NEW SQUARE

# Civil liability of non-medical professionals for personal data breaches

*In this article, 4 New Square's Paul Mitchell QC, Stephen Innes and Helen Evans consider the potential civil liability of professionals in this jurisdiction for data breaches after GDPR comes into force on 25 May 2018.*

Professionals in England and Wales act as the catalysts speeding up and enabling millions of transactions every year, from the issuance of debt to the valuation and purchase of property, from dispute resolution to mergers and acquisition, from planning to judicial review, from challenging local authorities over schooling and homelessness to immigration. Their skill is the application of judgment to data; through their offices flow the records and the secrets of natural and legal persons across the world.

## The key principle

The GDPR recognises as a "fundamental right and freedom" of all natural persons the power to protect and have control over their "personal data". Personal data is defined as "any information relating to an identified or identifiable natural person". It is convenient to think of this regulation as giving personal data a similar status to money: it now has, of its very nature, a value; and natural persons at least are not to be deprived of it, or control over it, save in tightly regulated circumstances.

Note that the data protected by GDPR do not need to possess any quality of confidentiality per se: this is not a regulation aimed at sophisticated sectors of society's marketplaces, but rather at the creation of a new paradigm for viewing all data pertaining to all natural persons.

At present, the regulation does not apply to data belonging to non-natural persons; but it is to be noted that much data transmitted by non-natural persons to professionals for the purposes of their retainers will relate to natural persons, who in turn will enjoy the protection of GDPR.

## Exposure of professionals to new forms of civil liability

GDPR provides certain basic minimum standards for the treatment of personal data by those responsible for handling it: data "controllers" and data "processors". Data controllers are those who decide the purpose and means of processing personal data, where "processing" means "any operation or set of operations which is performed on personal data… such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclose by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction".

Against a definition of such breadth, it is difficult to conceive of any retainer of a professional involving in any way the consideration of identifiable natural persons which does not engage the professional's obligations under GDPR.

Many professionals are liable to assume that the GDPR will class them as "data controllers" rather than "data processors". For example, the Bar Council's Guide to the GDPR classes barristers in this way. However, in April 2018 the Bar Council became aware that some solicitors' firms were asking barristers to sign contracts which designated them as "data processors". This is potentially problematic for two reasons: first because "data processors" are subject to different duties to "data controllers" and liable for greater penalties but also because the Bar Council regards such arrangements as liable to put barristers in breach of the Code of Conduct (see further our regulatory article here).

**What are professionals obliged to do or prevented from doing?**

Those obligations of a professional acting as a data controller are, in summary, to do as little processing as possible having regard to the purposes for which the data are being processed; to store as little data as possible for as short a time as possible; and to protect the personal data so stored "in a manner that ensures appropriate security of the personal data, including protection against unauthorised and unlawful processing and against accidental loss, destruction or damage".

Natural persons whose personal data are not adequately processed or protected have rights against the controller of their data to compel him or her to grant access to the personal data in its processed form; to compel restriction of the degree of processing; and to seek damages in relation to loss caused by breaches of the GDPR, such loss to include general damages for distress.

GDPR permits national governments to restrict the degree of protection available to protect the administration of justice and in particular the operation of civil litigation, but exactly how the general rules will interact with the exceptions in this country is as yet unknown, since the Data Protection Bill has not yet been passed into law, let alone construed in the context of legal proceedings.

Damages are payable to persons whose rights under GDPR have been infringed and who have suffered damage as a result; it is, however, for the controller or processor who has infringed the right to prove that "it is not in any way responsible for the event giving rise to the damage" (Article 82) if it is to be exempted from paying compensation. The wording governing the standard of proof on the defendant once a prima facie case has been made out suggests that professionals might find it difficult to escape liability entirely for losses alleged to have been caused by their processing failures.

As noted above, only natural persons are protected by GDPR, but in the event a professional caused loss to, say, the lay client of an institution which had instructed the professional, both the professional and the institution could well be liable; and GDPR Article 82 provides for contribution claims between all potentially liable data controllers.

As well as being exposed to civil claims for breach of duty owed under GDPR, data controllers are also liable to very substantial fines in respect of the same breaches. The basis for levying such fines and calculating the quantum is far more refined than the rules relating to the mere awarding of damages (see Article 83). But the sums involved could be very large (and worse for "data processors" than "data controllers").

**Areas of risk of potential civil liability for professionals acting as data controllers**

The most likely areas of risk seem to us to be these:

- Data loss as the result of carelessness by staff (e.g., losing hardware; using employer hardware for personal purposes and picking up viruses etc which permit unauthorised third-party access to personal data processed by the employer);

- Data loss as the result of malicious third-party activity such as hacking;

- Obtaining data regarding natural persons by means that do not involve the consent of the data subject, e.g., by use of private enquiry agents as data processors;

- Accidental disclosure within legal proceedings of privileged material, which could, if it contained "personal data" vest a cause of action in any of the natural persons whose data was so disclosed.

Although it seems likely to be rare for any individual to suffer very large direct financial loss as the result of any breaches by the controller of the GDPR, the fact that compensation may be awarded for "non-material damage" (i.e., distress: see the draft Data Protection Bill, clause 164(1)) suggests that professionals could face numerous small claims, each of which would of course result in the incurring of defence costs.

Given the very strict regime of fines capable of being levied on professionals, and the fact that the way the professional responds to the allegation made by the data subject is likely to be a factor in the calculation of any fine (see GDPR Article 83(2)(c) and (k)), it seems likely that professionals and their insurers will not frequently wish to defend allegations of "non-material" damage with any real enthusiasm, for fear of demonstrating lack of insight into the newly-recognised value of all personal data.

**Conclusions**

The new regime for the protection of personal data appears to be in tune with rapidly-changing public attitudes to the value of privacy; and to a large extent, professionals are already used to treating their clients' data as prima facie potentially confidential. What remains to be seen is the extent to which the new rules alter the traditional relationship between professional and client as the balance of power over personal data shifts in favour of the client.

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