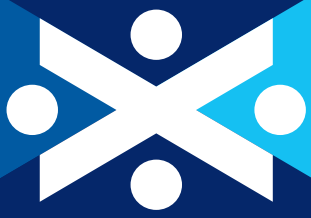
COMMERCIAL BANKING

READY, STEADY, GO

Are you prepared for the General Data Protection Regulation (GDPR)?

March 2018



BANK OF SCOTLAND

Table of Contents

Introduction to GDPR

The General Data Protection Regulation (GDPR) is an opportunity for every organisation to embrace the changes that give individuals' more control and rights over their personal data.

Safeguarding the personal data of our customers and colleagues is a priority for Bank of Scotland and we welcome the measures introduced through GDPR, and encourage our customers' partners to take action too.

The new Regulation is receiving a lot of attention. If your business works with personal data, then you need to make sure you are GDPR ready by the time it becomes enforceable on 25th May 2018.

Compliance involves a lot of planning and preparation. We cannot tell you how to be GDPR compliant. However, we hope that this booklet helps you understand:

- Some of the steps you can take
- What to look out for and what you may like to consider
- A few simple things to get you started

The clock is ticking. GDPR will be here in no time.

What is GDPR about?

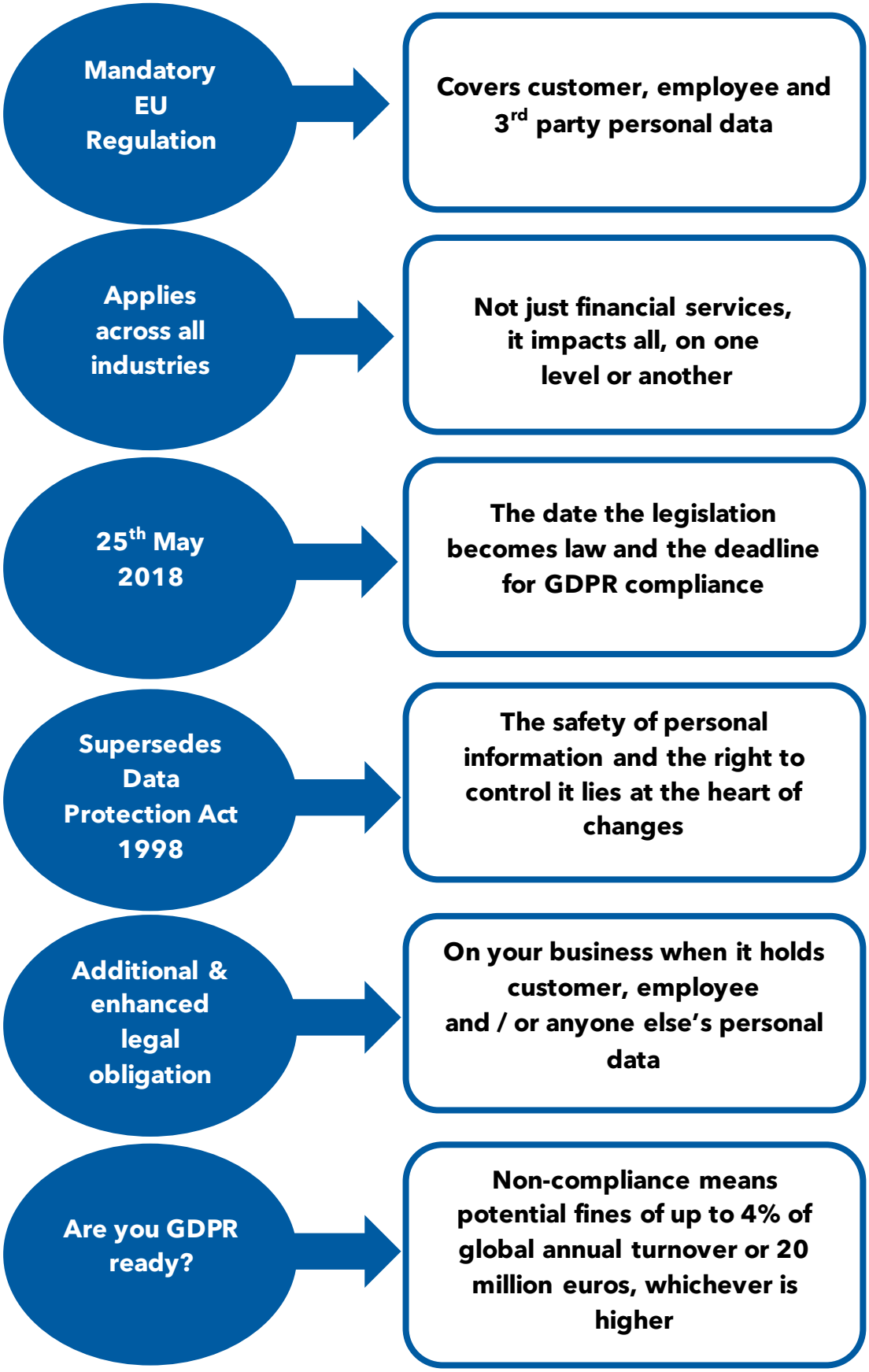
The GDPR regulation is all about giving people greater control over what happens with their personal data and strengthens everyone's rights.

Here are some of the key changes that GDPR brings:

- Greater control for everyone – your customers and your employees
- More responsibility and obligations for controllers and processors to ensure individuals' rights are protected
- Keeping individuals' informed and provide clarity about what your organisation is doing with the personal data you collect, hold and use
- Increased Individual rights including the 'right to be forgotten', the 'right to portability' and the 'right to restrict' what is being done with personal data
- Increased rights to compensation when an individual's rights have not been upheld
- Mandatory reporting for data breaches
- Quicker response times and no charges for subject access requests
- Changes to the way in which consent is given – pre-ticked boxes are no longer compliant
- Greater responsibility on everyone to take personal data seriously

GDPR summary

GDPR is a wide reaching legislative change that supersedes the Data Protection Act. It applies to all personal data and sets a new bar for privacy rights, security and compliance.



Why you need to comply?

All organisations have legal and regulatory obligations to ensure compliance with existing and any new data privacy legislation.

This new EU legislation strengthens individual privacy rights and requires that data privacy is part of everything we do. Whether you are designing new products, working with customers and/or suppliers or dealing with staff, every organisation has a responsibility to ensure compliance when dealing with personal data.

GDPR represents the biggest overhaul of European Data Privacy legislation in twenty years, superseding current EU Member State laws on Data Privacy including the UK's Data Protection Act 1998. Everyone needs to be working within the new and enhanced framework.

The new law requires you to:

- Deliver on the privacy rights of your customers and employees
- Protect their personal data
- Be transparent around what you are doing with personal data
- Be able to evidence that you can meet the requirements of the new law

GDPR impacts your people, your processes and procedures, and your technology

Considerations

The handling and managing of personal data is everyone's responsibility, not just those who have to do it. No one wants to be responsible for non-compliance. There are a number of things you can be looking at:

- Consents
- Data Privacy Notices (DPNs)
- Data Subject Access Requests (DSARs)
- Third Party suppliers and contracts
- Individual rights
- Data storage and flow
- Risks and controls
- Data Protection Impact Assessments (DPIAs)

Consent must be as easy to withdraw, as it is to give

Consents

It is important that you know why you use personal data, and the conditions you are relying on for processing this information.

If you currently rely on consent for the use of personal data then the threshold for how valid consent is given is significantly raised.

Customers must take a positive action to give their consent; pre-ticked boxes and silence are not valid under GDPR.

Consents - continued

- Do you need to update your Data Privacy Notices (DPNs)?
- Does your staff know how a servicing message differs from a marketing message?
- Are your customers clear on what they are consenting to?

Data Privacy Notices (DPNs)

The new regulation requires that you provide individuals with a Data Privacy Notice (DPN) informing them of how you will use their data.

This is usually provided at the point of data collection. Under the new regulation, DPNs need to be more detailed (e.g. contact details of the organisation's Data Protection Officer (DPO) (if applicable) and the right to make a complaint to the Data Privacy Authority.

- Are your DPNs GDPR compliant?
- What do you need to do to make your DPNs GDPR compliant?
- Do you need to let your customers and employees know that it will be easy to understand, in your DPNS, how you will be more open and transparent in your handling of their personal data?

DPNs must be in an easily understood format

Data Subject Access Requests

The response time for Data Subject Access Requests (DSARs) is reducing from 40 days to one month and the request fee for information removed. This may result in an increase in DSAR requests.

- Can your processes meet the faster response time?
- Can you respond to requests in a machine-readable format?
- Do you have a process in place for contacting third parties who may also be involved in the DSAR request?

Requestors can now opt for the choice of an electronic response

3rd Party Suppliers & Contracts

Where a third party processes data on your behalf, the third party also needs to be compliant with the new regulation.

- Are your suppliers' contracts compliant?
- How do you know?
- How do you ensure compliance is upheld?

What if your supplier asks whether you are GDPR compliant – how would you respond?

Individual Rights

There are eight individual rights:

- ✓ Data Privacy Notices (DPNs)
- ✓ Data Portability
- ✓ Data Subject Access Requests (DSARs)
- ✓ Right not to be subjected to automated decisions and profiling
- ✓ Right to rectification
- ✓ Right to restriction of processing
- ✓ Right to erasure (also known as the right to be forgotten) - new
- ✓ Right to object to processing
- ❖ How would you respond to a request to erase someone's personal data i.e. Right to be forgotten?
- ❖ Do you need to retain personal data for legal reasons?

People have more control than ever before

Record of processing

Under GDPR, as a data controller or an organisation, you need to understand the types of data you process, who it is for and why it is collected. You also need to know where it is held and stored within your organisation.

This means you must keep up to date records of processing activities that involves personal data. You also need to hold a record of activities you undertake for other data controllers.

- ❖ Have you looked at your end-to-end processes so you know where personal data sits and flows?

Records need to be up to date and maintained

Risk & Control Framework

The new regulation significantly increases fines (current UK maximum of 500k).This could be as high as 4% of global turnover or 20 million euros, whichever is the greater.

- ❖ What would you share with the regulator to show how you are complying?
- ❖ Do you have a point of contact for all matters relating to data privacy?
- ❖ Are your data privacy policies GDPR compliant?

Data Protection Impact Assessments

The new regulation looks to embed a culture of 'privacy by design'. This means data privacy needs consideration when planning significant change e.g. launching a new product.

- Are you embedding good practice throughout your organisation?
- Would your staff know what to do when making changes that may impact your record of processing?
- What can you do to build awareness?

The ICO expects impact assessments to be completed prior to any high risk processing and it has the power to ask for evidence

Things to think about

Here are some quick things to be thinking about to help get you up and running:

- Are all employees aware of GDPR and their role in looking after personal data? It could be theirs!
- Do you have a training and communication plan to bring your staff on the journey? What do you plan to tell your customers?
- Do you need to update your website/social media channels to reflect the GDPR?
- Are you still referring to the Data Protection Act 1998 in your marketing material and in your privacy policies and notices?
- Who would your customers or staff go to if they had a complaint about personal data?
- How would you respond if asked by an external party whether your organisation is GDPR compliant?

Personal Data Breaches

Under GDPR, data privacy incidents need to be reported to the Information Commissioner's Office (ICO) within 72hrs of becoming known, where there is a risk to the individual. In some cases, customers need to be notified.

An important role of the Data Protection Officer (DPO) is to ensure this is done.

- Do you know what a data breach looks like? Would you know what to report?
- Once identified, can you respond within 72 hours?
- Who will do this?

Complaints and Compensation

The regulation is looking to ensure that the management of data privacy complaints is in line with the data subject's rights under GDPR.

- Does your complaints process cover the enhanced data privacy regulations?
- Are you and your staff aware that everyone may now be entitled to compensation if a complaint is upheld?

Accountabilities and Data Protection Officer (DPO)

The regulation is looking to ensure that there is clear accountability within organisations regarding the management of personal data.

It introduces a new role for organisations called a Data Protection Officer, who is ultimately responsible for data privacy and reports into the highest governance body within the organisation.

- Under GDPR, do your data processing activities require the appointment of a Data Protection Officer? If so, who is this?
- Does your staff know about this new role? Would they know how to contact them and what they are responsible for?

Security

You should already be looking after any personal data held in a secure and protective way. The key change here is that the burden of proof will be on you, as the controller of data i.e. you will need to prove to the regulators, the Information Commissioner's Office (ICO), that effective security controls are in place.

The regulation strongly recommends the use of 'pseudonymisation' to provide additional security for personal data. This is the ability to scramble data at rest and then be able to use a 'key' to descramble.

- Do you need to think about 'scrambling' your data?
- Do you have the right level of operational and technical controls in place?

Data Portability

We are all hearing about how we will be able to ask an organisation to share our data in an open way. GDPR supports this through data portability requests. This is similar to a Data Subject Access Request (DSAR). However, there are subtle differences in the scope of data returned and the issuing format.

If an individual provides you with their consent or a contract to handle their personal data and you process it by automated means, under GDPR, you must be able to share it. In addition, you must complete any request within one month and in some cases, this can be up to three months. Responses need to be issued in a structured, commonly used and machine-readable format.

- Is your organisation able to respond to this?
- Would you know when you could extend the deadline?

Where can I find out more?

- Further information and regular updates can be found at the Information Commissioner's Office (ICO) website
- ICO website for organisations including sector guidance
- More in-depth information on new legislation and what it means at EU General Data Protection regulation
- The ICO has a dedicated advice line that offers help to small organisations, including charities, Access the ICO helpline on 0303 123 1113 and select option 4.