

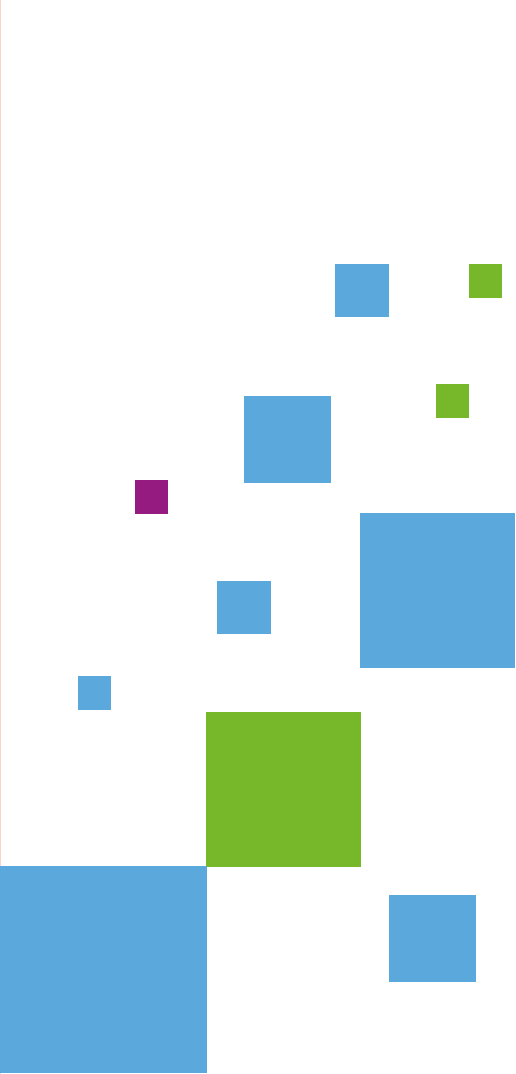


# FIVE STEPS TO COMPLIANCE

---

**GDPR:** KEY CONSIDERATIONS  
FOR CUSTOMER SERVICE TEAMS





Unless you've been living a life of blissful regulatory-ignorance, you will have heard of the impending General Data Protection Regulation (GDPR). The new regulation requires businesses to gain the customer's consent before they can capture, store or process any personal data or information from them. GDPR also allows the user to change their consent status at any time, giving them the right to demand to be removed from a database.



Despite the UK's decision to leave the European Union, British businesses will be required to comply with the EU directive when it is implemented in May 2018. The new standard replaces the existing Data Protection Act (DPA) and promises to enforce tougher punishments for businesses that fail to comply with the rules on storing and handling personal data.

The DPA was introduced in the early 1990s, when only a handful of large businesses had the ability to collect and store significant amounts of customer data. Today, thanks to the simplicity of data collection and the accessibility of data acquisition technology, every Tom, Dick and Harry has access to their own extensive customer database.

During the run-up to GDPR, there's been plenty of scaremongering to highlight the potential consequences of failing to comply. Businesses have been threatened with fines of up to €20 million for non-compliance, or four per cent of the company's worldwide annual turnover — whichever figure happens to be higher.

While we're all aware of the significant penalties of non-compliance, there is a lack of information on how businesses can ensure they comply in the first place. Moreover, there is ambiguity on which businesses and industry sectors are affected by these regulations.





## ..... Why should I care?

It's simple. GDPR affects any organisation that handles personal data. There is no avoiding the impending regulations, and because of the nature of the rules, pretty much every business will be affected in some way. However, for customer service teams, the relevance of GDPR is obvious.

Up until now, hordes of customers have voluntarily signed up to customer database lists, approving the use of their data during lengthy terms and conditions fields that — let's be honest — they haven't bothered to read. As consumers, this negligent approach to protecting our own data has enabled businesses to use data in any way they please, but thanks to GDPR, customers are regaining power.

We aren't suggesting that all customer service departments use data to spam their customers with unwanted sales material. In fact, in the customer service realm, data is usually used to simplify and streamline the customer service process. For example, if a customer was to raise an enquiry with an ecommerce website about a delivery, the contact centre agent could access their data to find their order history, chosen delivery method and any dispatch details related to the order.

However, outside of this innocent method of using personal data for customer service, many highly profitable, but somewhat dubious, business models have been built on access to data.

Consumer data is used in an array of business activity, from sales and marketing to market research and customer service. However, regardless of how your organisation uses customer data, preparations need to be made in advance of the GDPR's implementation in May 2018.

## So, who is responsible for making these preparations?




.....  
You're already a data controller

If you've done any research into the GDPR rules you will have probably stumbled across the phrase 'data controller'. But, what exactly does that mean?

According to the GDPR, a data controller is a person who determines what, why and how data can be collected. Basically, if you collect customer data — whether it is to update a customer relationship management (CRM) system or for prospect detection purposes — you become a data controller.

On the flipside of this coin is the data subject. This phrase describes an individual who can be identified through the information collected about them — which can refer to everything from their name or location, to an online identifier such as their IP address. In other words, your customers are the data subjects.



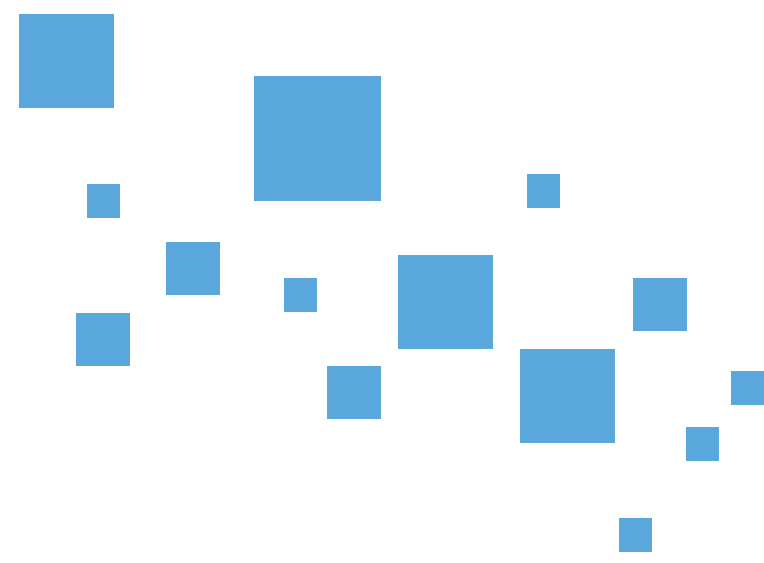
As a data controller, you need to be aware of the potential data touch points you use during your customer service process. By understanding how data is collected in your organisation, you can ensure it is collected lawfully.

All businesses will have different touch points. These include incoming emails, social media channels, live chat applications, reverse IP lookup or cookies on the company's website. For users of [Parker Software's WhosOn, an enterprise live chat solution](#), for example, touch points include pre-chat survey forms, form field capture, prospect detection, in-chat data exchanges and data population.

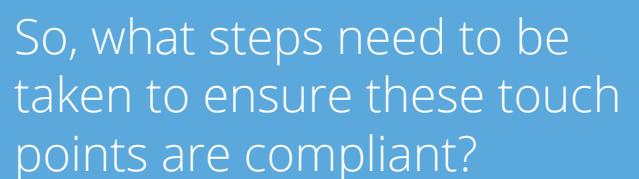
For customer service departments, touch points can refer to any part of the customer service process that collects data. For example, if a customer were to call the contact centre of an ecommerce retailer, it is essential that the contact centre agent takes the customer's details to complete the transaction. However, if the contact centre plans to store this data, the company's privacy policy must be made clear to the customer over the phone.



.....  
Careful where you touch



Similarly, if a customer was to begin a live chat discussion with a business on their website, they need to be given the opportunity to decide whether they are happy for the company to acquire their personal data from the chat. A business's privacy policy should explain exactly how the business does this and, importantly, how that data will be used.



So, what steps need to be taken to ensure these touch points are compliant?



.....  
Time for a re-write

To comply with GDPR, it is vital that you have a comprehensive privacy policy. This policy needs to cover key company details including: the name and nature of the business, what kind of data you will collect, where the information will be kept and importantly, how the customer can get in touch if they would like to remove their data from the system.

Re-writing an existing privacy policy may seem like a tedious task, but if your existing privacy policy doesn't fit the new regulations, you will have to do the work to comply. There are plenty of helpful resources online to help you get this right. Once the GDPR-compliant policy is completed, it can be used to gain consent from customers to use their data. The easiest way to do this is to add a permission checkbox on your website, or at any other data touch point.

GDPR makes it clear that as all customer data must be collected legally, it must also be stored legally. Data controllers are also responsible for this.

For customer service teams that use the cloud to store data, it is vital to take security into consideration. Choosing a high security datacentre in an EU-approved country should ensure this. Alternatively, organisations can use on-premises storage. In these instances, businesses should take steps to protect this data from internal errors or external security threats. Implementing passwords, using firewalls and using data encryption are all ways to improve security.



# The new rules surrounding data protection are a lot to take in, but the GDPR is not optional.

The current DPA regulation is enforced by the Information Commissioners Office (ICO). Currently, the ICO has several options to take when it finds an organisation is breaching the rules. There are fines of up to £500,000 for serious breaches of the DPA and potential prison sentences for those companies that are intentionally breaching the DPA or choosing to ignore the rules. However, when GDPR is enforced in May 2018, the fines businesses face will increase dramatically.

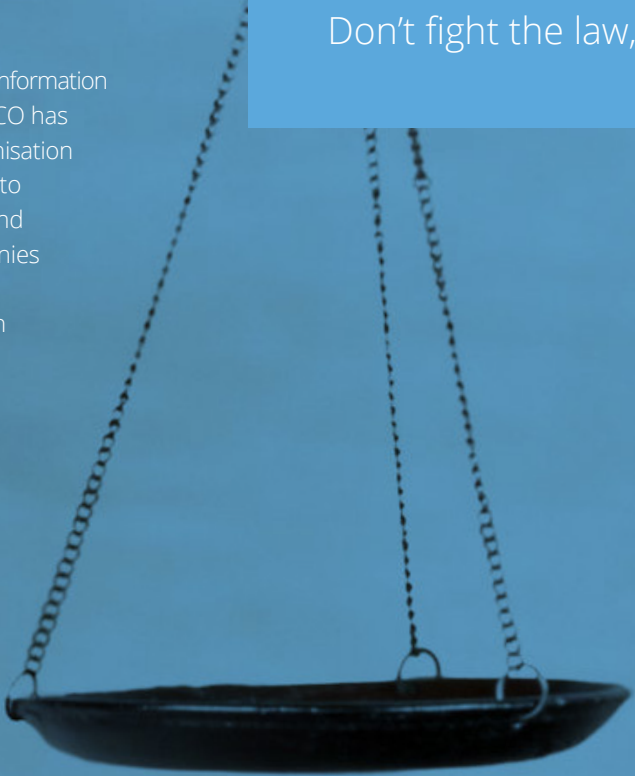
Under GDPR rules, penalties can reach an upper limit of €20 million. For larger businesses, to which a €20 million would not be as detrimental, the regulation could present a penalty of 4 per cent of the company's annual turnover.

The new regulation is also taking a tougher approach to data security than its predecessor. Data controllers are subject to Article 32 obligations, which require organisations to “implement appropriate technical and organisational measures to ensure a level of security is appropriate to the risk.” Failure to do so can result in fines of up to €10 million, or two per cent of the company's annual turnover.

Businesses that have already begun making efforts to ensure they comply with GDPR will be familiar with the lengthy plans, audits, research — and looks of exhaustion on the company's GDPR taskforce — as the implementation date looms.

GDPR seems scary, but it may not be as intimidating as some businesses believe. In fact, it may just be a blessing in disguise, particularly for the customer service realm.

.....  
Don't fight the law, it'll win





.....  
A blessing in disguise?

It is estimated that 60 to 80 per cent of data that organisations are storing could be completely redundant, obsolete and trivial. GDPR compliance is a big task, but it will force you to audit, review and organise your data — an area that's usually a chaotic realm. In fact, GDPR could provide the perfect opportunity for a spring clean.

Maintaining a tidy dataset is hard work and for most customer service departments, the concept of a clean, streamlined data management system is a thing of fantasy. Achieving this is a colossal task, so it's no surprise that it is so regularly avoided. These new regulations mean it is the law to keep things in order, so it can't be put off anymore.

Until now, there hasn't been a unified set of guidelines for companies to adhere to regarding data management. GDPR puts an end to this disorder. When there is uniform legislation in place, it becomes much easier to understand how to sort and manage data in an organised way.

GDPR forces businesses to better understand their data. It requires a comprehensive revision of data handling procedures and provides an opportunity to categorise, clarify and correct data problems. In doing so, businesses can be more informed, more efficient and, ultimately, deliver better service to their customers.

Plus, if the penalties of non-compliance aren't enough motivation to get this data in order, we don't know what is.

## ..... Five steps to compliance

There's no shortage of information on the GDPR guidelines on the internet and in the media, but with the introduction of the regulation getting closer, it's time to take real steps to get your data in order, before May 2018. Here are our five steps to compliance.

### Step one Take it to the boardroom



Having heard of GDPR is one thing, but actually complying with the regulation is an entirely different game. You might understand the implications of failing to comply with GDPR, but are the decision makers and key people in your organisation aware that the law is changing? You might be surprised.

Unfortunately, future regulations are often seen as just that — a problem for the future. GDPR implementation in May 2018 is more than just an introduction to the new regulation: this is the date it is legally implemented. If you're unsure whether your business is taking steps to compliance, speak up now. Your bosses will thank you in the future.

## Step two

Delve into your data



We've already established that data records can be messy, for small and large businesses alike. Often, personal data for marketing activity will be held separately to customer service records, lists of personal data may have been purchased from a multitude of different sources and missing fields in some datasets can result in a chaotic attempt at organisation.

Assessing your records can seem like a mammoth task, but it is non-negotiable. Understanding the data that you hold takes an investment of time and resources. Where did the data come from? Who in the organisation has access to it? And, perhaps most importantly, do you have the right to hold it?

It may be tempting to avoid this data cleanse, but in doing so, you're only delaying the impending consequences of failure to comply.

## Step three

Don't be ashamed of surrender

Faced with the task of organising hordes of data, there may be a temptation to deny all knowledge of this unlawful information, in the simple hope that you won't get caught out. Please, don't take the risk.

GDPR is not designed as a money-making scheme. It is designed to protect personal data and there are several schemes in place to help you do just that. If you're struggling to be compliant, ask for assistance before it is too late.



## Step four

Make changes, immediately



Some organisations may need to appoint a data protection officer to ensure GDPR compliance. Legally, an official data protection officer is only required when the data is held by a public authority, or if the organisation is undertaking regular monitoring of data on a particularly large scale. The only other exception is when companies manage data related to 'sensitive' categories, such as criminal convictions or offences.

Currently, there's a high demand for data protection officers – with organisations across the country racing to address new requirements. However, for most businesses in the customer service realm, appointing one is not enforced by law.

That's not to suggest that businesses in the sector shouldn't consider the advantages of appointing an expert. The new appointment doesn't necessarily need to be a data protection officer — just a dedicated member of staff to ensure the company complies, and continues to comply, with GDPR.

Alternatively, if hiring new staff is out of the question, it would be worth investing in training for existing staff.

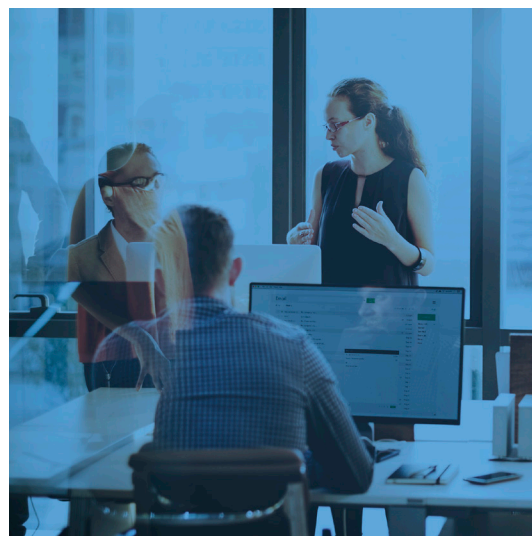
If your methods for data collection and the procedures associated with your data touch points don't meet GDPR regulation, you need to make the appropriate changes now. Legally, these changes don't need to be implemented until May 2018, but there is absolutely no benefit in waiting until then.

Updating your procedures now will ensure that all incoming data is compliant, giving you until May 2018 to review and correct your datasets. Failing to act now won't avoid the issue, but it will leave you with a colossal chore to begin (and complete) in May.

It is advisable to familiarise yourself with the ICO's code of practice on Privacy Impact Assessments. As well as the latest guidance from the Article 29 Working Part, this can guide you on how and when to implement them in your organisation.

## Step five

Appoint an expert





.....  
Ready, set, comply?

You've already invested some time to read this whitepaper, so at least you're taking some steps to understand GDPR. Preparing for and complying with these new rules is not easy, so good on you for trying to be prepared.

When spring comes around, you want to be ready and, more importantly, you want to stay ready. There are several digital tools you can use to ensure you remain compliant after the implementation date and, for users of Parker Software's WhosOn, compliance is simple.

Parker Software can help you to ensure your use of [WhosOn is fully GDPR compliant](#). The company has security and policy experts in-house and is happy to help ensure your procedures are watertight.

We're ready. Are you?