SLAUGHTER AND MAY

The General Data Protection Regulation: what financial institutions need to know

July 2016

The General Data Protection Regulation (GDPR) marks a significant development in the field of EU data protection law. The GDPR will have direct effect in all EU Member States from May 2018. It will replace current EU data privacy laws including the Data Protection Directive 95/46/EC and will lead to the repeal of the UK Data Protection Act 1998.

While some of the basic principles of the existing regime will be retained, the GDPR will introduce several new concepts and new data subject rights. Some of these could have a significant impact on financial institutions and may require a change to both the handling and use of personal data. We set out in this briefing the ten most relevant aspects of the new regime for these firms.

The FCA and PRA have demonstrated their concern for data security by issuing significant fines to firms that do not meet required standards. The level of fines that can be imposed under the GDPR (see further below) will provide ample reason for regulated firms to invest in ensuring compliance in this area.

In terms of scope, it is worth noting that the GDPR will apply to controllers and processors of data established both inside and outside the EU whose processing activities relate to the offer of goods or services to individuals in the EU. In practice this means firms established outside the EU but targeting customers inside the EU will have to meet GDPR standards.

1. Accountability and transparency

Accountability is one of the core principles of the GDPR. Data controllers will need to demonstrate that any processing activities undertaken comply with the GDPR's requirements and keep records of those activities to be made available to supervisory authorities on request. The principle of accountability is new in the context of data protection law. However financial institutions are already subject to comparable obligations under the FCA's regulatory regime, including the requirement to take reasonable care to organise and control their affairs responsibly and effectively with adequate risk management systems.

There is also an overarching transparency requirement in the GDPR. Data controllers will need to provide more detailed information notices to data subjects regarding the processing of their data. Financial institutions will need to ensure that their notices contain the comprehensive list of items of information that need to be communicated to data subjects under the GDPR, and provide that information in a 'concise' and 'intelligible' way.

2. Consent

Much of the processing of personal data that takes place today in the UK by regulated and non-regulated firms relies on the 'legitimate interests' or 'consent' ground, both of which remain a lawful basis for the processing of data under the GDPR. Consent under the GDPR must be 'freely given, specific, informed and unambiguous' and, in some cases, 'explicit' (including in relation to the processing of 'sensitive' data, which will expressly include genetic and biometric data). Consent may be provided via a written or oral statement from the data subject or by clear affirmative action which signifies the data subject's agreement to the processing. Silence, the use of pre-ticked boxes or inactivity are unlikely to amount to consent. 'Explicit' consent will require the data subject to actually 'opt in' (via a tick box, for example) or a declaratory consent.

The standard of consent is more exacting under the GDPR, compared to the existing Data Protection Directive, in several respects. A controller may not make a service conditional upon consent, unless the processing is necessary for the service. Consent must be specific to each data processing operation. The data subject will also have a right to withdraw consent and 'it shall be as easy to withdraw consent as to give it'.

3. 'Privacy by design' and 'default'

Under the GDPR data controllers will be required to consider privacy risks at the outset of any new project, referred to as 'privacy by design'. Financial institutions should already be taking data privacy into account throughout the lifecycle of any data processing; once the GDPR applies they will find themselves subject to a specific obligation to consider data privacy as any new products and services are developed. Firms that already do this as a matter of best practice will have a head start on compliance; others may need to implement changes to their policies, procedures and systems.

A specific 'privacy by default' requirement will also apply. Controllers will need to minimise the amount of the data collected, the extent of processing, the period of their storage and their accessibility. This means financial institutions should, by default, only process personal data to the extent necessary for their intended purposes and should not keep it for longer than is necessary for these purposes. To achieve this in practice, firms are likely to consider increasing the use of pseudonymisation techniques.

4. The future of big data and 'profiling'

Financial institutions are continuing to learn about big data technologies and deploy them in their businesses to improve customer intelligence, reduce risk, and meet regulatory objectives. The use of telematics data to assist in the insurance underwriting process, for example, has been well-documented, including in the FCA's Call for Input on Big Data in the retail general insurance sector, published in November 2015[1].

The existing tension between current data protection law and the use of big data is likely to come into sharp focus once the GDPR applies. This tension was identified in the FCA's Feedback Statement on its

[1] https://www.fca.org.uk/news/big-data-call-for-inputs-published

Call for Input: Regulatory barriers to innovation in digital and mobile solutions published (FS16/2) in March 2016[2]. Unlike the DPA, the GDPR imposes specific constraints on 'profiling', defined as 'any form of automated processing of personal data …using those data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements'.

In short, where profiling is the basis of automated decision-making, it will be permitted under the GDPR if the data subject has provided 'explicit' consent; where it is necessary for the performance of a contract; or otherwise permitted under the applicable law. Firms that conduct big data activities will need to consider ways in which they can satisfy this standard. There are likely to be some uncertainties in practice, particularly in the absence of legislation that expressly permits a type of profiling currently undertaken. For example, it might be difficult for a firm to argue that profiling for fraud analysis is strictly necessary for the performance of the relevant contract.

Profiling will also be permissible under the GDPR when it does not 'produce legal effects concerning [the individual] or similarly significantly affects him or her'. The interpretation of this phrase may ultimately vary between member states, though the Recitals provide as an example 'the automatic refusal of an online credit application'. 'Profiling' on the basis of sensitive personal data (e.g. health) will only be permitted in exceptional circumstances.

Firms that make use of profiling will need to conduct a data impact assessment. This requires data controllers to evaluate the necessity and proportionality of the proposed processing, how it impacts on the privacy of the individuals involved and measures the data controller will take to address those risks.

5. Data subject rights - data portability and the 'right to be forgotten'

Under the GDPR, individuals can ask to receive back their personal data in a useable format so that it can be transferred to another data controller (referred to as data portability) or have their personal data erased in some circumstances (known as the 'right to be forgotten'). Individuals will also have the right to opt-out of direct marketing.

The right to be forgotten is exercisable where data is no longer necessary for the purposes for which it was collected or processed. It does not apply to the extent that processing of personal data is necessary, for example, 'for compliance with a legal obligation which requires processing of personal data by Union or Member State law to which the controller is subject'.

To be able to meet these requirements, financial institutions will need to put in place the right processes to be able to search for and extract all personal data relating to a particular data subject, and then to transfer it to a new provider, or erase it. Services offered by digital rights management organisations,

[2] https://www.fca.org.uk/your-fca/documents/feedback-statements/fs16-02

including the creation of a digital vault in which consumers can store their personal data, may prove useful in this regard.

6. New fines and penalties

The FCA and ICO set out their working arrangements, including in an enforcement context, in a Memorandum of Understanding dated 28 January 2015. The ICO currently has a range of powers available to it to ensure that organisations comply with data protection requirements, including the possibility of levying fines of up to £500,000. Breach of FCA requirements, of course, carries potentially greater penalties. Data protection is already an area of potentially serious legal and reputational risk for financial institutions.

Under the GDPR various sanctions can be imposed for breach of requirements - including fines of up to 4% of annual worldwide turnover or EUR 20,000,000, whichever is highest, in respect of some serious breaches. Going forward, firms will need to be prepared for the possibility of the ICO taking stricter enforcement action independently of the FCA and using its increased fining powers. Sanctions under the GDPR are required in each individual case to be 'effective, proportionate and dissuasive' and will depend on a range of factors including the 'technological and organisational measures and procedures' implemented by the data controller.

7. Cross-border data sharing

There is no radical departure from existing requirements governing international transfers of data. Data transfer compliance will remain a complex issue for international organisations and for firms using supply chains to process personal data outside the EEA.

As is currently the case, firms will be prohibited from transferring personal data outside the EEA to a third country that does not have adequate data protection measures in place. The European Commission currently has the power to approve particular countries as providing an adequate level of data protection and it is envisaged that this will continue under the GDPR (which also provides for the designation of one or more specified sectors within the third country as providing an adequate level of data protection).

A number of alternative arrangements will be available for international transfers of data. A controller or processor may transfer personal data to a third country if that controller or processor has adduced 'appropriate safeguards' and on condition that 'enforceable data subject rights and effective legal remedies for data subjects are available.' There are also derogations where 'the data subject has explicitly consented to the proposed transfer' and where 'the transfer is necessary for important reasons of public interest.'

The GDPR allows for transfers of personal data based on standard data protection clauses (i.e. Model Clauses) adopted by the Commission and gives official recognition to the possibility of transfers based on an organisation's approved Binding Corporate Rules. Such transfers may be made without requiring specific authorisation from a supervisory authority.

8. Reporting breaches

The GDPR will introduce a mandatory data breach notification to the supervisory authority without undue delay (72 hours where feasible), unless the breach is 'unlikely to result in a risk for the rights and freedoms' of individuals. This may appear to a challenging timescale, but in practice many financial

institutions will already have procedures and policies in place to handle breaches and ensure they can notify when required. Indeed, the UK ICO already expects all data controllers to report 'serious breaches'.

Firms will be well-advised to review their reporting lines to ensure that any data breaches – whether occurring within the firm or reported by a data processor engaged by the firm – can be identified and dealt with appropriately.

9. Data protection officers

Data protection officers will need to be appointed by controllers and processors in certain circumstances including when their core activities consist of processing operations which require regular and systematic monitoring of individuals on a large scale. The majority of large organisations will be caught by this requirement including, for example, large insurers using telematics technologies to collect and process personal data.

10. Impact of Brexit

Financial institutions should not let Brexit become a distraction from their current plans and strategies to implement the GDPR. Any formal UK exit from the EU is likely to occur after the GDPR becomes applicable law in Member States in May 2018. Moreover, if the UK negotiates to join the EEA, the GDPR will continue to apply post-Brexit. If the UK does not join the EEA, the GDPR will in any event continue to apply to all UK entities that do business in the EU.

There will, in any event, be significant pressure from the UK business community for the UK Government to reform the current UK data protection regime in line with the GDPR. One reason for this will be to ensure the UK (assuming it does not join the EEA) obtains an 'adequacy decision' from the EU Commission for the free flow of personal data from the EEA to the UK, without the additional regulatory and administrative burden of EU standard model clauses or binding corporate rules. To achieve this adequacy decision, the EU Commission will want the UK to implement similar standards of compliance as required under the GDPR. Moreover, many multinationals have used, and will continue to use, the EU standards of compliance as their 'highest common denominator' across their global operations.

In conclusion: financial institutions should now be taking steps to anticipate and where necessary adjust for the application of the GDPR from May 2018. This should include seeking to understand the data currently being held by the firm, what processing of data is undertaken, and whether that processing is based on consent. Once that process is complete firms can assess whether additional measures will need to be taken before 2018.

If you would like to talk about any of the matters raised in this briefing, please speak to your usual contact at Slaughter and May.