AMI Factsheet: General Data Protection Regulation

Introduction

This factsheet has been prepared by the Association of Mortgage Intermediaries as an introductory briefing to the EU General Data Protection Regulation.

The General Data Protection Regulation (GDPR) replaces the Data Protection Directive and was designed to harmonise data privacy laws across Europe, to protect and empower all citizens' data privacy and to reshape the way organisations approach data privacy. It will come into effect from 25 May 2018.

While the new legislation is generally an extension of the Data Protection Act 1998 (DPA) and other provisions, it adds explicit requirements and introduces new obligations. The GDPR is focused on a data minimisation approach and transparency around the purposes for using data. It applies to all organisations that control and process data.

We strongly recommend that firms read the information that is available on the Information Commissioner's Office website (links are included throughout with additional reading at the end). Our factsheet is only intended as a guide and does not set out all the requirements with which firms will need to comply.

Summary

Principles

Under GDPR, the data protection principles set out the main responsibilities for firms. These are similar to those in the DPA with added detail in certain areas, but the most significant addition is the accountability requirement. The GDPR requires firms to show how they "shall be responsible for, and be able to demonstrate, compliance with the principles", for example by documenting the decisions they take about a processing activity. The principles are that personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;
b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d) accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;
f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Lawful basis for processing

Firms must have a valid lawful basis in order to process personal data. There are six available lawful bases for processing:

(a) Consent: the individual has given clear consent for a firm to process their personal data for a specific purpose.
(b) Contract: the processing is necessary for a contract a firm is to have with the individual, or because they have asked the firm to take specific steps before entering into a contract.
(c) Legal obligation: the processing is necessary for firms to comply with the law (not including contractual obligations).
(d) Vital interests: the processing is necessary to protect someone's life.
(e) Legitimate interests: the processing is necessary for a firm's legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.
(f) Public task: the processing is necessary for a firm to perform a task in the public interest or for a firm's official functions, and the task or function has a clear basis in law.

No single basis is 'better' or more important than the others – which basis is most appropriate to use will depend on a firm's purpose and relationship with the individual. For example, where a customer approaches an intermediary for help finding a mortgage, the firm may deem "contract" as the lawful basis of processing, whereas they may use "consent" to process data relating to advice on protection products.

If firms use the basis of "consent", they will need to seek explicit consent from an individual to process their data: silence, pre-ticked boxes or inactivity do not constitute consent. The consent should outline the specific activity for which their data will be processed. Firms will not be able to rely on consent given for one activity and use it for other purposes, so firms will need to decide how they will obtain consent for each processing activity. The declaration of consent has to be provided in an intelligible and easily accessible form, using clear and plain language and not contain unfair terms. This move from firms providing long and complex terms and conditions to needing to effectively engage with consumers has been encouraged by the FCA in their recent work on smarter communications.

Firms must determine their lawful basis before beginning processing and it should be documented. Firms should not swap to a different lawful basis at a later date without good reason. Privacy notices should include the lawful basis for processing as well as the purposes of the processing.

Individuals' rights

One key area of GDPR is the strengthening of individuals' rights. Depending on the requirement, there are timescales in which firms have to comply with an individual's request. GDPR provides the following rights for individuals:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling

Under the DPA, the right to erasure is limited to processing that causes unwarranted and substantial damage or distress. However under GDPR, individuals have a right to have personal data erased and to prevent processing in specific circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
- When the individual withdraws consent.
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
- The personal data was unlawfully processed (i.e. otherwise in breach of the GDPR).
- The personal data has to be erased in order to comply with a legal obligation.
- The personal data is processed in relation to the offer of information society services to a child.

Firms can refuse to comply with a request to erasure where the personal data is processed for specific reasons, including to comply with a legal obligation for the performance of a public interest task or exercise of official authority. The ICO understands that deleting certain data may be difficult for financial services firms: firms should clearly document the reasons why they may not comply with such a request (e.g. to fulfil regulatory obligation; in order to effectively manage any future complaint). Firms still need to consider what data they need to hold, and for what periods of time, under the overarching principles. For example, firms may consider that retaining payslips and bank statements indefinitely is not justifiable.

Subject access requests will have to be provided free of charge. In addition, individuals will be allowed to obtain and reuse their personal data for their own purposes across different services. Firms will therefore have to provide the data in a structure that is commonly used and in a machine readable format, e.g. CSV file. If the individual requests it, firms may be required to transmit the data directly to another organisation if this is technically feasible. However, firms are not required to adopt or maintain processing systems that are technically compatible with other organisations.

Individuals will have additional rights if data is used for direct marketing purposes, profiling or automated decisions. In the context of automated processes, firms will have to ensure that individuals are able to obtain human intervention, express their point of view and obtain an explanation of the decision and challenge it.

Breach notification

The GDPR will introduce a duty on all organisations to report certain types of data breach to the ICO within 72 hours, and in some cases to the individuals affected. The enforcement action taken by the ICO will depend on the firm's compliance with GDPR, how this is evidenced and how a firm has responded to the breach. Firms should therefore consider how GDPR will interact with their cyber security policy and data recovery plans.

Failure to notify a minor breach when required to do so will result in a fine up to €10 million or 2% of total global annual turnover (whichever is higher), and failure to notify a major breach results in a fine up to €20 million or 4% of total global annual turnover (whichever is higher).

Firms will need to consider whether the data breach also needs to be reported to the FCA.

Next steps

Firms should be planning now for the changes they will have to make and consider how these will be properly documented, along with the justification behind the decisions made. This includes, but is not limited to, data protection impact assessments and the allocation of a data protection officer.

As a starting point, for processing to be legal under the GDPR, firms will need to identify and document the lawful basis in which they process personal data (referred to as the "conditions for processing" under the DPA). This becomes more of an issue under the GDPR because the lawful basis for processing has an effect on individuals' rights. For example, if a firm relies on consent to process their data, they will generally have stronger rights, such as to have their data deleted (although firms can set out why they may not erase certain data). The ICO has set out draft guidance on consent and provided subsequent feedback on when it may or may not be appropriate for firms to use consent as their basis for processing. Firms will need to consider which of the six bases are appropriate for each processing activity, e.g. advising on a mortgage, advising on protection etc.

As with the DPA, the GDPR applies to third parties acting on behalf of the data controller, so firms will need to revisit contracts with service providers to ensure compliance. Firms will need to consider at what point in a transaction they are a "controller" or "processor" (they may transition between the two), as there are different obligations. We will soon start to see lenders updating their contracts with intermediaries to incorporate GDPR. We advise firms to review these carefully to ensure that responsibilities are appropriately defined, particularly ensuring that unfair obligations are not placed on firms.

If firms consider what GDPR is trying to achieve then they will not only find it easier to comply with, but also end up in a positive position from a regulatory perspective. In the current world we have technology firms holding full profiles of individuals and using their data for purposes that are not particularly transparent, nor do they allow opting out of additional processing. The regulation is designed to address this by empowering individuals and giving them more rights; it will be consumers who control their data. If firms aim to effectively communicate how data is held and what it will be used for, instead of relying on complex terms and conditions or trying to find alternative ways to avoid complying with certain requirements, then these firms are unlikely to be a focus for either the FCA or ICO.

Useful support material

The Information Commissioner's Office has a dedicated website on GDPR for businesses, which includes:

- GDPR overview
- Preparing for GDPR: 12 steps to take now
- Getting ready for GDPR: checklist
- Blogs on busting GDPR myths
- Updated guidance on GDPR
- Further guidance: what to expect and when

The legislation that will enforce GDPR has yet to be implemented. Progress on the Data Protection Bill can be found here.