BARCLAYS

# Is your business ready?

## The General Data Protection Regulation

# Need to know

- We expect the GDPR to have far-reaching consequences for businesses
- It could affect the way your business manages any personal data it holds on EU citizens
- Changes will still apply in the UK – even after Brexit

# Focusing on personal data

The GDPR focuses on personal data, examples of this includes (but is not limited to):

- Names and addresses
- ID numbers
- Location Data
- Economic and social status

Your business probably collects lots of other data, including:

- Business information
- Financial data
- Analytical data

# Understanding the GDPR

- Understanding the GDPR
- Individuals' rights
- Your business
- Examples
- More information

# Understanding the GDPR

## The General Data Protection Regulation

BARCLAYS

# Current law

In the UK, we have the Data Protection Act 1998. It means:

- Those responsible for using data have to follow data protection principles
- Enforced by the Information Commissioner's Office
- Serious breaches can result in fines up to £500,000, however there is still the potential for the FCA to become involved in data related breaches meaning fines could be considerably higher.

# From 25 May 2018

The General Data Protection Regulation is introduced.

- Applies to any company dealing with the personal data of individuals residing in the EU, regardless of the company's location
- Individuals can ask for compensation if businesses don't comply
- Non-compliance = big fines. Up to 4% of global turnover or €20million
- UK government has confirmed legislation will apply in full and after Brexit the 'UK Data Protection Bill 2017' will cover UK organisations and individuals
- ICO remains the enforcing body

# Strengthening rights

## What customers and staff can expect

BARCLAYS

# How rights will be strengthened

The GDPR covers all information on individuals stored electronically and most recorded physically.

Individuals have enhanced rights to:

- Be **informed** about the way their data is processed
- Request **access** to a copy of their personal data
- **Object** to their data being processed for some specific purposes
- **Restrict** a business from processing their personal data if it's inaccurate, or if the reason for processing is contested
- Correct or **erase** mistakes in the personal data a businesses stores about them
- Make their personal data **portable** so they can share it with other data controllers
- Not be evaluated by **profiling** based solely on automated processing of their data
- Get access to **remedy** by compensation if data controllers or processors use their data improperly

# Your business

## What the GDPR could mean

BARCLAYS

# Data controller or data processor?

**The GDPR defines two roles:**

1. Data controller: Responsible for how and why personal data is processed.
2. Data processor: Acts on a controller's behalf.

**How to check**

Businesses that collect, store and use data using only their own systems are **both a controller and a processor**.

Those using third-party applications or storage are **controllers**.

Those providing applications or storage to other organisations are **processors**.

Those that provide a service to other organisations (including having access to and using their customers' or employee's data) are **processors**.

# Data checkpoints

**If you're a data controller, check:**

- The data you're collecting – is it relevant?
- How long you're storing it for – must only be while it's required
- You've told the individuals whose data it is about the two points above
- Who has access to the data
- You can provide evidence to back up your answers

**If you're a data processor, check:**

- Where the data's stored – must be in the EU
- The security you have in place
- You're only using the data for the purpose the controller has authorised
- You can provide evidence to back up your answers

# Real-world examples

## Putting the GDPR into practice

BARCLAYS

# Example: first contact

Business A provides accountancy services. Any visitors need to sign in at reception by providing their name and car registration.

## Is personal data being collected?

Yes.

## What's the role of Business A?

Data controller and processor

## What should Business A consider?

Individuals must know how their data is being used and how long it will be kept.

Whether the data could be destroyed at the end of every day as it will no longer be needed.

# Example: harvesting emails

Over many years, Business B has collected individual email addresses along with the customers name and any other personal details online and at events. They've added this information to a mail client for marketing purposes.

## Is this personal data?

Yes.

## What's the role of Business B?

Business B is the data controller. The mail client is the data processor.

## What should Business B consider?

If they can provide evidence that they've adequately explained to the individuals that they'll be using their email addresses for marketing purposes.

Whether they have the ability to delete or amend individual records if requested and update marketing preferences if the individual chooses not to receive marketing in the future.

Where the mail client (the data processor) stores the data.

# Example: online purchases

Business C sells products through its website. This means asking customers for their name, address, and contact number.

## Is this personal data?

Yes

## What's the role of Business C?

Data controller and data processor.

## What should Business C consider?

That customers are notified:

- Why the data is being collected (to send the product)
- For how long it will be kept (until delivery is complete)

# More on the GDPR

## Where to look

BARCLAYS

# Information Commissioner's Office (ICO)

The ICO has put together a plan of Key actions you can start straight away:

1. Awareness
2. Information you hold
3. Communicating privacy information
4. Individuals' rights
5. Subject access requests
6. Lawful basis for processing personal data
7. Consent
8. Children
9. Data breaches
10. Data protection by Design and Data Protection Impact Assessment
11. Data-protection officers
12. International

https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf

# Information Commissioner's Office (ICO)

Barclays GDPR guide:

- https://www.barclays.co.uk/business-banking/articles-and-guides/gdprforbusiness
- Barclays cyber security webinar: please ask your Relationship Manager.

Information Commissioners Office:

- https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

Experian's guide to data governance:

- https://www.edq.com/uk/guide-to-gdpr

# Disclaimer

The views and opinions expressed in this presentation do not necessarily reflect the views of the Barclays Bank PLC Group nor should they be taken as statements of policy or intent of the Barclays Bank PLC Group. The Barclays Bank PLC Group takes no responsibility for the veracity of information intimated by a third party and no warranties or undertakings of any kind whether express or implied, regarding the accuracy or completeness of the information are given. The Barclays Bank PLC Group takes no liability for the impact of any decisions made based on information contained and views expressed in this presentation or article.