THOMSON REUTERS
PRACTICAL LAW™

# Know your GDPR: self-reporting and enforcement considerations for contentious regulatory lawyers

by *Stacey McEvoy, Senior Associate, Allen & Overy LLP*

This document is published by Practical Law and can be found at: **uk.practicallaw.com/W-015-3500**
To learn more about legal solutions from Thomson Reuters, go to **legal-solutions.co.uk**

This article considers some specific issues that may arise under the General Data Protection Regulation (*(EU) 2016/679*) (GDPR) in a contentious regulatory context.

RESOURCE INFORMATION

RESOURCE ID

W-015-3500

RESOURCE TYPE

Articles

STATUS

Law stated as at 26-Jun-2018

JURISDICTION

United Kingdom

With the recent implementation of the *General Data Protection Regulation* (*(EU) 2016/679*) (GDPR), many financial services institutions are asking themselves what it may mean from a more traditional financial services regulatory perspective, particularly in terms of firms' ever-present reporting obligations.

This article (originally published as a blog post on Allen & Overy's *Investigations Insight blog*) considers some specific issues that may arise in a contentious regulatory context in relation to document retention, self-reporting obligations and possible overlap between enforcement agencies.

## Competing regulatory obligations: striking the balance

In February 2018, the FCA and the Information Commissioner's Office (ICO) issued a *joint update*, setting out their joint expectations of firms.

The FCA does not believe that the GDPR imposes requirements that are incompatible with rules in the *FCA Handbook*. For example, it points specifically to crossover between the requirement to treat customers fairly, both as part of data protection law and a firm's regulatory obligations.

On the other hand, there may be a tension between regulatory obligations on financial services firms leading to a need or preference to retain data for long periods and firms' general obligation under the GDPR to ensure data is kept no longer than is necessary. For example, firms have enhanced mandatory obligations under MiFID II to store and record communications that resulted in or might result in transactions for five years. Similarly, firms may be facing regulatory investigations (or possible follow-on litigation) for periods stretching back well over five years.

At first glance, retaining documents in such circumstances may be regarded as justifiable on a common sense basis. For the firm, however, it is important to be aware of this potential tension when it comes to handling personal data, consider the firms' legal obligations and ensure that processing is necessary for the purpose of that legal obligation (or justifiable on some other basis). This should be combined with clear decision-making around data handling at all stages of the potential action.

## Self-reporting: to whom?

Regulated firms are well aware of their obligations to comply with *Principle 11* by disclosing to the FCA appropriately anything relating to the firm of which the FCA would reasonably expect notice. An equivalent obligation to notify the PRA is set out in *Fundamental Rule 7*.

Under the GDPR, firms are obliged to report personal data breaches to the competent supervisory authority, where they are the data controller or the user of a data processor suffering a breach. For firms with the UK as their main establishment, this supervisory authority would generally be the ICO. The report must be made without undue delay and (where feasible) not less than 72 hours after the firm becomes aware of the breach.

The only exception where firms do not need to report to the ICO is where the data breach is unlikely to result in a risk to the rights and freedoms of data subjects. In those circumstances, the firm must keep a clear record of its own decision-making process when coming to this view.

In addition, if the breach is likely to result in a "high risk" of adverse effects to individuals' rights and freedoms, the firm must also directly inform the affected individuals without undue delay. This is a higher threshold than for reporting to the ICO: so not every personal data breach will need be reported directly to individuals.

For regulated firms, there is no absolute or express obligation to notify the FCA (or PRA) of all personal data breaches. However, firms will still need to assess on a case-by-case basis whether or not the severity of any incident means that the FCA or PRA must be notified. This would include circumstances where:

- A data breach meets the criteria set out in the FCA's *Supervision manual* (SUP) (for example, because it could have a significant adverse impact on the firms' reputation, or where it could affect the firm's ability to continue to provide adequate services to its customers and which could result in serious detriment to a customer of the firm).
- The breach is a matter of which the FCA may expect notice (for example, if the data breach amounted to a significant failure in the firm's systems or controls).

Firms should anticipate that the FCA and ICO may share information about breach notifications with each other, which may in turn influence reporting decisions.

## If all else fails... what would enforcement action look like?

The enforcement powers of the ICO under the previous Data Protection Act 1998 (DPA 1998) are extended and enhanced under the new *Data Protection Act 2018* (DPA 2018). The DPA 2018:

- Bolsters the ICO's existing power to serve information notices with a sanction if a false statement is made in response to such a notice.
- Broadens the ICO's ability to conduct on-site assessments to all data controllers and processors (as opposed to government departments or public authorities).
- Increases the scope and quantum of penalty notices.

The FCA is continuing to develop its relationship with the ICO post-GDPR, and an updated memorandum of understanding (MoU) between the agencies is expected to be published shortly. The *current MoU*, in place since 2014, provides that both the FCA and ICO have the discretion to alert each other to any potential breaches of legislation applicable to the other regulator it discovers whilst undertaking its duties (subject to any legal restrictions on the disclosure of information). They may also cross-refer matters to each other if the other body is more appropriately placed to deal with an incident.

The ICO will be responsible for regulating the GDPR, but the FCA has been clear that it will also have regard to firms' compliance with the GDPR under its rules. For example, under the FCA's *Senior Management Arrangements, Systems and Controls sourcebook* (SYSC), firms are obliged to establish, maintain and improve such systems and controls as are appropriate to their business, which would include appropriate technology and cyber-resilient systems.

Similarly, the FCA has noted that compliance with the GDPR is a board-level responsibility, and it expects firms to be able to demonstrate that they have taken steps to comply with it. This may also result in queries being asked of senior managers with overall responsibility for any areas suffering from data breaches.

## Where to next?

In the post-GDPR world, regulated firms face uncertain regarding the division of enforcement responsibility when it comes to issues with their handling of personal data. Although there are no recent FCA or PRA enforcement decisions in this space, the financial services regulators may well take an interest should such data breaches be serious enough to amount to a systems and controls issue, or where firms face a risk of serious reputational harm.

In its *2018-19 Business Plan*, the FCA identifies big data and technology as one of its cross sector priorities. Whether one agency would step aside in such a case may come down to the issue of their respective strategic priorities or resourcing. If not, firms may face a "dual-track" investigation with simultaneous scrutiny from the FCA and/or PRA and the ICO.

### Practical Law GDPR toolkit

Practical Law has a toolkit of key resources to assist organisations to comply with the GDPR, see *Toolkit, EU General Data Protection Regulation*.