UK FINANCE

Frequently Asked Questions on the General Data Protection Regulation (GDPR)

What is the General Data Protection Regulation (GDPR)?

The General Data Protection Regulation (GDPR) is an EU law aimed at protecting privacy and ensuring that all firms, including in the financial services industry, take proper care when handling consumers' personal data.

The GDPR comes into force on 25 May 2018 and will replace the 1995 EU Data Protection Directive, which formed the basis for the 1998 Data Protection Act in the UK.

The GDPR builds on previous data protection laws and updates them to reflect recent developments such as the growth of the digital economy, the internet and big data. It will also ensure varying data protection rules across different EU countries are more closely aligned.

How will GDPR impact on consumers of financial services?

Individuals' rights over their personal data will be expanded. In particular:

- Firms will need to explain in more detail how a customer's personal data is used, for example websites will have more detailed 'privacy notices'.
- Customers will have better access to information about who their personal data has been shared with.
- Customers will be able to request that inaccuracies in data about them are corrected.
- In some situations, customers will be able to withdraw their consent and request that firms stop processing their personal data (see below for more detail).
- In some specific cases, customers will be able to request that personal data about them is erased under the 'right to be forgotten' (see below for more detail).

Other key aspects of the new rules include:

- Firms will need to put in place special safeguards if they use automated processes to make decisions that would have a significant effect on a customer, such as potentially when deciding whether to provide a loan.
- There will be more transparency around serious data breaches. If a customer's personal data is compromised in a breach and this poses a high risk, the company will have to inform the person affected (except in very specific cases, for example when this would tip off a criminal that they are being investigated).
- As now, a customer will be able to request a copy of data held about them, which will need to be provided within one month (or sometimes longer if there are a lot of data requests or if the request is complex).

What changes will financial services customers notice most?

Most of the changes will be behind the scenes. The most obvious sign of GDPR to customers will be that businesses in all sectors, including financial services, will be updating their 'privacy notices' that explain the personal data they collect and how it is used. Consumers will likely receive notifications of these updates from some businesses. For example, people may have noticed internet search engines and other websites using pop-ups to let users know that their privacy policies are changing.

Consumers are likely to receive more detailed information about how their personal data will be used when they download a new app or sign up for a new service.

How will the obligations on firms change?

Firms will need to have comprehensive systems in place to ensure they are complying with the new standards and protecting personal data effectively. The exact requirements will depend on the firm and its business, but changes will generally include:

- Building privacy and data protection into new products from the start of the design process. This includes using 'data protection impact assessments' to evaluate high-risk new products and services and ensuring appropriate safeguards are in place when designing them.
- Keeping detailed records of all personal data held, such as the reason it is needed and how long it is required for.
- Notifying the Information Commissioner (ICO) of personal data breaches and notifying individuals if the breach poses a high risk for them.
- Appointing a 'data protection officer' to help ensure high standards are maintained.
- Explaining to customers how their data is used in more detail than before.
- High standards of information security, for example using encryption when appropriate.
- More detailed rules for outsourcing, to make sure that any external providers meet the necessary standards.
- In addition, if firms want to transfer data out of the EU they will need to put in place special protections. These are similar to the current Data Protection Act rules, and include:
  - Signing specially designed contracts with data recipients out of the EU, to ensure they look after the data properly.
  - Getting a group-wide data protection policy approved by the ICO so that international business groups can share personal data with other group firms.

How will it be enforced?

Like the current Data Protection Act, the GDPR will be enforced in the UK by the Information Commissioner's Office (ICO).

However, the enforcement framework will become stronger. The ICO will have enhanced powers to enforce the rules and the maximum fines for breaches will increase.

Will firms always need a customer's consent to process personal data?

The GDPR introduces stricter standards when obtaining an individual's consent to process their personal data, including allowing individuals to withdraw this consent at will. However, the rules also recognise that obtaining a customer's consent is not always appropriate, for example where firms have to process data in order to comply with a legal obligation, to perform a contract or where they have a 'legitimate interest' in processing the data (see details below).

For example, in the context of financial services a firm would not need to ask a customer for consent when processing data needed to detect fraud and money laundering, as this would allow criminals to withdraw their consent and escape detection. Similarly, a lender would not have to ask for consent when processing personal data needed to provide a loan, as the borrower would later be able to withdraw their consent to avoid making repayments. As most personal data processing by financial sector firms will be necessary to comply with legal obligations or to ensure contracts with customers can be enforced, consent will often not be required.

Whether or not a firm is asking for consent, it will still need to provide a comprehensive explanation of how personal data will be used. It's important for consumers to read this information and make sure they are comfortable before signing up for a service.

What sort of data processing could be considered in a firm's 'legitimate interests'?

Firms will be permitted to process data without asking for consent when they can show they have a 'legitimate interest' in doing so, for example for commercial interests, fraud prevention or IT security. For instance, a financial services sector firm may need to collect personal data to help it detect fraud and protect its customers.

When relying on legitimate interests, firms need to make sure that personal data is only used in ways that are fair and proportionate. If the potential negative impact on the individual outweighs the need for data by the firm, then it will not be able to collect the data.

Again, whether nor not firms ask for consent, they need to explain their processing and customers should read this information carefully.

More information:

ICO information on when personal data can be processed: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/

ICO information on consent under the GDPR: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/

For companies that do ask for consent, how will this change under the GDPR?

If a firm does seek consent, it will need to meet new, higher standards. For example, consent will require a 'clear affirmative action' so consumers will need to 'opt in' for consent to be valid, with 'opt out' boxes needing to be phased out. Similarly, the request for consent will have to be prominent, more detailed and more direct than in the past.

More information:

ICO guidance on consent under the GDPR: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/

What about the 'right to be forgotten'? Can a customer force a company to delete all the data they hold on them?

The 'right to erasure' or 'right to be forgotten' allows individuals to request that personal data held by firms about them is erased. Individuals can make a request for erasure verbally or in writing and firms then have one month to respond.

However, the 'right to be forgotten' is not absolute. It can only be invoked in specific circumstances, such as where data has been processed illegally, where the data is no longer needed by the firm or where the individual has withdrawn consent for the data to be processed (see above).

If the right is invoked, it can be overridden in some situations, for example if the firm needs the data to comply with a legal requirement, for reasons of public interest or as part of legal proceedings.

The financial services industry has many regulatory obligations that require them to retain data, for example anti-money laundering rules, so in practice a lot of the data held by firms in the sector will not be able to be erased in this way.

More information:

ICO information on the right to erasure: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/

Will people still be able to make a 'subject access request' to a company and get a copy of their personal data?

Yes, the right to access your personal data will stay in place under the GDPR. Firms will generally need to respond within one month but can take longer if there are a lot of data requests or if the request is complex.

How will the GDPR impact marketing?

The Privacy and Electronic Communication Regulations (PECR) currently require firms to obtain consent for direct marketing to individuals. Firms can also market directly where they have an existing relationship with the customer without consent, provided they give the customer an 'opt out'. This will remain the same under GDPR, but firms getting consent will now need to meet new GDPR standards (see above). Individuals will continue to have a right to unsubscribe to direct marketing at any time.

More information:

ICO guidance on direct marketing: https://ico.org.uk/for-organisations/guide-to-pecr/electronic-and-telephone-marketing/

How does the GDPR relate to the Data Protection Bill currently going through Parliament?

The GDPR provides most of the over-arching rules, but it leaves some areas where national governments can set the detail. The Data Protection Bill fills this space. In relation to financial services, for example, the Bill clarifies that firms can process personal data to detect and prevent unlawful behaviour such as fraud or money laundering.

The Data Protection Bill also applies data protection rules to law enforcement and intelligence services, as these are not covered by the GDPR directly.

Lastly, the Data Protection Bill introduces new criminal offences to enhance protections. In particular,

- It will be a criminal offence to knowingly obtain or disclose personal data without the permission of the firm responsible for that data.
- It will be a criminal offence to sell illegally obtained personal data.
- Where a firm has removed personal details from a dataset so that individuals cannot be identified, it will be an offence to try to 'reverse engineer' their identities without the firm's permission.

Is there any connection with Open Banking or the Payment Services Directive 2?

The goal of the GDPR is to protect individuals' rights, by giving them control over their personal data and requiring firms to take appropriate care when processing it.

Open Banking and the Payment Services Directive 2 (PSD2) are primarily about innovation and encouraging new market entrants. They allow customers to transfer their online banking data from their bank (or other account provider) to 'third party providers' like mobile apps. This will help third party providers to develop innovative services, such as personalised account comparisons.

GDPR means that PSD2 and Open Banking must be implemented carefully, both by banks and non-bank service providers handling customers' account data.

More information:

UK Finance FAQ on Open Banking and the Payment Services Directive 2: https://www.ukfinance.org.uk/wp-content/uploads/2018/01/Frequently-Asked-Questions-on-PSD2-and-Open-Banking.pdf

What impact will Brexit have?

Data protection standards should remain the same after the UK leaves the EU. The Data Protection Bill and the European Union (Withdrawal) Bill will apply GDPR directly into UK law. This means that post-Brexit the GDPR's protections and rules will continue to apply in the UK, subject to a few necessary changes to accommodate the UK's exit, such as changing references in the legislation to UK institutions instead of EU ones.

However, Brexit could impact on the transfer of personal data. Under the GDPR (as under the current rules) firms can transfer personal data around the EU freely, as all companies within the EU need to meet the same standards of protection. However, after the UK leaves the EU it will become a 'third country'. Transfers to 'third countries' are prohibited unless the transferring firm puts in place special protections, which can be complex and costly. The same will be true for transfers out of the UK to the EU unless a separate agreement is reached. This creates a risk of disruption to the digital economy of both the EU and the UK.

To address this problem and maintain the free flow of data, UK Finance is calling for the UK and the EU to recognise each other's respective data protection frameworks as 'adequate'. Mutual adequacy agreements would mean firms can continue transferring personal data between the two jurisdictions freely after Brexit, as they can today. To achieve this outcome:

- Both the EU and the UK should begin their adequacy assessment processes as soon as possible.
- A 'stand still' transitional arrangement for a set term in order to avoid a cliff-edge in the movement of personal data should be agreed immediately.
- The UK should consider implementing additional measures to ensure that any EU concerns about the UK's data protection framework are addressed, particularly regarding processing of data for UK national security purposes.
- The UK should ensure that its international and 'onward transfer' regimes, including with the US, provide equivalent levels of protection to those set out in the EU's regime, as this will form a key part of the EU's adequacy assessment.

More information:

UK Finance 'quick brief' on the movement of personal data post-Brexit:

https://www.ukfinance.org.uk/wp-content/uploads/2017/11/BQB5-Data-protection-and-transfer-NEWER-FINAL.pdf

A more detailed UK Finance report on the movement of personal data post-Brexit:

https://www.ukfinance.org.uk/no-interruptions-options-for-the-future-uk-eu-data-sharing-relationship/

What is UK Finance doing?

UK Finance is working closely with members, the Government and regulators to ensure that the GDPR is effectively implemented in the UK. This means in particular ensuring that firms can continue to meet their wide-ranging obligations, including protecting customers, managing risk and preventing crime such as money-laundering and fraud. Firms need to be able to achieve these important objectives while also meeting the GDPR's data protection and privacy standards.

Where can I find out more?

The Information Commissioner's Office has a lot of resources on GDPR available here:

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

The Information Commissioner's blog is also a useful source of information on topical GDPR and other privacy issues:

https://iconewsblog.org.uk/category/elizabeth-denham/

Technical guidance from the Article 29 Working Party (made up of the ICO and other EU data protection authorities):

http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358

Information on the Data Protection Bill is available on the Parliament website:https://services.parliament.uk/Bills/2017-19/dataprotection.html