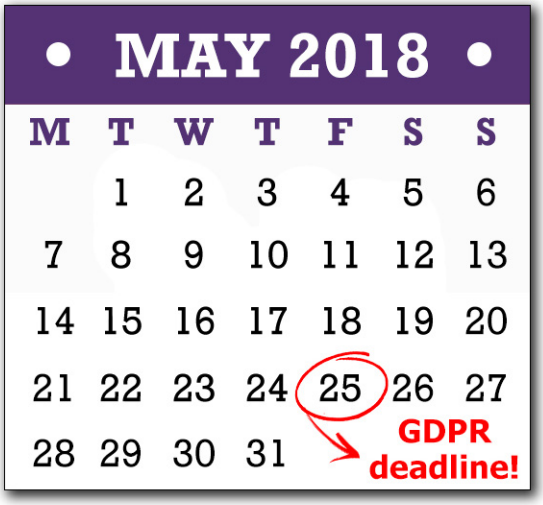
Crystal
Specialist Finance

The Mortgage Broker's Guide to GDPR.

The data privacy laws are changing - **get prepared!**



An introduction to the GDPR

Hopefully by now you have heard of the **General Data Protection Regulation (GDPR)** which is due to come into effect on **25th May 2018**. It will change the way all UK businesses have to handle client data (by demanding more accountability on how they use personal data), and it is very important that you understand how it will affect your business and what your responsibilities are.

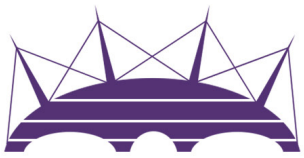
Your legal obligations and responsibilities on how you collect, record and also administrate your customers' data are changing. All UK businesses that hold client data will have to comply with the new regulations, which replace the **Data Protection Act 1998**. Non-compliance and data breaches will be monitored by the **Information Commissioner's Office (ICO)** and penalised with substantial fines.

There is a lot of preparation needed, so please do not leave this until the last minute!

Our guide aims to help you understand what you need to do by outlining:

- the main points of the new legislation
- how you can start planning
- the areas you may need to consider

The world in 1998...



Construction begins on the Millennium Dome.

DVD format is released to the UK market. Jumanji is among the first set of titles released.

Ford Focus is launched in the UK market.

Google and Windows '98 are both launched.

David Beckham is sent off against Argentina and Michael Owen scored his famous goal.

'Baby One More Time' by Britney Spears is released and 'Believe' by Cher is the UK's biggest selling single.

Europeans agree on a single currency - the Euro.

UK hosted the Eurovision Song contest (with Israel taking the winners' crown).

The Harry Potter and the Chamber of Secrets book is released.

We watched Godzilla, Saving Private Ryan and Armageddon at the cinema.

All of the above events occurred during 1998, however perhaps more significantly, there was no broadband internet in 1998. In fact, only 9% of UK households had any internet access in 1998. By way of comparison, this figure now stands at 88% in 2017. Social media was non-existant, and mobile phones could only be used to make actual phone calls!

This was the world that the current Data Protection Act (DPA) 1998 was designed for.

The GDPR is the biggest overhaul to data protection in 20 years. Many of its main concepts are similar to those in the DPA, so if you are already complying with the current legislation then most of your processes will still be valid under the GDPR, and will be a good foundation to build on in order to comply with the new enhancements.

In relation to the advances in technology, it is also worth noting that the **Privacy and Electronic Communications Act (PECR)** is being updated to the **ePrivacy Regulations (ePR)** on the same day as the GDPR - **25th May 2018**.

What is the GDPR?

The General Data Protection Regulation (GDPR) will put individuals in control of their personal data, empowering them to choose how (and whether) businesses use their data. Where personal data is not treated correctly, individuals will have increased rights to legal recourse and can, in some instances, claim compensation. Regulators across the EU will have unprecedented power to enforce the legislation and impose hefty fines in instances of non-compliance.

It is not enough to simply understand the headline requirements of the GDPR. What is more important is understanding what the GDPR is intended to achieve and what the real risk issues are for your organisation.

Plan, Plan, Plan

If you haven't already, you need to put a plan together on how, who and when to implement the processes by which you collect, keep and use personal information.

Compliance with the GDPR is likely to require substantial changes to ensure that an individual's ("data subject's") personal data is processed in compliance with the GDPR requirements. You need to be aware that these changes may require a significant amount of time to implement.

HINT

Talk to your team to ensure that everyone is aware of the new legislation.

You should all clearly understand what preparations and measures are in place to ensure you will be GDPR compliant by 25th May 2018.

Regulatory highlights

What data is covered by the GDPR?

Personal data is covered by the GDPR. The GDPR has a new definition of **'personal data'**, which has a wider reach than the existing definition under the DPA. It is to be defined as:

"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."

Check what information you currently have for your clients and ensure that it is kept secure and up-to-date.

Personal data also applies to your business customers and employees, as well as your direct consumers. It includes:

- Personal details
- Family and lifestyle details
- Education and training
- Genetic, biometric and health data
- Online identifiers (IP addresses, cookies)
- Contractual details (i.e. goods and services provided to a data subject)
- Medical details
- Employment details
- Financial details

Assess how you are handling personal data and keep documented evidence that you have considered the risks of handling the data and how you have addressed these risks.

For example, use encrypted emails to pass personal data and limit the number of people within your business who can access such data.

What changes need to be made?

In a nutshell, there are a few key areas that businesses need to address to be GDPR compliant. The good news is that they are things that all businesses should be doing anyway:

Security

Your IT systems need to be secure – including laptops, tablets and mobile phones.

Encrypted backup

All personal data you hold must be encrypted and automatically backed up.

Partners & Suppliers

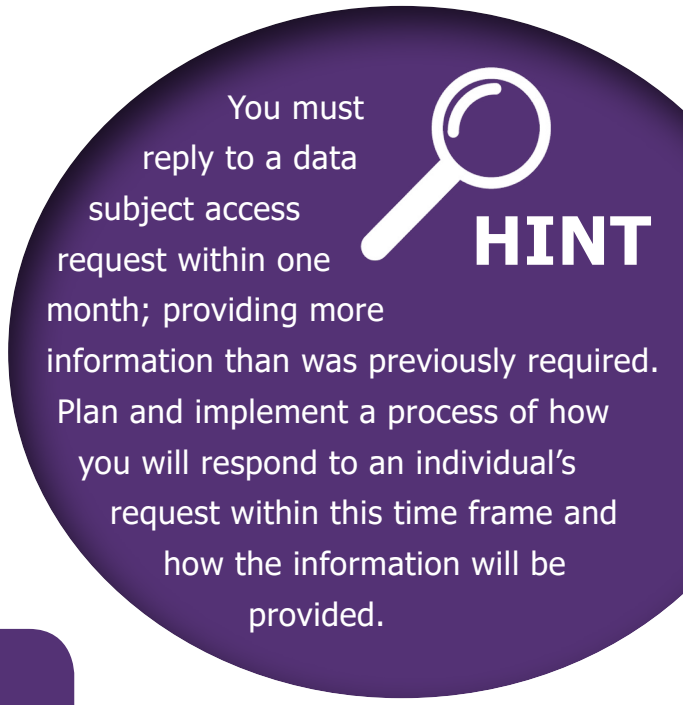
Check that your partners and suppliers are GDPR compliant and enable you to be as well.

Client access

If a client wants to see the information you hold on them, you must be able to provide it in a digital format that allows them to re-use it elsewhere.

Right to be erased

(Also known as the right to be forgotten). If a client wants to be deleted from your systems, you need to be able to sufficiently action this (subject to conditions), as they are withdrawing their consent to you holding their personal data.



Opt-in and consent

Opt-out will no longer be valid. People must give their informed and proactive consent to the processing of their personal data by choosing to opt-in. Boxes can no longer be pre-ticked in advance or confusing language used – you need to evidence that the customer has fully understood how their personal data will be used and stored.

Notification

The ICO, customers and staff need to be informed of any data breaches within 72 hours.

Cookies, privacy policies and T&Cs

All of these policy and procedure documents will also need updating. As well as the need to be clear to read and easy to understand, these documents must specify why information is needed, who it will be shared with and for what relevant and legitimate purposes.

Top 3 tips for brokers

Once the relevant systems and procedures are in place, you will need to ensure they stay up-to-date and that you have a secure system to handle data requests and recording your processing activities and any data breaches.

You can get more information from **www.ico.org.uk**.

1 Do you need to pay a GDPR expert?

The chances are, you won't need them. The Information Commissioner's Office website will be an adequate source of information to enable you to implement all of the necessary changes.

Visit the ICO website here

2 Adhere to a checklist

Use the free GDPR checklist which is available on the ICO website. It will help you to target the areas which require your attention to ensure you are fully compliant:

See the ICO checklist here

3 Train your staff

It is extremely important that you and your colleagues are aware of the imminent changes in the new legislation and can handle and process your clients' personal data correctly.

Penalties for non-compliance and data breaches

The maximum fine under the current DPA is £500,000, however this changes to 4% of global annual turnover or up to €20million.

Don't forget...

The GDPR implementation date is 25th May 2018.

Thank you for reading.

Find out more about Crystal Specialist Finance at
www.crystalsf.com

Unit A Ventura House, Ventura Park Road, Tamworth, Staffordshire, B78 3LZ

01827 301 070 ◆ www.crystalsf.com ◆ info@crystalsf.com
