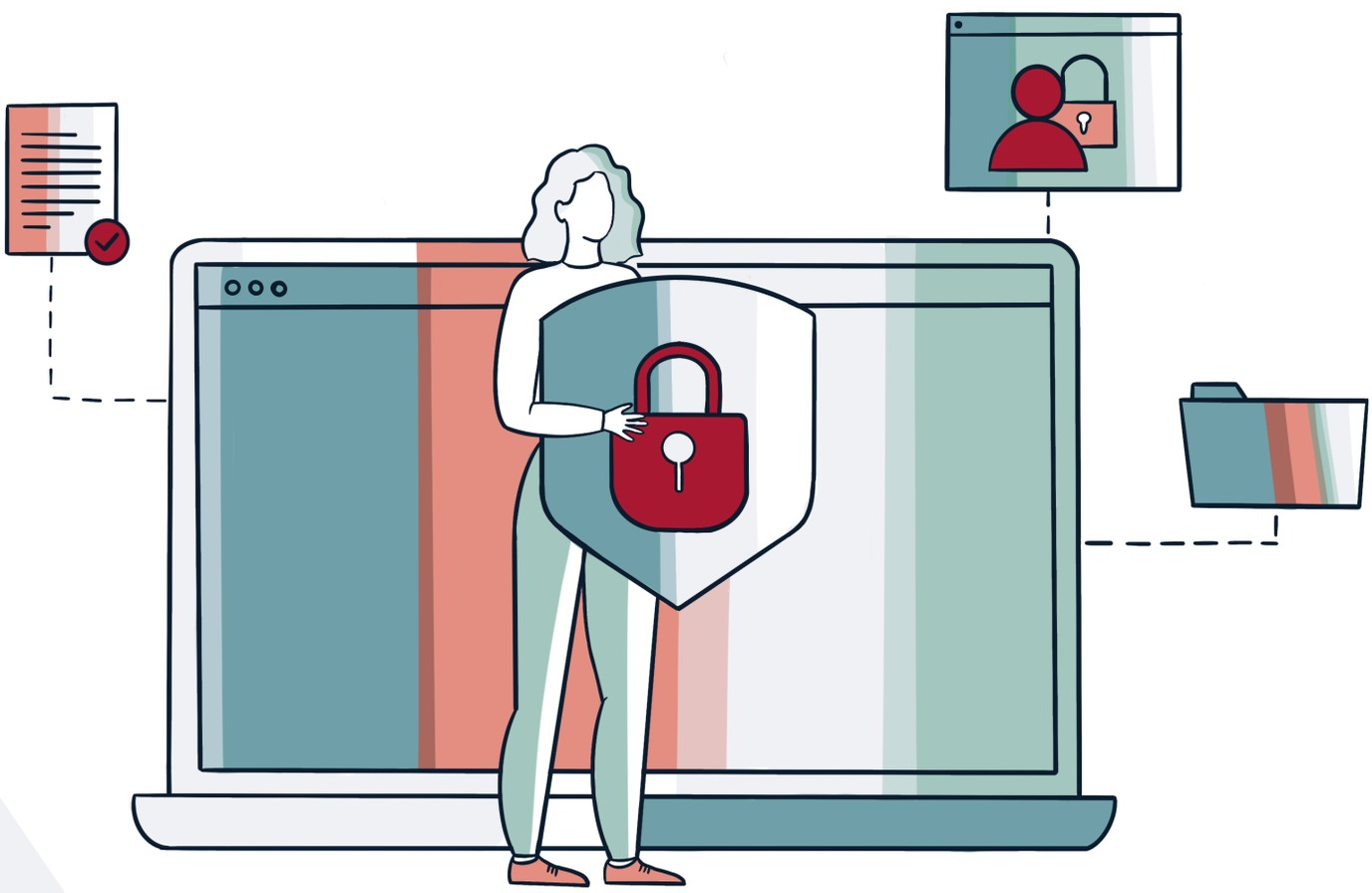
Source™

A GUIDE TO GDPR

Read time: 5 mins



Hello,

GDPR can seem like a never ending task to overcome, however, in spite of what many other people say, GDPR doesn't need to be a daunting topic for you and your business.

This eBook has been put together to help highlight some of the most important aspects of UK GDPR and how to apply these regulations to your everyday role.

This eBook is brought to you by

Phil Lewis
Head of HR and Compliance

Connect on LinkedIn
Click here

THE WORLD IN 1998

It was the year that both Windows98 and Google were launched. The biggest films of the year were Titanic, Armageddon and, a personal favourite of mine, There's Something About Mary. Perhaps unsurprisingly, the top hits included I Don't Want to Miss a Thing by Aerosmith, My Heart Will Go On by Celine Dion, and Viva Forever by The Spice Girls.

Aside from the pop culture trends, a lot has changed in the last three decades. There was no broadband internet in 1998. In fact, only 9% of households in the UK had internet access in 1998. By way of comparison, as of 2020, that figure stands at 96%.

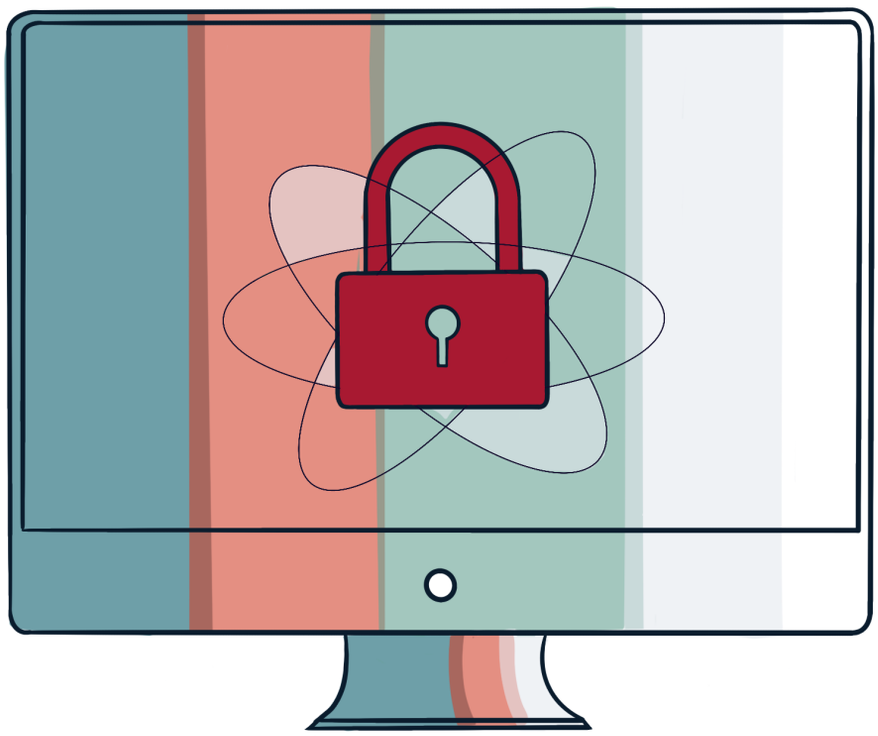
View stats **here.**

Social media was non-existent; no Facebook, Twitter or Snapchat. Mobile phones were more like bricks, and could only be used to make actual phone calls (and potentially play Snake!).

This was the world that the Data Protection Act (DPA) was designed for.

The UK General Data Protection Regulations (UK GDPR) is a wholesale overhaul of the previous DPA. It was created to recognise the rise of the internet and the increased availability of email, both of which have had a massive impact on how companies use (and sometimes abuse) personal data. It is also worth noting that there is a sister piece of legislation, the Privacy and Electronic Communications Act (PECR), also known as the ePrivacy Regulations (ePR). This Act has been updated a number of times to take account of advances in technology.

You can find the most up to date information on the **ICO website.**



OVERVIEW:
REGULATORY HIGHLIGHTS

WHAT IS *personal* DATA?

Under UK GDPR, there is a new definition of 'Personal Data' which has a wider reach than the previous definition under the DPA. The new definition includes online identifiers such as IP addresses and website cookies, alongside more expected details such as names and addresses.

WHAT IS *sensitive* PERSONAL DATA?

Under UK GDPR, there are also categories of "Sensitive Personal Data", which can only be processed in limited circumstances. As a broker, you will need to be mindful that some of the information you collect will be considered "Sensitive Personal Data".

For example, if you are collecting information about medical conditions for insurance purposes or if you photocopy passports to satisfy KYC requirements (as passports contain racial/ethnic information, which is classified as Sensitive Personal Data). Extra safeguards apply to anybody processing sensitive personal data, so there are just a few extra steps you'll need to take in order to be fully compliant with UK GDPR.

WHO DOES GDPR APPLY TO?

GDPR applies to anyone dealing with client data. One of the first things to determine is whether you are a data controller or a data processor.

If you make decisions about how personal data is processed (for example, if you decide which insurers/platforms/lenders to send personal data to in order to get a quote, policy or mortgage), then it's likely that you will be a data controller. As a data controller, your obligation is to ensure your contracts with processors comply with the UK GDPR and you are not relieved of your obligations where a processor is involved.

A data processor acts on behalf of and under the instruction of a data controller. If this applies to you, the UK GDPR places specific responsibilities on you, such as maintaining records of the personal data and your processing activities.

You will have legal liability if you are responsible for a breach.

The ICO sets out the specifics **here.**

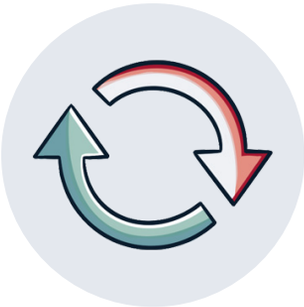
CONSUMER RIGHTS

THE RIGHT TO BE *informed*

The right to be given accurate information about how their data is used and why. This is what you should set out in your Privacy Policy.

THE RIGHT OF *access*

The right to access their own personal data at any time. For example, via a Subject Access Request (or SAR).

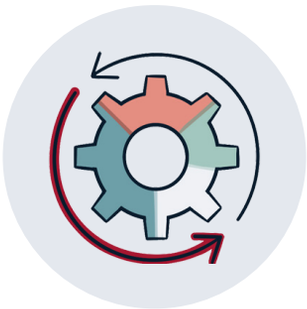


THE RIGHT TO *rectification*

The right to have any inaccurate or incomplete information rectified and updated. A client can request this verbally or in writing.

THE RIGHT TO *erasure*

The right to request to have their data deleted, if for a justifiable reason. You also have the right to refuse this if you have a justifiable reason, such as a legal obligation.

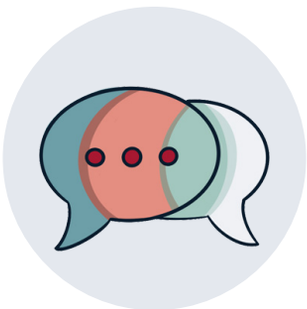


THE RIGHT TO RESTRICT *processing*

The right to restrict the processing of their data. In this instance, you may store your client's data, but not process it, unless you have their consent or a legal or public interest.

THE RIGHT TO DATA *portability*

The right to request their personal data in a structured and commonly used format. Your client can request their data be transferred to themselves, or directly to another controller.



THE RIGHT TO *object*

The right to object to the processing of their data. Your client can ask you to stop processing their data altogether or for a specific purpose, such as direct marketing.

RIGHTS IN RELATION TO AUTOMATED DECISION MAKING AND *profiling*

The right to not be subject to a decision, based solely on automated processing. For example, if your client was declined an insurance policy or mortgage based on an automated underwriting algorithm, they could request a manual review.

CONSUMER RIGHTS

In most instances you have 30 days to process a client's request, under each of these rights.

GDPR has updated people's rights to be more reflective of the fact that personal data is, generally speaking, kept in electronic formats these days. Some of these rights, such as the 'right to be forgotten' and the 'right to data portability', are explicit acknowledgements that personal data 'belongs' to the subject of that data, and so they should have an active say in who uses it and how.

One of the other big changes that came along with GDPR (and the ePR), is around consent. Under the DPA, pre-ticked boxes to give consent were allowed, and as such many people's inboxes are regularly filled up with marketing emails. Under UK GDPR, consent must be "freely given, specific, informed and unambiguous". This means that pre-ticked boxes or implicit consent will no longer be allowed, and people will have to actively choose to provide consent for their personal data to be processed.

Additionally, consent can be withdrawn at any time, so it is important that clear and flexible records of consent are maintained, in order to allow people to withdraw their consent at any point after it has been given.

Read in further detail here.

PENALTIES FOR NON COMPLIANCE

Failure to comply with the UK GDPR principles will leave you open to the highest tier of administrative fine - up to 20 million euros or 4% of your annual global turnover, whichever is higher. It's vital that you are up to date with legislation and your regulatory requirements, not only to provide your clients with the best service, but also to avoid the fines associated with non-compliance breaches.

3 TOP TIPS FOR BROKERS

DO YOUR *research*

The ICO's website is an adequate source of information for all brokers looking to remain compliant with UK GDPR. It's a little dry, which is not surprising given the subject matter, but it is very helpful and the whole GDPR section could be read in just a few hours.

Go to the ICO's website >

ADHERE TO A *checklist*

Use the GDPR checklist which is available (for free) on the ICO website. It will help you to target the areas which require your attention in order to be compliant.

Download your relevant ICO checklist >

EDUCATE YOUR *staff*

Under CPD requirements, brokers must have necessary knowledge of regulations. Use this as an opportunity to ensure your staff are up to date on the latest UK GDPR requirements, whilst helping towards achieving their overall CPD goal.

Complete our GDPR LearningLab module >

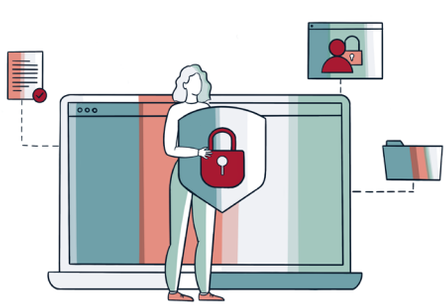
RSM SUPPORT

Here at Source, we have dedicated Regional Sales Managers (RSMs) covering all areas of the UK, to offer you the support you need with General Insurance (GI). After reading this guide we hope you now have a good idea of the necessary requirements for your business and the confidence to apply the regulations to your role.

If you have any queries please contact your RSM, who will be happy to discuss this further with you, and provide practical examples and advice.

You can arrange an appointment by calling one of our team on **02920 265 265** today.

Finally, if you are aware of other intermediaries who may find this information useful, feel free to share this eBook with them!



Your General Insurance Experts