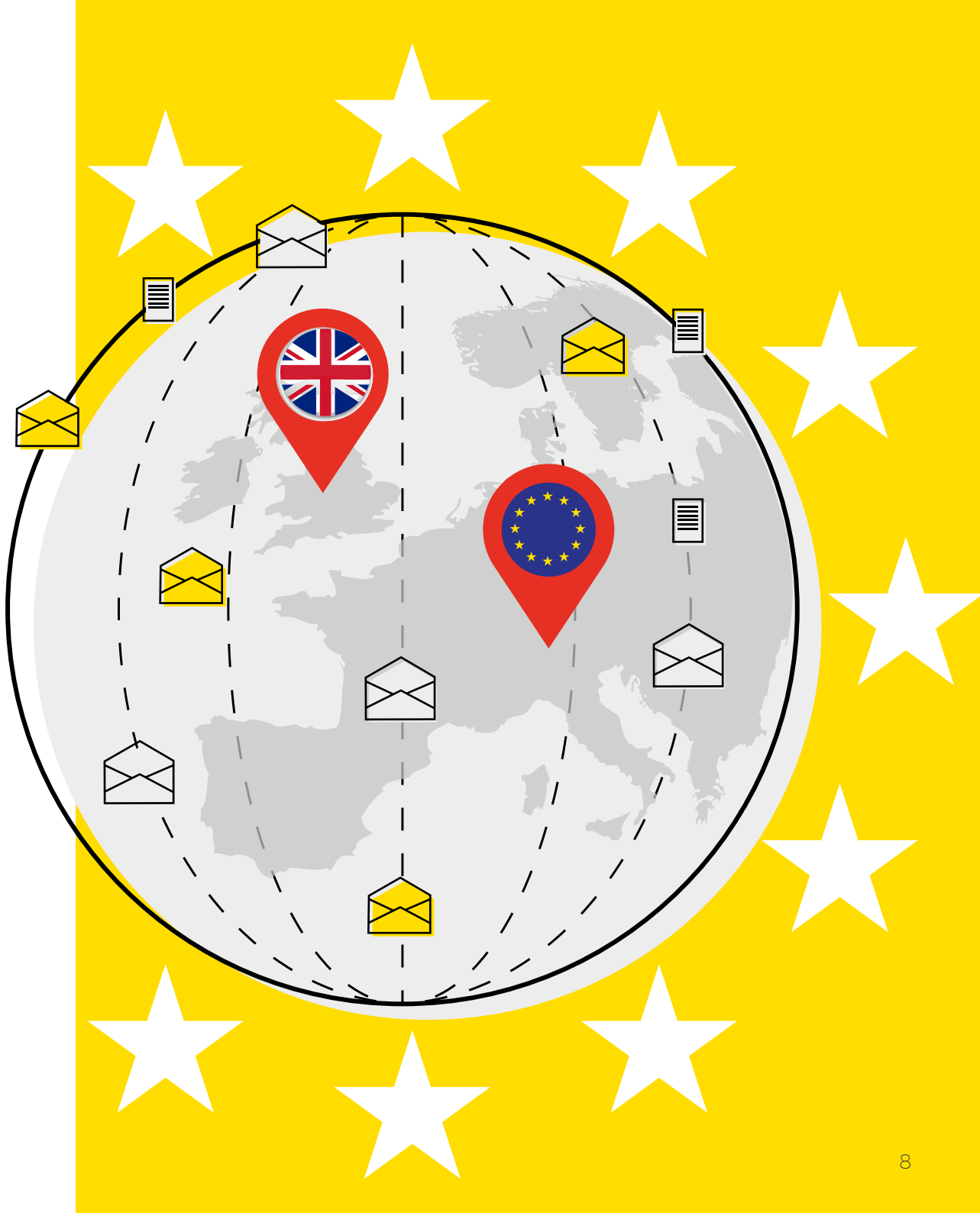
*Source: DMA (GDPR for marketers)

Is GDPR replacing the Data Protection Act?

If GDPR wasn't tricky enough to get your head around, the question 'will GDPR replace the Data Protection Act?' is not actually as straightforward as it may seem; the answer is both 'yes' and 'no'.

The current Data Protection Act (DPA) came into force in 1998. Since then, data capture has become standard practice, and with everyone from your hairdresser to a myriad of retailers holding some kind of personal information on you, the DPA no longer covers enough digital ground to offer the right level of protection.

In 2017, the government published the first draft of the Data Protection Bill (due to become the Data Protection Act 2018 and technically, it is this which will replace the current DPA, bringing EU GDPR standards into UK law. The DPA deals exclusively with data protection for the UK (as will the Data Protection Bill), whilst the GDPR is designed to raise standards and introduce a consistent approach to data protection across the EU.



Your questions answered...

What's the point of the Data Protection Bill?

There are a couple of reasons why we need the Data Protection Bill.

- It covers the areas of the GDPR that are left up to the individual EU member states to decide.
- When Brexit finally comes about, there will be terminology used in parts of the GDPR, which no longer applies to the UK.
- It offers some consistency and maintains the same standards as the GDPR, making it easier to continue trading.

Do I still need to worry about GDPR?

Absolutely, and here's why:

- Until Brexit finally takes place we are still a member of the EU and subject to the penalties for failing to comply.
- The rules of the GDPR have to be adhered to in order to process the data of anybody from an EU member country, even if they live in the UK.
- The Data Protection Bill purposely works the rules of the GDPR into UK law along with the allowed variations. The general gist is essentially the same, with the intention of keeping things consistent pre, and post Brexit.

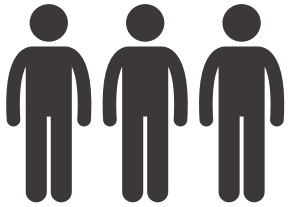
Why do we need both?

- The Data Protection Bill works alongside the GDPR. It references sections of the GDPR, but doesn't replicate them, so you need to cross-reference.
- The Bill also contains legislation that is specific to the UK.
- Any country outside of the EU has to have equivalent data protection standards in order to trade with EU states. The Data Protection Bill will uphold the standards introduced by the GDPR.

How will GDPR be enforced?

With a maximum fine of €20 million (or 4% of your annual global income, whichever is higher), we're well aware of the potential financial costs, but what are the other consequences of non-compliance and who is going to hold your business to account?

There are two key parties responsible:



Consumers

Consumers have the right to report you to the ICO or to take you to court if they feel their data has been misused.

Supervisory Authority (ICO)

The ICO can take action against an organisation if it suspects non-compliance. It has the power to issue fines, warnings, orders to comply and to restrict or even ban you from processing data.

What are the consequences of non-compliance?

The UK Supervisory Authority (ICO) has the power to take the following action:

Guidance

Warnings

Restrictions

Fines

How can you protect your business?

There are so many conceivable scenarios that it would be impossible to provide a complete guidebook on how to stay fully compliant with GDPR, so every organisation will need to make their own risk-based decisions.

3 tips to help you on your way...

1 Be safe, be seen

Don't just comply, be seen to be compliant. The key is being able to prove that you are doing as much as possible to adhere to the GDPR. Issues will always arise, but taking positive steps to process personal data fairly and lawfully will demonstrate your accountability.

2 Stay vigilant

Make sure that you monitor your customer feedback, ensuring that all potential issues are dealt with swiftly. Your customers can issue a complaint to the ICO if they believe their data is being misused. Quickly responding to negative feedback around data usage will show customers that you take their complaints seriously and respect their right to privacy.

3 Be honest

Being open and honest about how you use an individual's data is vital. Consumers who trust that their data will be used to benefit them (e.g. for personalised experiences) are more willing to share personal information, but it's then your responsibility to meet their expectation. Remember, if a customer has given consent for you to use their data, they can also revoke it at any time.

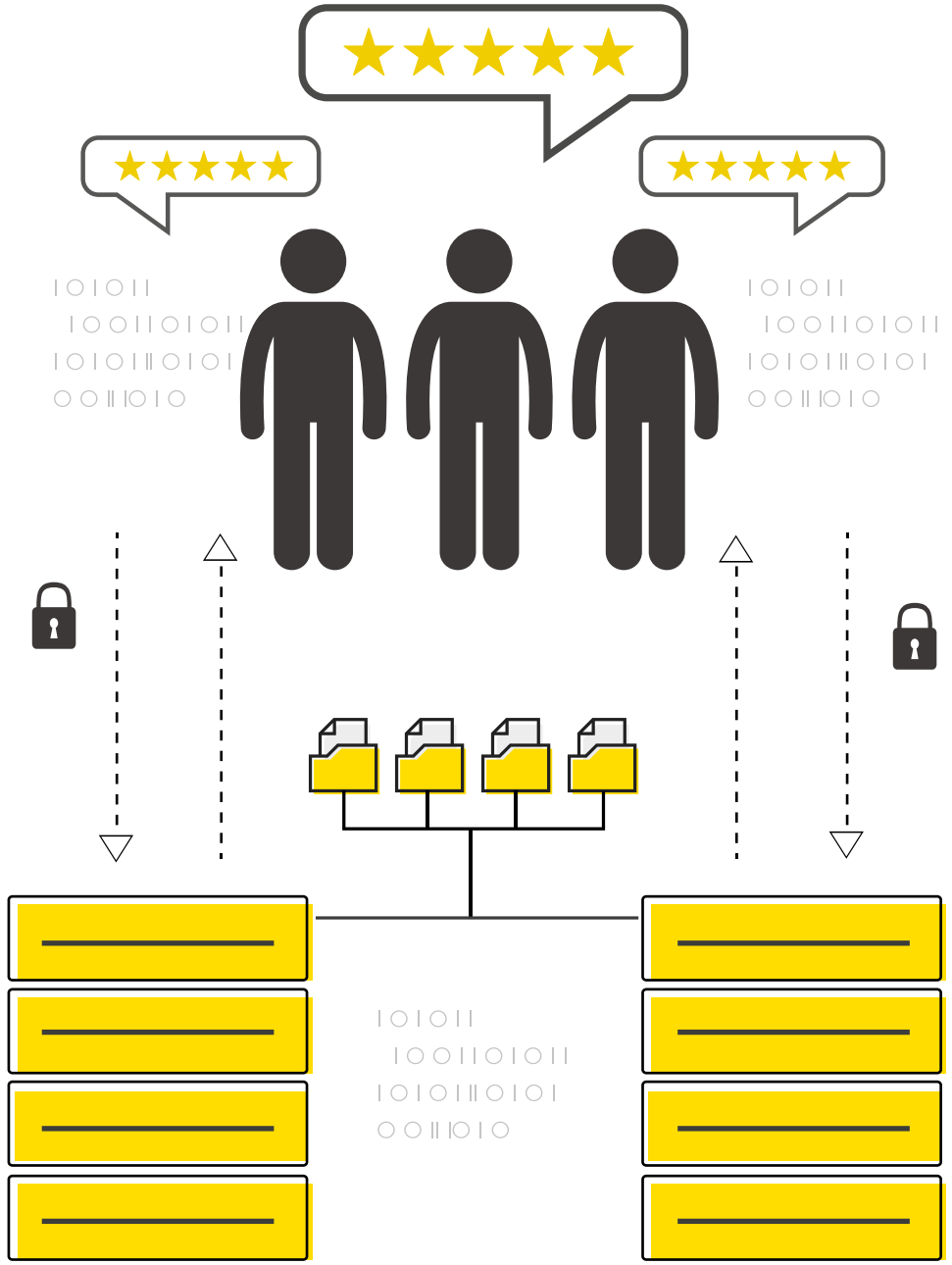
How will GDPR affect gathering customer feedback?

Understandably, the issue of collecting customer feedback raises a few questions when it comes to the new GDPR guidelines.

Does it count as marketing? Will you need to ask permission from every customer before you can send them a feedback request? Will GDPR make it harder to collect customer feedback?

We've been working closely with the Direct Marketing Association, the ICO and various legal representatives to understand where exactly reviews fit into the new guidelines and what this means for businesses who rely on customer feedback.

It's a business's responsibility to ensure that their data processors are up to scratch and compliant with GDPR. You'll want to review your contract with them to make sure that it contains the new conditions, outlined in Article 28. Your reviews provider will need to maintain a record of their processing operation and inform your business immediately if there are any data breaches.



Your questions answered...

Is customer feedback a form of marketing communication?

No, it falls under the heading of market research. Collecting feedback and reviews, demonstrates how consumers have rated their experience with your company, and so forms a normal and crucial part of the customer journey. Feedback is a way for businesses to understand how they can improve their customer service and provide better marketing communications in the future.

Does a business require consent to collect feedback from a customer?

No. As customer feedback is considered to be market research, you can contact a customer about a specific sale or service without consent as long as it is directly linked to that transaction. You can't then use that information to market to the customer in any way without gaining their consent.

Your reviews provider is the Data Processor and as long as they do not require a customer to log in or create an account in order to leave a review, you will not need to get your customers to opt-in in order to send a feedback request.

What else will you need to do to keep the feedback flowing?

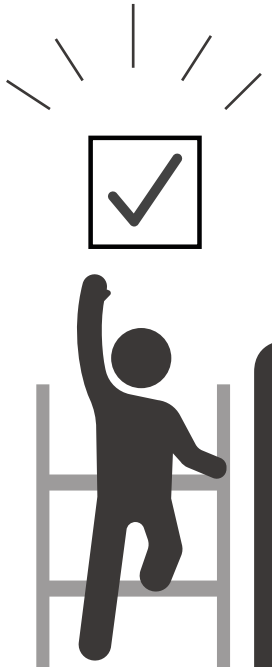
GDPR is not here to ruin the world of customer reviews and you'll still be able to use feedback to improve your business and enhance the customer experience. You should be aware that some customers may question why they received a feedback request when they opted out of your marketing communications, and it's important that you respond to them accurately and quickly.

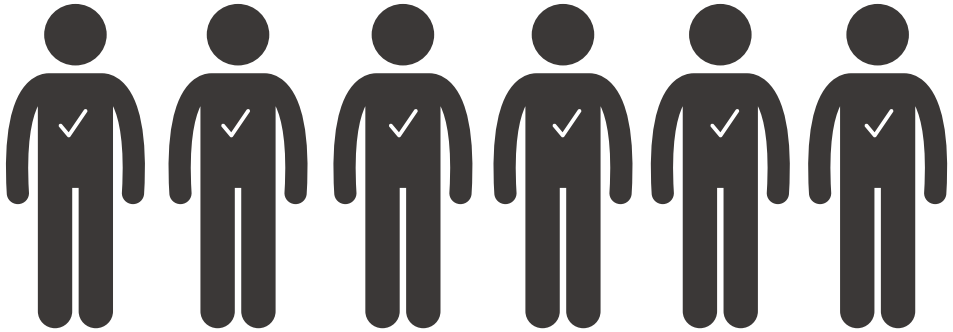
How to encourage your customers to opt in & stay in

The GDPR gives people far more control over their personal data. One of our most frequently asked questions, is 'how do you encourage individuals to give consent, and how do you create the type of rewarding relationship that will prevent them from opting out?'

More than 80% of customers want brands to get to know them and understand when to approach them and when to not

*Source: Marketing Dive





Top tips to follow...

- **Be honest and open**
  Why do you want it? How will you use it? How will you protect it?
- **No more sneaky tactics**
  Goodbye to pre-ticked boxes and lengthy Ts and Cs.
- **Make sure it's worth their while**
  Personalised experiences. Tailored content. Exclusive news and offers.
- **Keep it interesting**
  Use your insight to deliver the right information to the right people at the right time.
- **Meet expectations**
  If you promise something, make sure you deliver.
- **Let them control their experience**
  They say how. They say where. They say how much.

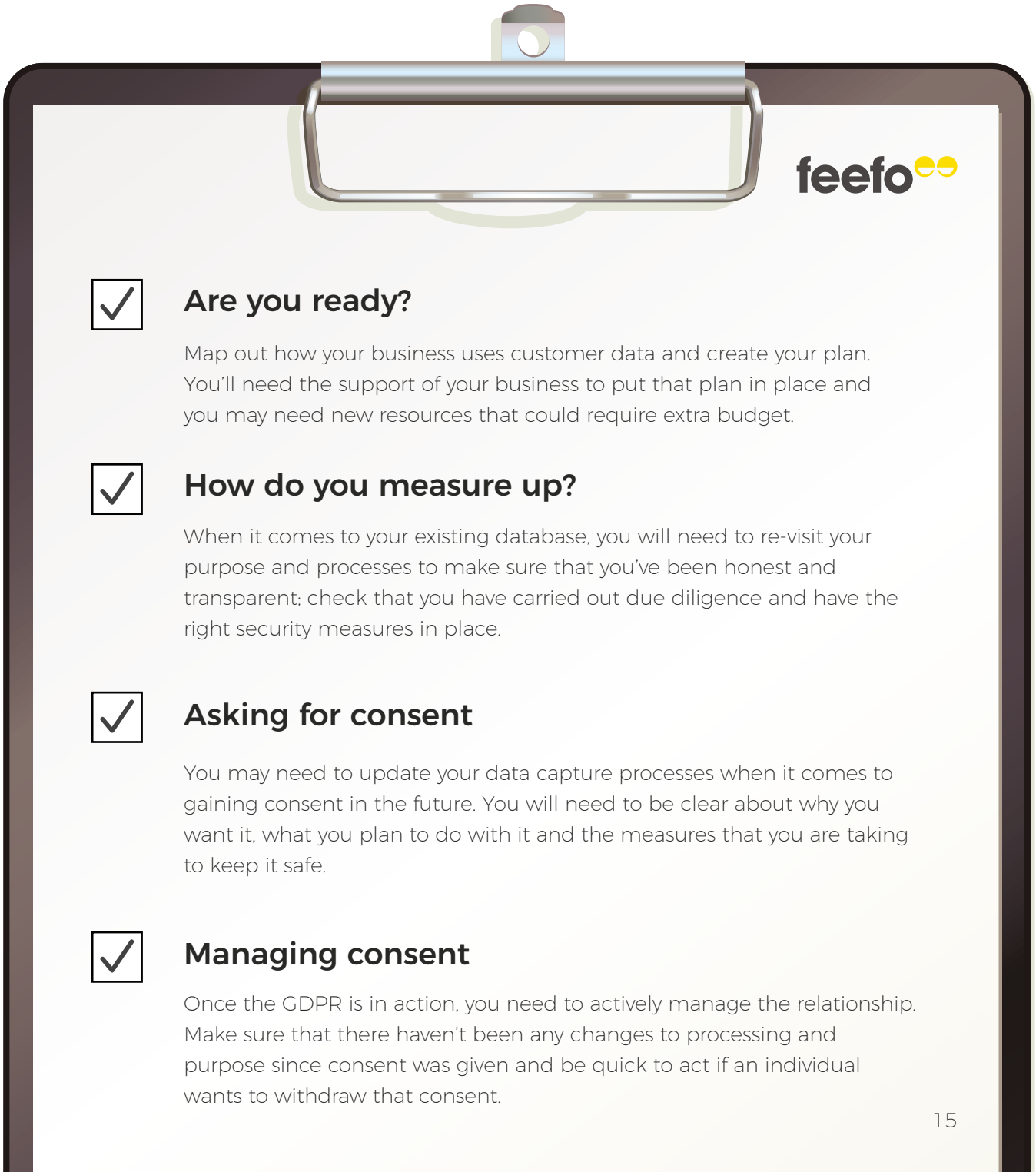
Our simple GDPR checklist

There are some questions that only you can answer, and depending on whether you're a Data Processor or Controller there will be specific standards that you have to meet. Here are the main checkpoints on the road to becoming GDPR compliant.

click here to read the full GDRP Checklist

We've put together a handy checklist that guides you through some of the questions you should be asking of your business to make sure that you are GDPR friendly.

Be aware, our GDPR compliance checklist is based on the most up-to-date GDPR information available, but is subject to change. It is not a substitute for legal advice. We recommend that every business seeks their own legal consultation to make sure their specific practices are compliant with the new legislation.



feefo

Are you ready?

Map out how your business uses customer data and create your plan. You'll need the support of your business to put that plan in place and you may need new resources that could require extra budget.

How do you measure up?

When it comes to your existing database, you will need to re-visit your purpose and processes to make sure that you've been honest and transparent; check that you have carried out due diligence and have the right security measures in place.

Asking for consent

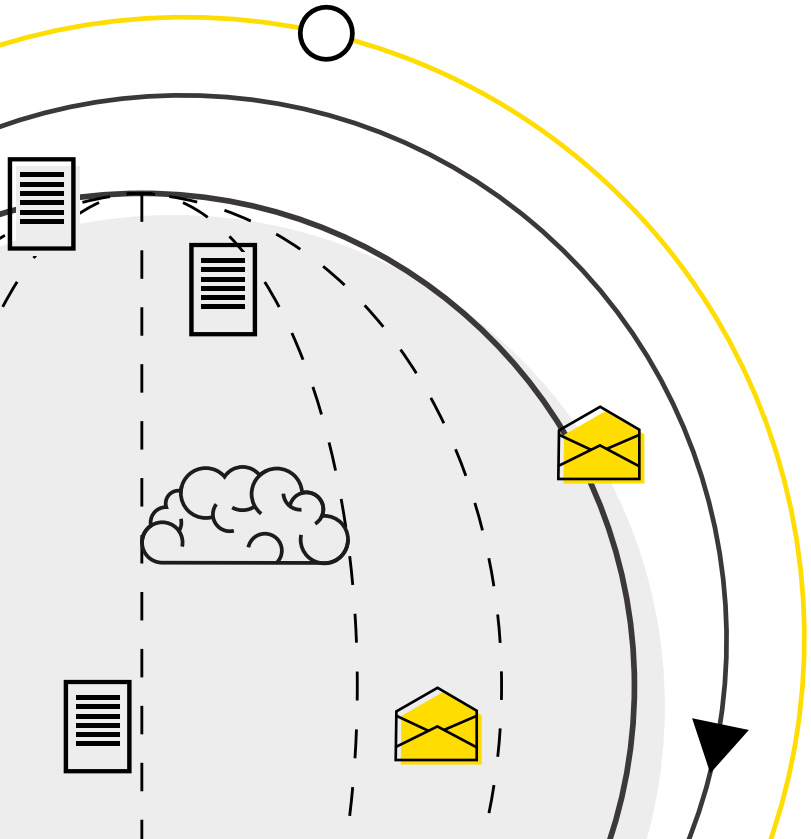
You may need to update your data capture processes when it comes to gaining consent in the future. You will need to be clear about why you want it, what you plan to do with it and the measures that you are taking to keep it safe.

Managing consent

Once the GDPR is in action, you need to actively manage the relationship. Make sure that there haven't been any changes to processing and purpose since consent was given and be quick to act if an individual wants to withdraw that consent.

Your top questions answered...

Here are the most frequently asked questions that are coming through to Feefo headquarters.



Are reviews covered by my general marketing information opt-in?

A big part of the GDPR is about being open and transparent with customers and clients, and it is important that you are clear about the possible ways in which you may use their data. You don't need an opt-in to gather feedback, but you should make sure that your customers are aware of your intentions to do so in your terms and conditions.

Are customers automatically opted in with Feefo, and is this compliant?

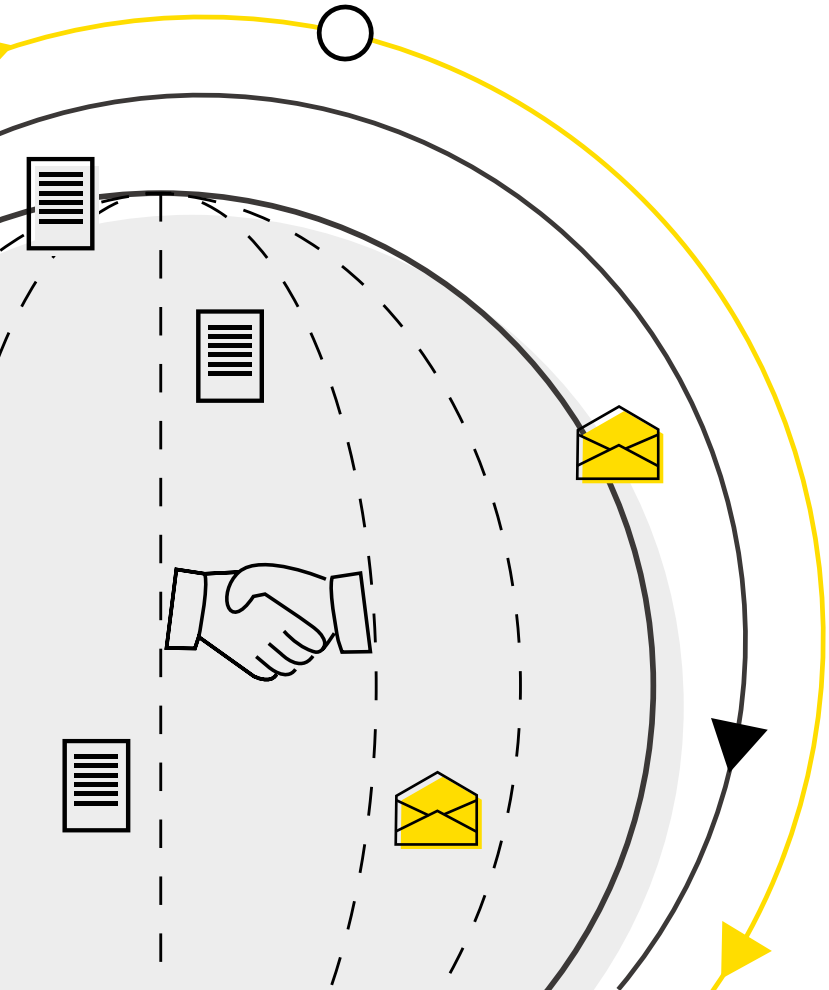
We act as a data processor on behalf of your business. It is important for you to conduct market research to gather feedback, better understand the customers who buy from you and improve the service that you provide for them. If a customer has been made aware of your intention to seek feedback in your terms and conditions, then we can invite them to leave a review, This is the only instance in which we can use their data. If we wanted to remarket to these individuals, we would have to seek our own consent to seek our own consent.

Does GDPR prevent sharing photo and video reviews on social media?

If a customer chooses to upload photos or a video review instead of, or as well as, a review you have requested for market research purposes, then it acts as consent in the same way as if they uploaded content to a social channel. It's fine to share it, but it must be used for the purpose it was intended for; you can't use it to remarket to or retarget them in any way and you must be quick to react should they request for the review to be taken down.

Your top questions answered

continued...



Are there any current practices e.g. retargeted marketing, that are non-compliant?

The GDPR isn't designed to outlaw specific marketing practices; it is about returning control of personal data to the consumer. The days of pre-ticked consent boxes and unwittingly dropping cookies on visitors to your site without consent are over. If you want to use an individual's personal data to market to them, you must clearly ask for their permission, outlining exactly how you intend to use it.

If a customer buys a product, are we allowed to send a feedback request without speaking to them?

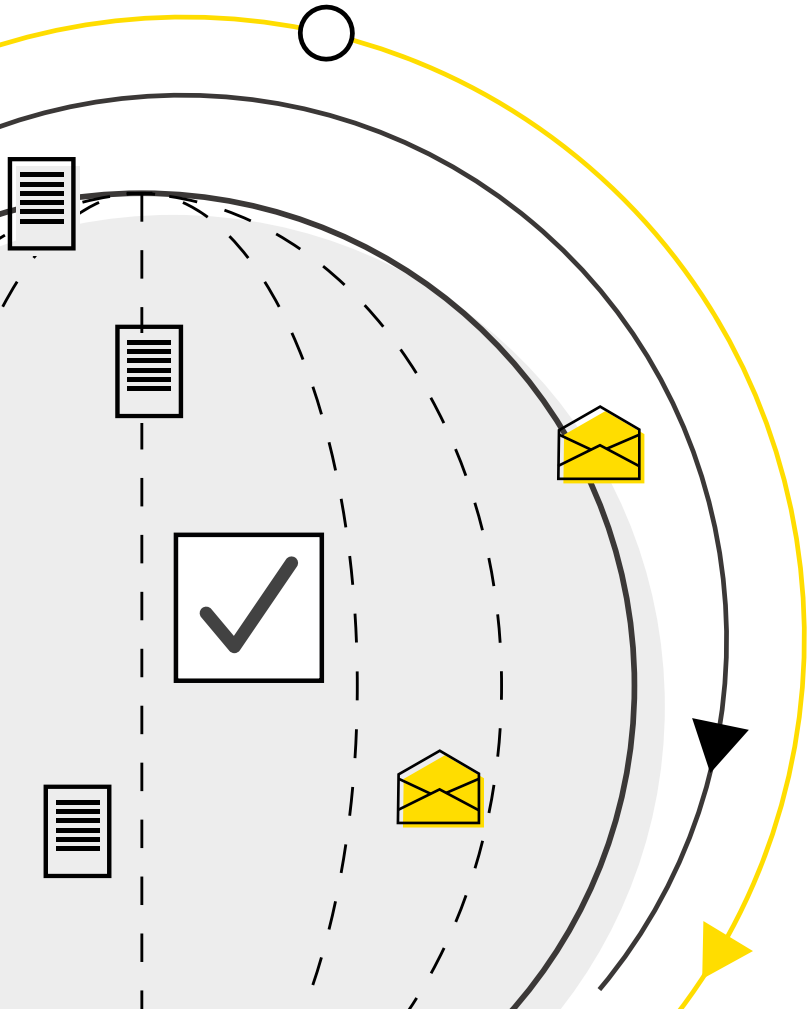
If a customer has given their details as part of a transaction, you can contact them, but it should be directly related to that specific transaction (i.e. a product recall, order fulfilment etc). A feedback request falls under the remit of market research, and while it is acceptable to send a feedback request following a purchase or customer service experience, you can't use that data for remarketing or retargeting unless specifically requested.

How should we update our terms and conditions to make our intentions clear to consumers?

Make sure that you have a section in your terms and conditions that explains that the customer may be contacted with a review request. It would also be advisable to include some messaging in your marketing collateral or in-store point of sale that references your work with a reviews company. By making your use of reviews a key part of your messaging, your customers will be more receptive to a review invitation and you could see a significant increase in your response rate.

Your top questions answered

continued...



Does GDPR impact the use of ecommerce software that sends Feefo data at the point of sale?

Capturing a customer's data for something like an e-receipt, is permitted because it is a necessary part of the purchase process. You can use this information to contact the customer as long as it is related to that specific sale. A review request is considered to be market research and is therefore permitted. You cannot use that data to remarket to the customer in any way without gaining specific consent to do so.

Will we have to contact everyone in our existing database to get fresh consent?

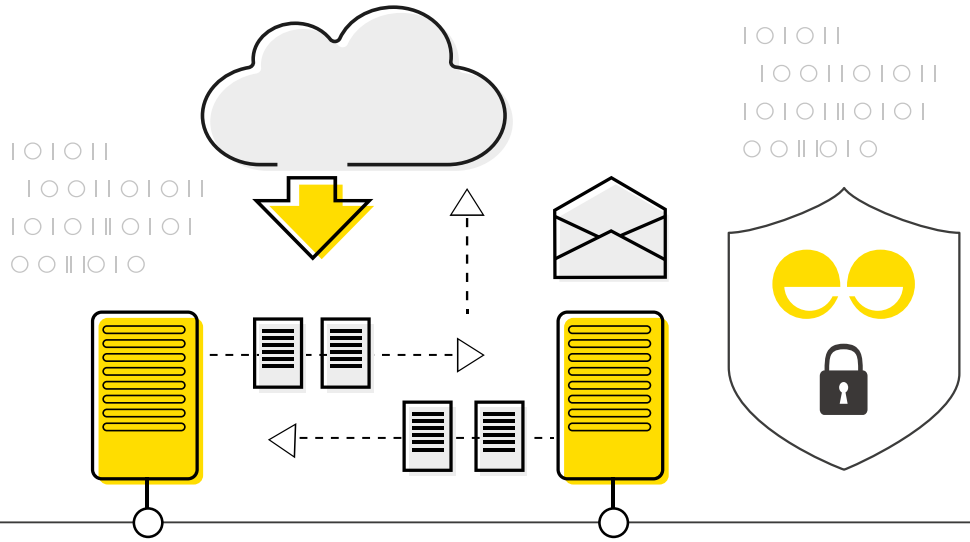
This will depend on how you acquired the customer data in the first place and the quality of the data that you obtained. Check out our **Basic GDPR Checklist** for some of the questions that you need to ask yourself to work out if your existing data is compliant. If you can prove that you were clear about how you intended to use the data and that your customers chose to share their data with you, then you should not need to contact them again. If your previous data capture processes do not meet GDPR standards, then you may need to contact the members of your current database and ask for consent.

How long will Feefo hold the data for?

Feefo holds very little personal data. We can securely keep the review and associated data indefinitely, but only for the purpose of replying to a customer in the event of a Subject Access Request (SAR). The review will be available for as long as you would like it to be used, although if a customer decides to exercise the Right for Erasure (right to be forgotten), all data will be deleted within 24 hours.

Feefo and GDPR

At Feefo, we have always gone to great lengths to ensure high data protection standards, but we are taking the opportunity to raise those standards even higher.



You can trust us

Trust is at the heart of everything we do and we want the businesses that work with Feefo, to feel totally confident that their reviews provider is GDPR compliant.

Your Customer data is secure

The privacy and security of our clients' customer data is extremely important to us, All of our data is stored in the UK and we'll continue to review our processes to make sure they are always up-to-date with the latest legislations.

We will keep you updated

We will be updating our Data Privacy Policy and changing the terms that we issue to consumers with a review request. We will also be sending out an amendment to the Feefo terms.

thank you

We would like to thank our customers for their questions. It's great to know that everyone is working so hard to become compliant and we have enjoyed sharing some of the insight that we've picked up on our own journey.

We would also like to thank the Direct Marketing Association, for their guidance and support.

The Feefo Team

Fancy a chat?

To find out more about Feefo, get in touch and our friendly team will be happy to help.

Sales@feefo.com | www.feefo.com

UK: +44 203 362 4209
US: +1 617 861 0611
Australia: +617 5406 1249

feefo