ARE You Ready For GDPR?

Content

---

1. Rationale

IMLA is a trade body whose lender members offer support to the intermediary mortgage market in a variety of forms such as education and information. This fact sheet has been prepared with the assistance and input from a broad number of lender members to provide insight into the main changes posed by the introduction of the GDPR to mortgage brokers.

(NB: This fact sheet is only intended as an informative guide and does not set out all the requirements with which firms may need to comply).

What is GDPR?

GDPR is the **General Data Protection Regulation** and replaces the existing Data Protection Act (DPA).

Or it might also be referred to as ***Getting Data Protection Right!***

When is it being introduced?

25 May 2018.

Who is introducing it?

It has been drafted by the European Commission and will be adopted in the UK whatever the Brexit outcome.

Why is it being introduced?

There are essentially three main reasons for the introduction of GDPR and these are as follows:-

- To keep pace with advances in technology and the way we exchange or transmit data e.g. Social media, tablets and smart phones,
- To strengthen the digital economy in the European Union;
- To reduce the compliance burden for organisations operating in multiple EU member states by introducing a single set of rules.

Summary

Many of the principles which apply currently under the DPA will remain, however there are some new elements being introduced under GDPR and there are also some things that need to be done differently.

The implications of GDPR compliance may need you to review and indeed implement new procedures, your governance of data and storage of data for example. If you are a data controller there is a greater emphasis on documentation which is retained to demonstrate accountability.

It is worth noting that the maximum fine that can be levied for non-compliance has been increased to €20m (approx. £17m) or 4% of Annual Turn Over whichever is the higher (this is up to €10m or 2% of annual turnover for a minor breach).

2. Main Changes

Transparency

GDPR requires openness and transparency with data subjects and national Supervisory Authorities (SA); the Information Commissioner's Office (ICO) is the national SA in the UK.

For instance individuals must be provided with concise and meaningful information about the processing of their personal data. Organisations must also document their processing activities and provide this on request to their national SA. Such documentation should include what personal data is processed and why, who it is about, the types of organisation it is shared with and how long it is kept.

***Question* - Have you documented your processing activities?**

Accountability

Under GDPR, organisations are required to be able to show how they comply with data protection principles by having effective policies and procedures in place.

***Question* - If you were audited by the Information Commissioner's Office (ICO) can you demonstrate you meet the requirements of the GDPR?**

New (Strengthened) Rights of Customers

These include:-

- The Right to be Informed
- The Right of Access (aka Data Subject Access Request)
- The Right to Rectification
- The Right to Erasure
- The Right to Restrict Processing
- The Right to Data Portability
- The Right to Object
- The right not to be subject to Automated Decision Making

You may want to consider whether your procedures cover all these rights individuals have, including how you would delete personal data. Going forward certain data provided by a data subject will be required to be capable of being transmitted electronically in a commonly used machine readable format such as a CSV file. Different customers and records containing personal data may warrant different data retention periods (e.g prospects vs completed clients). Clients or customers have the right to ask about what you know about them and to be provided with a copy of this data.

In most cases you won't be able to charge individuals for exercising their rights. You have 1 month to comply (rather than 40 days under DPA) - If you refuse a request it is a requirement to tell the customer why and that they have the right to complain to the ICO.

***Question* - Can your system successfully locate and delete data?**
How long do you keep data for?
Do you have a records retention Schedule?
How will you handle requests?
Who do you need to tell in your organisation?

Consent

GDPR restricts the use of consent as a means of lawfully processing personal data to instances where a person has a genuine choice, for instance in relation to their marketing preferences. It is not appropriate to rely on consent where such a choice does not exist, for example it would not be appropriate to obtain a customer's consent to share information with a credit reference agency if the sharing will continue even if a customer later withdraws their consent.

It is suggested you review how you or your firm seek, record and manage consent. Consent must be freely given, specific, informed and unambiguous and if existing consents don't meet GDPR requirements then they are best refreshed.

One of the main changes for GDPR is that there must be a positive "opt in" by the customer. Customers must also have simple ways to withdraw their consent.

If you are relying on an individual's consent to process their data then they must meet the following GDPR standards of being:-

Specific
Granular
Clear
Prominent
Opt in
Properly Documented
Easily Withdrawn

It is worth remembering that you can't assume responsibility for answering consent questions on behalf of the customer and that the customer will be required to be informed about what data will be shared and at what point during the mortgage process. This is part of a greater focus on transparency and understanding.

Question **- What changes (if any) do you need to make in how you capture and record consent? Have you reviewed customer facing documentation and considered any uses of the word 'consent'?**

Personal Data Breaches

A personal data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Under GDPR there is a duty for ALL data controllers to report certain personal data breaches to the ICO and in some cases to individual customers, so procedures are required to detect, report, investigate and respond to a data breach.

You would need to notify the ICO if a data breach is likely to result in a risk to the rights and freedoms of individuals being compromised. This should happen within 72 hours. Individuals should be written to if there is a high risk of damage, financial loss, confidentiality, economic or social disadvantage.

Question **- Do you know or your colleagues know the procedure to follow if you detect a data breach?**

Communicating Privacy Information

When you collect personal data you currently have to give your customers certain information such as the identity of the data controller and how you intend to use their data. This is usually done through the issuance of a privacy notice. Under GDPR there are additional items to explain which include such things as the lawful basis for being able to process their data and how long you would hold their data for.

Question **- Have you reviewed your current Privacy Notice and made any changes to comply with the GDPR?**

Lawful Basis for Processing Data

The lawful bases for processing data under GDPR are in essence similar to those under the DPA. It is suggested firms identify, document and update their privacy notices to explain these.

There are 6 bases that firms can use as their basis of processing depending on their business model & what data is being collected. The basis of "contract" could be appropriate where an individual customer approaches an intermediary for help finding a mortgage, whereas the intermediary could use "consent" to process data relating to advice on protection products for example.

***Question* - Have you thought about your lawful basis for processing personal data?**

Summary - GDPR through a broker lens

a) If you are compliant with the current Data Protection Act then you are a long way down the road to complying with the GDPR.
b) Lenders that currently rely on an 'opt out' approach to obtaining marketing preferences will be required to change to a clear 'opt in' policy.
c) Be aware you cannot assume responsibility for answering consent questions.
d) Create a records retention schedule.
e) You may require different retention periods for different customer types and records.
f) Look at how you can deal with requests from individuals exercising their individual rights.
g) What oversight can you evidence on data collection and storage?
h) What information do you provide the customer on the process?
i) Review your lawful basis for processing personal data and Privacy Notice.

3. Changes For Lenders

To help with your preparations for being compliant with and implementing GDPR it is also worth considering some of the changes lenders will be making & how these might affect how you carry out your daily business.

1. Lenders will be making changes to their Marketing Preferences & how consent is collected from potential borrowers.
2. Lenders will be making changes to their Privacy Notices (usually included in their T&C's & on their websites) to comply with GDPR
3. They will be reviewing their contracts when sharing data with other organisations
4. They will be looking at how they meet the new requirements of satisfying the strengthened Individual rights e.g., Right to be Forgotten
5. They will be looking how they evidence & document the decisions they take about their processing activities.
6. Lenders will be required to show & evidence accountability & compliance with the principles of GDPR.
7. Lenders will be required to carry out data protection impact assessments where either a new technology is being deployed or there is processing on a large scale of special categories of data.

4. Questions for Consideration

- **Have you documented your processing activities?**
- **If you were audited by the Information Commissioner's Office (ICO) can you meet the requirements of the GDPR?**
- **Can your system successfully locate and delete data?**
- **How long do you keep data for?**
- **Do you have a records retention Schedule?**
- **How will you handle requests?**
- **What changes (if any) do you need to make in how you capture and record consent?**
- **Have you reviewed customer facing documentation and considered any uses of the word 'consent'?**
- **Do you know the procedure to follow if you detect a data breach?**
- **Have you reviewed your current Privacy Notice and made any changes to comply with the GDPR?**
- **Have you thought about your lawful basis for processing personal data?**

5. Other sources of Information on GDPR

- ICO – Preparing for the General Data Protection Regulation (GDPR)
- ICO – Guide to the General Data Protection Regulation (GDPR)
- AMI Factsheet: General Data Protection Regulation
- ICO guide to SME's on GDPR

You may find it beneficial if you have any particular queries on GDPR to ring the following number:-
ICO dedicated helpline for small businesses: 0303 123 1113 (Option 4)