General Data Protection Regulation

What is GDPR?

•Updated Data Protection Legislation implemented by The European Commission

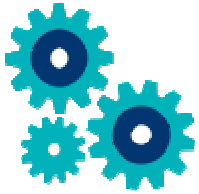
•Comes into force 25th May 2018

•Gives both new and enhanced rights for individuals in relation to their personal information •The government has confirmed that the UK's decision to leave the EU will not affect the commencement of the GDPR

•Introduces the ability for data protection authorities across the EU to fine organisations up to 4% of annual worldwide turnover for non -compliance, or 20 million Euros in turnover, whichever is the greater (Current UK regime maximum fine £500,000) •Applies to 'controllers' and 'processors'

•The ICO (Information Commissioner's Office) is committed to assisting businesses and public bodies to prepare to meet the requirements of the GDPR ahead of May 2018 and beyond

Operating Model and Governance

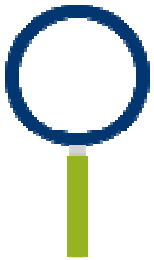


Existing obligation: Staff must be trained on their data protection obligations and will therefore need to be aware of their new responsibilities under the GDPR

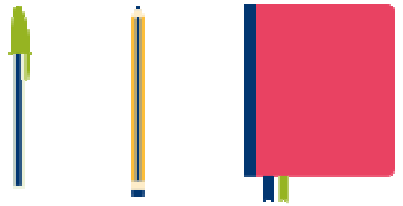
New obligation: Organisations of certain sizes and who conduct certain high risk activities will need to appoint Data Protection Officers (DPOs)

New obligation: Organisations must have a clear accountability model for privacy

New obligation: Privacy must be built into new product/ service/ process/ system design at the outset. Privacy impact assessments have also been made mandatory for all high risk processing activities



Documentation and Processing



New obligation: Inventories of all activities involving the processing of personal data must be created and maintained

Enhanced obligation: Every processing activity requires a legal basis for processing under the GDPR

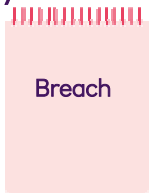
Enhanced obligation: Biometric data is now included in the list of sensitive data along with data relating to health, race, religion, etc

New obligation: Records will need to be kept of privacy impact assessments and decisions regarding data breaches

ONLY FOR USE BY MORTGAGE INTERMEDIARIES

General Data Protection Regulation

Transparency and Breach notifications



Enhanced obligation: Privacy notices will need to be far more detailed (for example, explaining (i) the rights of individuals, (ii) what legal bases the organisation relies on and (iii) how long each type of personal data is kept for)

Enhanced obligation: Where consent is being relied on as the legal basis for processing it needs to meet the new requirements for consent. Namely it must be fully informed and freely given, demonstrated by affirmative action and evidence of consent must be maintained.

New obligation: Breaches will need to be notified to data protection regulators within 72 hours where there is the risk of harm to individuals. Individuals are at significant risk of harm also need to be notified as soon as possible

3rd Party Management

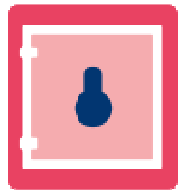
Enhanced obligation: Due diligence must be conducted on 3rd parties to ensure they will be able to meet their data protection obligations and adequately protect personal data. Ongoing checks must be performed to ensure compliance levels are maintained

New obligation: The mandatory content of data processing contracts has been extended. There will be direct statutory liability and specific responsibilities for 3rd parties processing personal data on behalf of organisations under GDPR

New & enhanced obligations: Individuals will have greater rights, including the rights to have data erased, held in restricted storage and downloadable in a portable format

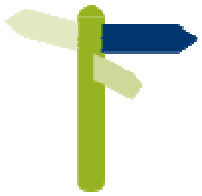
Enhanced obligation: Organisations will only have 30 days, rather than the current 40 days in the UK, to process subject access requests

Security and Retention



Existing obligation: As under current rules, personal data should only be retained in identifiable form for as long as it is needed for the purpose for which it was originally collected.

Existing obligation: As under current rules, only the personal data needed for a specific purpose should be collected (the principle of data minimisation) – if identifiable data is not needed anonymization or aggregation should be used instead.



ONLY FOR USE BY MORTGAGE INTERMEDIARIES