Feature

KEY POINTS

- The new EU data protection framework contains changes of emphasis and substance which are intended to strengthen the rights of EU data subjects, to extend the territorial scope of protection of EU data subjects to controllers established outside the EU, to achieve consistency across member states, and to ensure compliance by strong sanctions.
- These changes are of potential importance to all data controllers which process the data of EU data subjects, wherever they are based, and they need to evaluate and if necessary act upon the new requirements now in order to be in a position to comply with the revised regime when it comes into force and to avoid potentially serious sanctions.
- The challenges for banks and other financial institutions include the specific topics which are discussed in this article (data subject consent, the right of erasure, and international transfers of data), and meeting them is likely to require the investment of significant resources, but the framework is not unworkable and with sufficient effort they can be met.

Author Richard Spearman QC

The new EU data protection framework: do banks have grounds for concern?

This article considers some aspects of the debate about whether the General Data Protection Regulation may adversely affect the ability of banks to protect their own interests and to carry out their legal obligations.

The foundation of current European Union (EU) legislation concerning personal data is Directive 95/46/EC. This has two main objectives: first, upholding the fundamental right to data protection; and, second, guaranteeing the free flow of personal data between member states. However, the current regime was considered to be flawed, among other things because personal data protection was fragmented in the EU and due to the complexity of the rules on international transfers of data.

The European Commission concluded that the EU required a more comprehensive ... policy concerning the fundamental right to personal data protection.

The European Commission concluded that the EU required a more comprehensive and coherent policy concerning the fundamental right to personal data protection. The European Parliament and the Council of the European Union concurred. On 15 December 2015, after protracted "Trilogue" negotiations, the Commission, Parliament and Council of Ministers reached agreement on the Commission's proposal for a General Data Protection Regulation (GDPR) to replace the current Directive. The GDPR will come into force after a two year implementation period, and will be directly applicable in all member states without the need for implementing national legislation. The purpose of this article is to examine the GDPR from the perspective of banks (and other financial institutions), and to consider some ways in which it impacts on them.

THE CONTEXT: THE GDPR IN OUTLINE

The GDPR is detailed and complex, and even a cursory analysis of its provisions overall is beyond the scope of the present article. Nevertheless, the broad thrust of the new framework which the GDPR contains can be gleaned from the Recitals.

These refer, for example, to the fact that technological developments and globalisation 'require a strong and more coherent data protection framework in the Union, backed by strong enforcement'. The Recitals also refer to the considerations that:

> 'In order to ensure consistent and high level of protection of individuals and to remove the obstacles to flows of personal data within the Union, the level of protection of the rights and freedoms of individuals with regard to the processing of such data should be equivalent in all Member States'

and that:

> 'Effective protection of personal data throughout the Union requires strengthening and detailing the rights of data subjects and the obligations of those who process and determine the processing of personal data, but also equivalent powers for monitoring and ensuring compliance with the rules for the protection of personal data and equivalent sanctions for offenders in the Member States'.

So far as concerns territorial scope, the Recitals state that:

> 'Any processing of personal data in the context of the activities of an establishment of a controller or processor in the Union should be carried out in accordance with this Regulation, regardless of whether the processing itself takes place within the Union or not'

and that,

> 'In order to ensure that individuals are not deprived of the protection to which they are entitled under this Regulation, the processing of personal data of subjects who are in the Union by a controller or a processor not established in the Union

should be subject to this Regulation where the processing activities are related to the offering of goods or services to such data subjects irrespective of whether connected to a payment or not … [or] to the monitoring of the behaviour of such data subjects as far as their behaviour takes place within the European Union.'

Member states are required to establish supervising authorities, which shall have a range of investigative and corrective powers. These include, for example, carrying out data protection audits, issuing warnings and reprimands, imposing a limitation or even a ban on processing, and requiring a data controller or processor to bring operations into compliance with the GDPR or to comply with a data subject's requests or to communicate a personal data breach to the data subject.

Various sanctions may be imposed for breach, including fines of up to 2% of worldwide turnover in respect of some breaches and up to 4% of worldwide turnover in respect of others. These sanctions are subject to the basic criteria that they should be 'in each individual case effective, proportionate and dissuasive'. Their effect in practice will depend upon a range of matters, including 'the nature, gravity and duration' of the breach, whether it was 'intentional or negligent', and the 'technological and organisational measures and procedures' implemented by the data controller for ensuring 'data protection by design and by default'. This last factor involves 'ensuring that, by default, only those personal data which are necessary for each specific purpose of the processing are processed and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage'. It also illustrates a point of considerably wider application, namely the importance for data controllers of reviewing, and if necessary adapting, current processes and products well in advance of the date when the GDPR is to come into force.

All these features of the new EU regime are of importance to any data controller. However, there are some aspects of the new framework which have been identified by commentators as being of particular relevance (and, indeed, potential concern) to banks and other financial institutions, and it is those specific aspects which this article now turns to consider.

THE DATA SUBJECT'S CONSENT

One concern which was expressed in advance of knowing the likely form which the GDPR would take is that banks would need to obtain their customers' consent to their personal data being used for purposes which are in the interests of the bank, such as modelling loan losses or dealing with fraud, and that, in the absence of such consent, banks would be exposed to an invidious choice of either having to forego uses which are of benefit to them or risk exposure to serious sanctions.

> … the consent of the data subject is only one of the grounds on which the processing of personal data may be lawful.

One of the grounds which may render the processing of personal data lawful is that the data subject has given consent to the processing of his or her personal data for one or more of the specified purposes. Consent in this context means 'any freely given, specific, informed and unambiguous indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed'. The conditions for consent include that the data controller should be able to demonstrate that consent was given; that where consent is given in writing the request for consent should be clearly, intelligibly and accessibly distinguishable from any other matters; that the data subject should have the right to withdraw consent (but not with retrospective effect); and that:

'When assessing whether consent is freely given, utmost account shall be taken of the fact whether, among others, the performance of a contract, including the provision of a service, is made conditional on the consent to the processing of data that is not necessary for the performance of this contract'.

Processing of personal data in special categories (such as data which reveals racial or ethnic origin, and data concerning health or sexual orientation) is prohibited without the explicit consent of the data subject, except where the laws of the EU or those of a member state provide that this prohibition may not be lifted by the data subject. Existing consents may satisfy these conditions, but they will need to be checked to see whether or not they do so.

However, the issue of the consent of the data subject needs to be placed in context. On the one hand, the overarching principles relating to personal data processing are that personal data must be 'processed lawfully, fairly and in a transparent manner in relation to the data subject' (the principle of "lawfulness, fairness and transparency") and in accordance with other principles, which are known, for short, as "purpose limitation", "data minimisation", "accuracy", "storage limitation" and "integrity and confidentiality". The data controller is responsible for, and is required to be able to demonstrate compliance with, these principles ("accountability"). On the other hand, the consent of the data subject is only one of the grounds on which the processing of personal data may be lawful. Other grounds include that 'processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller' and that 'processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in

particular where the data subject is a child'. Accordingly, the consent of the data subject is neither a necessary nor a sufficient basis for rendering lawful the processing of his or her personal data.

This language differs in a number of respects from that of the current EU framework, and in a manner which, overall, undoubtedly tends to enhance the rights of data subjects and to bolster the obligations and restrictions to which data controllers are subject. This is only to be expected in light of the general objectives of the new framework which are discussed above. It is also in keeping with (for example) the recognition in the Recitals to the GDPR that, 'Effective protection of personal data throughout the Union requires strengthening and detailing the rights of data subjects and the obligations of those who process and determine the processing of personal data'.

Nevertheless, these aspects of the new framework are not drastically different from the equivalent provisions in the current regime. Directive 95/46/EC was transposed into the law of England and Wales by the Data Protection Act 1998, which includes a requirement that (in the context of a banker/customer relationship) a customer's personal data shall not be processed unless the processing is necessary for the purposes of legitimate interests pursued by the bank or by the person(s) to whom the data are disclosed. In *Murray v Express Newspapers Ltd* [2007] EMLR 583 (reversed on appeal on a different point – see *Murray v Express Newspapers plc* [2009] Ch 481) Patten J held at [76]:

> 'It seems to me that "necessary" in this context means no more than that the processing should be required to be proportionate to the legitimate interests pursued by the data controller and I accept [the] submission that the pursuit of a legitimate business is a legitimate interest for these purposes. This condition seems to me to replicate the considerations which the Court has routinely to take into account under Article 8 and Article 10 [of the European Convention on Human Rights]… .'

The correct approach to the balancing exercise where both Art 8 and Art 10 rights are involved is that: (i) neither Article as such has precedence over the other; (ii) where the values under the two Arts are in conflict, an intense focus on the comparative importance of the specific rights being claimed in the individual case is necessary; (iii) the justifications for interfering with or restricting each right must be taken into account; (iv) finally, the proportionality test – or "ultimate balancing test" – must be applied to each (see *Re S* [2005] 1 AC 593, Lord Steyn at [17]). In this way, the rights of data subjects are not given undue weight.

On that basis, it would not appear that the new framework has brought about any major sea change in this particular area.

> If a structured approach is adopted, the ability to cater for the right to erasure should fall into place as part of a wider compliance exercise.

No doubt banks would be well advised to exercise increased vigilance to ensure that there is no infringement of the rights of data subjects. That is appropriate in light of both the "strengthening and detailing" of those rights and the increased penalties to which the GDPR gives rise. But there seems no reason to suppose that the new framework promotes those rights unduly.

THE DATA SUBJECT'S RIGHT TO ERASURE

In accordance with the GDPR, the data subject has the right to obtain, and the controller has the obligation to provide, erasure of his or her personal data without undue delay where various grounds apply. These include where the data subject withdraws consent, where the data have been unlawfully processed, where the data are no longer necessary in relation to the purposes for which they were collected or processed, and where the controller is under a legal obligation to erase the data.

These rights and obligations do not apply to the extent that the processing of the personal data is necessary for various reasons. These include 'for compliance with a legal obligation which requires processing of personal data by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller' and 'for the establishment, exercise or defence of legal claims'.

These rights and obligations have generated widespread debate, not least in the context of the judgment of the Grand Chamber of the Court of Justice of the EU in *Google Spain SL and Google Inc v Agencia Espanola de Proteccion de Datos and Mario Costeja Gonzalez* [2014] ECDR 16. The right to erasure is also referred to parenthetically in the GDPR as the "right to be forgotten", and the ramifications of that case are reflected in the provisions in the GDPR which require controllers who have made public the data which they are required to erase to take steps 'to inform controllers which are processing the data, that the data subject has requested the erasure by such controllers of any links to, or copy or replication of that personal data' and in the exception where processing of the data is necessary for exercising Art 10 rights.

However, the concern which has been expressed with regard to these provisions in relation to banks does not involve such controversial matters. Instead, it relates to whether banks have mechanisms in place to delete customer data in response to a legitimate exercise of the right to erasure. This concern is well-founded. Moreover, the right to erasure cannot be viewed in isolation. The need to be prepared to deal with requests for erasure is only one aspect of the overall desirability of moving toward compliance with the requirements of the GDPR before it comes into force. Nevertheless, this cuts both ways. If a structured approach is adopted, the ability to cater for the right to erasure should fall into place as part of a wider compliance exercise. For example, the basis on which the data subject's consent is sought and obtained will impact on whether and in what circumstances that consent

Biog box
Richard Spearman QC practises from 39 Essex Chambers. He has a wide ranging commercial, chancery and common law practice. His many reported cases include those concerning freezing injunctions, letters of credit, civil fraud, tracing, judicial review, insurance, banking, defamation, copyright, confidence, private information and data protection.
Email: richard.spearman@39essex.com

can be withdrawn; and the extent to which there is "accountability" – in other words, demonstrable compliance with the principles of "lawfulness, fairness and transparency", "purpose limitation", "data minimisation", "accuracy", "storage limitation" and "integrity and confidentiality" – will impact on whether the data have been unlawfully processed or are no longer necessary in relation to the purposes for which they were collected or processed.

If careful consideration is given to matters such as what processing of customers' data is undertaken, the nature and extent of that processing and the reasons for it, and whether that processing is based on the data subject's consent or on some other legal foundation, that should go a long way towards putting in place mechanisms for assessing whether requests for erasure are legitimate and, if so, for complying with them. This may not be easy or cheap to do, but it should be achievable.

TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES

The concern which has been expressed in this regard is that the new framework could prohibit international transfers of data even where the sharing of data is intended to aid the detection and prevention of terrorist financing and other criminal acts.

In fact, under the current regime the primary general principle is that member states shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if that third country 'ensures an adequate level of protection', which is to be assessed 'in the light of all the circumstances'. This is subject to a number of derogations, which provide that transfers to a third country which does not ensure an adequate level of protection may take place where (among other things) the data subject has given unambiguous consent to the proposed transfer or 'the transfer is necessary or legally required on important public interest grounds'. In addition, member states may authorise transfers to a third country which does not ensure an adequate level of protection 'where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights'.

The core concept of an adequate level of protection is maintained in the new framework. In accordance with the new framework, this is to be decided by the Commission. Further, in the absence of an adequacy decision by the Commission, a controller or processor may transfer personal data to a third country only: (i) if the controller or processor has adduced "appropriate safeguards" (which are set out in the GDPR); and (ii) 'on condition that enforceable data subject rights and effective legal remedies for data subjects are available'. The new framework also provides for derogations for specific situations, including where 'the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards' and where 'the transfer is necessary for important reasons of public interest'. It also contains a new derogation (which applies where none of the other bases for transfer to a third country which does not ensure an adequate level of protection are available) where 'the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the data controller which are not overridden by the interests or rights and freedoms of the data subject, [and] where the controller has assessed all the circumstances surrounding the data transfer and based on this assessment adduced suitable safeguards with respect to the protection of personal data'. Where this new derogation applies, the data controller must inform the supervisory authority which each member state must designate as having responsibility for monitoring the application of the GDPR and ensuring its objectives are achieved.

In the result, there are some differences in the language used. The GDPR deals with the rights of data subjects in terms which tend to strengthen those rights (for example, by tightening up the wording of the derogation based on the consent of the data subject) and to address them in greater detail (for example, by instancing "appropriate safeguards" at length). However, there is no fundamental change to the current regime. In substance, there would appear to be no greater inhibition on international transfers of data under the new framework. Indeed, although the new derogation is of limited ambit, in circumstances where it applies a transfer may be lawful where it would not have been lawful under the current regime.

CONCLUSION

The new EU data protection framework will undoubtedly present a host of challenges for banks and other financial institutions, including with regard to the specific topics of data subject consent, the right of erasure, and international transfers of data which are discussed in this article. Meeting these challenges will not be easy, and may well require the investment of significant resources. However, the framework is not unworkable, and with sufficient effort those challenges can be met. That effort is likely to require steps to be taken towards compliance well in advance of the date when the GDPR comes into force. Because the GDPR places increased obligations on data controllers and processors, the necessary steps will probably take some time to implement, and the consequences of failing to comply could be both serious and expensive. ■

Further Reading:

- The right to be forgotten: search engines today, banks tomorrow? [2014] 8 JIBFL 514.
- Disclosure of confidential information: Tournier and "disclosure in the interests of the bank" reappraised [2012] 2 JIBFL 78.
- LexisPSL: Financial Services: Data protection and privacy in 25 jurisdictions worldwide.