PolicyPlan

BROKER'S GUIDE TO GDPR

What is GDPR?

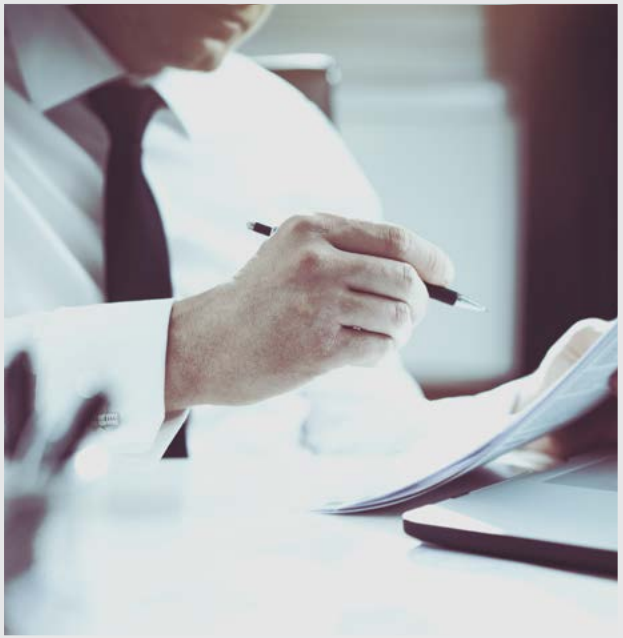
General Data Protection Regulation (GDPR) was conceived by the European Commission in 2012 and sets out plans for data protection reforms across the EU. GDPR is a new set of rules designed to give individuals greater control over their data. It aims to simplify the regulatory environment for businesses so both individuals and organisations can fully benefit from the digital economy.

This new framework has implications for businesses and individuals across the UK as almost every aspect of our lives now revolves around data.

So, what does it mean for brokers and how should you prepare for the new regulations?

"This new framework has implications for businesses and individuals"

Awareness



Is the leadership team aware of the change in law on the 25th May 2018 and what it means for the data you hold within your business? Have they engaged with the business areas affected by the changes?

Information you hold (Data Mapping)

Are you aware what type of data is impacted by GDPR and how? Some of the crucial questions you need to answer include:

What data do you have?

- Do you know what personal data you hold including business to business data, customer and employee data?
- Where it came from?
- How was it obtained?

What you do with it?

- How long do you keep it for?
- Who do you share it with?

Consent?

- Do you have explicit and unambiguous consent to hold it?
- When was this consent obtained?
- Where and how do you store consent?
- Is there an audit trail?

Privacy notices

Who you are and how you plan to use their personal information

The legal basis under which you are processing the data

Your data retention periods

Their rights to complain, obtain copies of data and to withdraw their consent.

Have you been clear and transparent in telling those that you hold personal data about:

Individual rights

Under the new GDPR regulations customers have the right to be forgotten from current systems, backups and marketing lists.

There are also requirements for procedures around the correction of information inaccuracies, data portability, automated decision making and any profiling also needs to be documented.

You will need to ensure that there are processes in place enabling your business to conform with these regulations.

Subject access requests

There are new rules surrounding Subject Access Requests and procedures will need to be amended to reflect how your business will handle these going forward.

There will be a reduced time limit of 1 month to respond to each customer request and, in the majority of cases, any charges for this service will need to be removed.

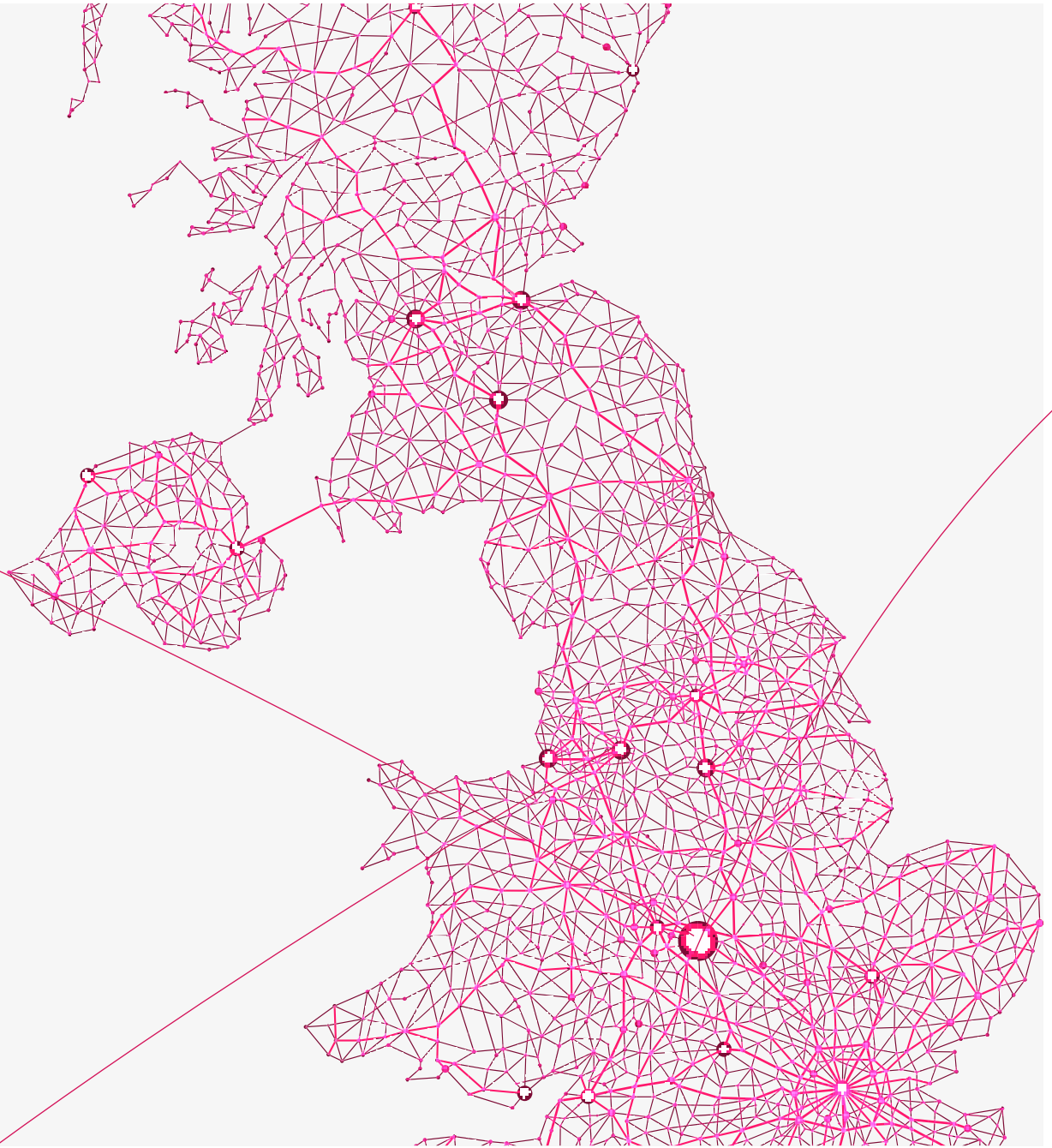
Legal basis processing

Do you have a legal basis on which to process and hold information?

Every organisation will need to identify under what legal basis they process and hold an individual's data.

For example, a motorhome broker would hold data categories X, Y and Z because without this information they would be unable to offer a motorhome insurance quote.

International



If your business operates internationally then you will need to establish under which data protection jurisdiction your supervisory authority falls.

This is normally where the major decisions for business administration are made.

Consent

Consent needs to be specific, informative and not open to interpretation. You are no longer able to pre-tick boxes on behalf of individuals.

When obtaining consent, you need to be clear, informative and specific. Records should show the date and time of when specific consent was achieved, for what purpose, by whom and how.

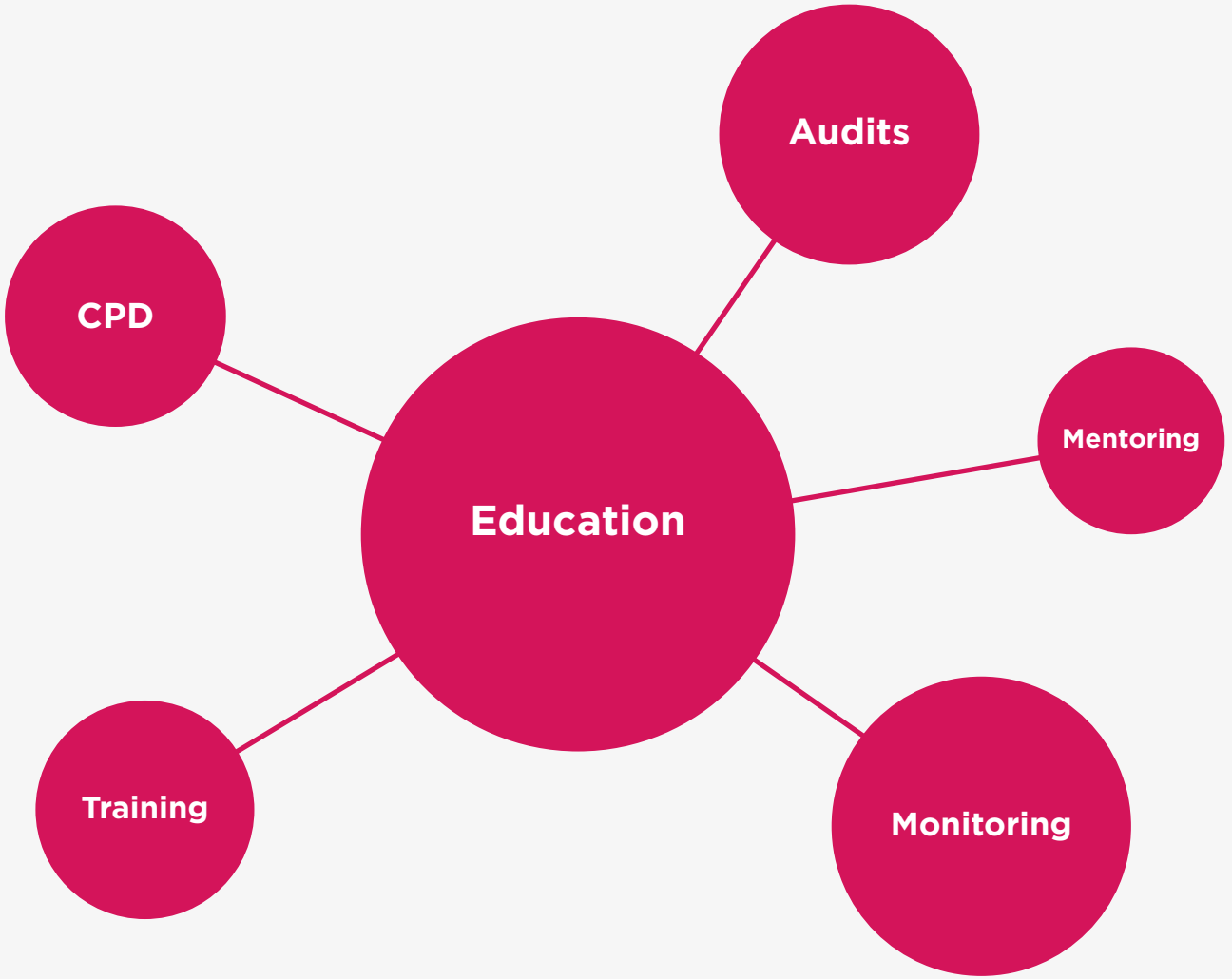
Data Protection Officer (DPO)

The appointment of a DPO is only mandatory in three situations; when the organisation is a public authority or body, or when the organisation's core activities consist of either:

Data processing operations that require regular and systematic monitoring of data subjects on a large scale; or

Large-scale processing of special categories of data (i.e. sensitive data such as health, religion, race, sexual orientation etc.) and personal data relating to criminal convictions and offences

Educating staff



You will need to ensure that all staff are aware of their responsibilities when dealing with personal data and can recognise and report any breaches that may occur.

Training on the changes and what they mean for your business must be given to every individual in the organisation.

Data breaches

If a data breach occurs it must be reported to the Information Commissioners Office (ICO) within 72 hours of its discovery.

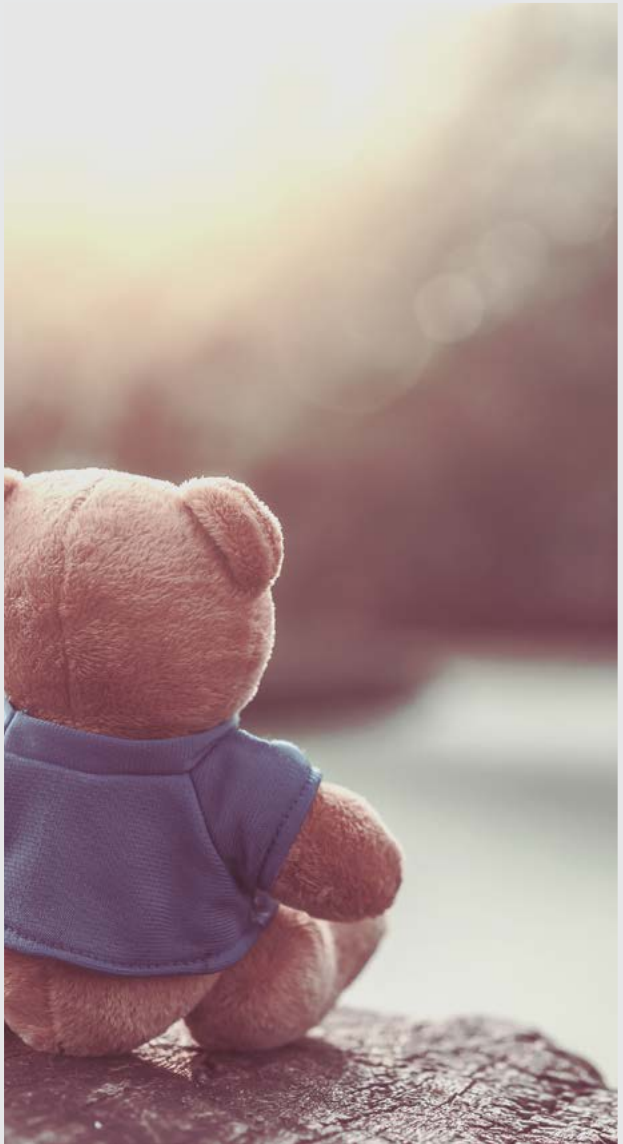
If not reported in full during this period then at a minimum a notification must be sent with further full details following on.

Children

Children are identified as “vulnerable individuals” and deserving of “specific protection” under the regulations.

Where services are offered directly to a child, notices must be drafted with a child’s understanding in mind.

Organisations impacted must ensure any reliance on “legitimate interests” to justify processing children’s data is backed up with a careful and documented consideration of whether a child’s interests override those of your organisation.



Next steps...

If you haven't already done so you may consider appointing an accountable director, setting aside some budget to manage the transition and establishing exactly what data your business is storing and how. It is essential to compile a detailed plan for compliance well in advance of the GDPR rollout in May 2018.

The bottom line is, GDPR is going to affect almost every organisation in the UK and there's no way around it. Businesses that don't put an effective plan in place may find themselves facing large fines. So, it's time to start planning and implementing your GDPR strategy now.

"GDPR is going to affect almost every organisation in the UK"

PolicyPlan Limited
Registered in England and Wales No. 6419377.
Registered office Staveley House, Church Street, Connah's Quay CH5 4AS.
Authorised and regulated by the Financial Conduct Authority.

Please note
This booklet is intended as a guide only and should not be considered legal advice. To learn more about GDPR visit the Information Commisioner's website at https://ico.org.uk