NEW SQUARE

Professionals, their regulators and personal data breaches: who is in charge of policing the GDPR?

The spotlight on the consequences for professionals of data or confidentiality breaches will only intensify once the GDPR comes into force. Paul Mitchell QC, Stephen Innes and Helen Evans of 4 New Square examine what those consequences are likely to be from a professional regulatory perspective.

Introduction

There have been some high profile data losses by professional firms which have hit the headlines- Mossack Fonseca's loss of the "Panama Papers" being a prime example. Other personal data losses or breaches of confidentiality have not attracted so much attention, but that does not mean that the problem is not a prevalent one. According to the Solicitors Regulation Authority ("SRA"), it receives some 40 reports of confidentiality breaches each month. Further, the Information Commissioner ("ICO") has identified the legal sector as one of the highest sources of data security cases. It is therefore not surprising that the SRA's 2017/2018 Risk Outlook identifies information security as one of its priority areas. The Institute of Chartered Accountants of England & Wales ("ICAEW") is clearly concerned about what the GDPR means for accountants as well: it has published draft engagement letters dealing with data protection rights, as well as detailed guidance on document retention policies. Guidance of this nature is likely to be of great relevance when regulators consider whether members have breached their principles or rules.

How does the GDPR overlap with existing professional regulatory rules?

Professional rules have long required members to keep their clients' affairs confidential. Professional requirements tend to require professionals not only to keep information confidential but to ensure that their employees and staff do too.

In recent years, regulators have also increasingly focused on the need for professionals to take steps to maintain efficient systems and controls to mitigate risks to client confidentiality. Key examples of this two-fold approach are both SRA Outcome 4 and Core Duty 6 (for solicitors) and rC89 in the Bar Handbook (for barristers). The ICAEW (in its Code of Ethics and its GDPR Guidance) also emphasises both the need to keep client's affairs private and to ensure that data protection is take seriously at an organisational level. The latter focus on maintaining appropriate systems is echoed in the GDPR, which requires data controllers to take responsibility for and to be able to demonstrate compliance with the GDPR data protection principles (known as the "accountability principle").

For some professions there is express interplay between data protection law and professional rules; for instance the Bar Handbook states in terms that barristers are under a duty to have proper arrangements in place to protect client confidentiality, which include "complying with data protection obligations imposed by law" (gC134).

Who can bring regulatory or enforcement proceedings against a professional in respect of personal data breaches?

One consequence of the overlap between the GDPR and professional regulatory rules is that professionals may find themselves subject to more than one set of regulatory or enforcement proceedings in relation to a personal data breach.

If there is a personal data breach, Arts 33 and 34 of the GDPR require professionals who are acting as data controllers to report to the ICO, and where the data breach is likely to "result in a high risk to the rights and freedoms of natural persons" and none of the exemptions apply, to the affected data subjects themselves. For these purposes, data breaches include not only losses of personal data to activities such as hacking but disclosure of that data by professionals themselves.

Data subjects are also permitted to report professionals who have failed to comply with the GDPR to the ICO (and this can be a powerful weapon in the armoury of a disgruntled client where the breach in question does not require a professional person to self-report).

The GDPR gives rise to potentially catastrophic levels of "administrative fines". Art 83 of the GDPR (which is expressly referred to in the current Data Protection Bill) provides for the ICO to impose fines that are "effective, proportionate and dissuasive". Depending on what part of the GDPR has been breached, the maximum level of fine set out in the GDPR is either €10m or €20m (or for undertakings, 2% to 4% of annual turnover). The level of potential fine greatly exceeds the maximum fine payable prior to the GDPR (which was £500,000). In addition, the GDPR provides that data subjects will be able to seek awards of compensation.

However, the punishment for data breaches does not end there. The current draft Data Protection Bill also contains various criminal offences relating to mis-use of data.

The fact that the ICO (or indeed the criminal courts) have become involved does not mean that a data controller will not also be pursued by his or her professional regulator. The solicitors' case of *SRA v Nazeer (*2017) is an example of disciplinary proceedings for breach of confidentiality where the ICO had declined to fine or censure a solicitor for leaving confidential documents on top of a bin rather than disposing of them securely.

Further, the SRA's Risk Outlook document for 2017/2018 suggests that even if the ICO levies a heavy fine, the SRA may decide to take further action against a professional person in the public interest. Other regulators, such as accountancy regulators, are likely to take a similar approach to taking measures against their members.

Professional regulatory bodies may receive complaints from clients who have been notified under Art 34 of the GDPR that a data breach has taken place. Alternatively, most professions have some form of rule requiring a member to report certain types of misconduct. The SRA's Outcome 10.3 requires solicitors to "notify the SRA promptly of… action taken against you by another regulator" as well as any "serious failure" to comply with or achieve the principles rules, outcomes and other requirements of the Handbook. The SRA Risk Outlook document for 2017/2018 makes plain that the SRA expects solicitors to report to it losses of client data. These types of rule or standard may lead to double jeopardy for professionals implicated in a personal data breach.

Paul Mitchell QC, Stephen Innes and Helen Evans, 4 New Square
p.mitchell@4newsquare.com, s.innes@4newsquare.com, hm.evans@4newsquare.com