



DATA: set phasers to stun

Is the GDPR likely to lead to a deluge of complaints and litigation by claimants who allege their data protection rights have been infringed?

Deirdre Kilroy looks at the likely impact, through an Irish lens

DEIRDRE KILROY IS A PARTNER IN THE TECHNOLOGY AND INNOVATION GROUP IN MATHESON. SHE WISHES TO THANK MICHAEL FINN, A PARTNER IN THE LITIGATION DEPARTMENT, FOR HIS KIND ASSISTANCE WITH THIS ARTICLE.



The *General Data Protection Regulation* (the GDPR) came into force on 25 May 2018, just 24 hours after the *Data Protection Act 2018*, resulting in the largest overhaul of Irish data privacy laws in over 20 years. The question at the forefront of

many practitioners' minds is whether there will be a deluge of complaints by claimants who allege their data protection rights have been infringed, and consequent litigation.

It has already been reported that there has been a significant number of data-breach notifications and complaints to the Data Protection Commission in Ireland since 25 May. While highly unlikely to be as ubiquitous as personal injuries litigation, practitioners will see activity in data protection litigation increasing significantly.

Potential civil claims are not

confined to classic data infringement disputes, but will also crop up as an additional heads of claim in all kinds of civil disputes, including employment disputes, contractual disputes, personal injuries, financial services claims, and breach of confidence actions.

AT A GLANCE

- There has been a significant number of notifications to the Data Protection Commission in Ireland since 25 May 2018
- Practitioners will see activity in data protection litigation increasing significantly
- Data subjects can authorise a not-for-profit organisation to lodge DP complaints on their behalf and to act on their behalf in breaches of DP laws
- Collective action mechanisms will assist data subjects to instigate litigation and to access legal assistance and knowledge in a novel way in Ireland

Claimants in the Irish courts?

Under the GDPR and the *Data Protection Acts 1988-2018* (DPA), for individual data subjects, the people identified or identifiable from the data that is processed (data subjects) are empowered to seek compensation if a breach of the GDPR has affected them (articles 79 and 82 GDPR).

With regard to collective actions, article 80 GDPR and section 117 DPA introduce different types of collective actions for data privacy breaches. Data subjects can authorise a not-for-profit organisation to lodge data protection complaints on their behalf, to act on their behalf in a



Lore and behold – Data protection

PICSHUTTERSTOCK

breach of data protection laws action, and to receive compensation on their behalf.

These collective action mechanisms will assist data subjects to instigate litigation and to access legal assistance and knowledge in a novel way in Ireland. The collective action mechanisms are likely to be used in large-scale data breaches, of which there have been plenty of examples,

nationally and globally, in recent years. However, there is no European collective action legal framework, so these actions will emerge on a state-by-state basis.

The Austrian registered not-for-profit organisation NOYB (an acronym for 'None of Your Business') was established by serial data protection litigant Max Schrems to facilitate funding and

identifying collective actions. NOYB filed complaints in Austria, Germany, Belgium and France against some global tech companies within hours of the GDPR coming into force. Complaints were also launched by French digital rights group La Quadrature du Net, also known as 'La Quad'. Expect Irish activity in this area before long.



THE COLLECTIVE ACTION MECHANISMS ARE LIKELY TO BE USED IN LARGE-SCALE DATA BREACHES, OF WHICH THERE HAVE BEEN PLENTY OF EXAMPLES, NATIONALLY AND GLOBALLY, IN RECENT YEARS



Q FOCAL POINT

WHAT'S THE DAMAGE?

The question of what 'damage' means in a data protection context has been hotly debated for many years. Ruling on pre-GDPR law in the case of *Collins v FBD Insurance plc*, the High Court decided that the plaintiff alleging loss arising from a data protection infringement must establish there had been a breach, that they had suffered damage, and that the breach had caused the damage. In other words, a plaintiff could only secure an award of compensation for breach of data protection law on proof of actual loss or actual damage caused by the breach. Non-material loss was not recoverable.

This differed from subsequent British jurisprudence on the issue of damages for breach of data protection rights (see *Google Inc v Vidal-Hall*).

The GDPR and DPA, from an Irish

perspective, expand the concept of damage in the context of breach of data protection rights. Damage is now clearly defined as including physical damage (recital 75 GDPR, among others) and 'material and non-material damage' (article 82 GDPR and section 128 DPA). Material damage involves actual damage that is quantifiable, and non-material damage covers any non-financial damage, such as pain and suffering. It remains to be seen how the Irish courts will approach compensating a person for non-material damage, including in terms of defining the concept and in assessing the quantum of damages to be awarded. We may have to wait for a 'classic' data protection action before the courts' approach to compensation is fully understood in Ireland.

Article 82 of the GDPR also provides that 'any person' who has suffered material or non-material damage as a result of an infringement of the GDPR has a right to compensation. This will clearly cover data subjects, but may extend to others (for example, family members) affected by an infringement. This aspect of the GDPR is not fully dealt with in the DPA, so how this article will be dealt with by the Irish courts remains to be seen.

Who will be the defendants?

Actions for compensation and damage may be taken against controllers and processors. This is a significant shift from a position where, principally, controllers had

liability – now any organisation processing personal data has significant liability risks. The GDPR (article 82) provides that if more than one entity is involved in the same processing activity, and each is liable for infringement, then they are each responsible for the entire damage caused. If one entity pays out for the entirety of the damage, it can recover against the other party or parties. As a result, data subjects may choose the best 'mark' for litigation as the defendant, and it will need to tackle this joint liability provision by claiming from the other processors/controllers involved. This position will inevitably see secondary litigation between multiple actors involved in processing,

in terms of allocating fault and liability as a fall-out of the primary action for infringement.

What claims can a claimant make?

The DPA introduces a tort called a 'data protection action', which will be the most common type of claim made.

Article 77 GDPR grants data subjects the right to lodge complaints with a supervisory authority, alleging that the processing of their personal data infringes the GDPR. If the supervisory authority fails to handle any such complaints appropriately, article 78 GDPR also gives data subjects the right to an effective judicial remedy against a supervisory authority.

Ingredients of an action

Under section 117 of the DPA, a data subject must claim that his or her data protection right has been infringed and that the infringement is as a result of the processing of his or her personal data in a manner that is noncompliant with data protection laws.

The DPA (section 117) provides that data protection actions, including for compensation, may be taken by the not-for-profit bodies acting for claimants in collective actions (discussed above).

But what's the harm?

As a law that is focused on the protection of ordinary citizens, the GDPR itself states that breach of data protection rights may cause harm. Recital 85 (GDPR) lists a menu of harms that a GDPR infringement may cause, including "physical, material or non-material damage to natural persons, such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality



IRISH DATA PROTECTION ACTIONS CAN NOW INCLUDE CLAIMS FOR COMPENSATION FOR STRESS AND EMOTIONAL SUFFERING, WHEREAS PRIOR TO THE GDPR, ONLY COMPENSATION FOR FINANCIAL AND OTHER MATERIAL LOSS COULD BE RECOVERED IN IRELAND



THE GDPR AND DPA, FROM AN IRISH PERSPECTIVE EXPAND THE CONCEPT OF DAMAGE IN THE CONTEXT OF BREACH OF DATA PROTECTION RIGHTS. DAMAGE IS NOW CLEARLY DEFINED AS INCLUDING PHYSICAL DAMAGE AND ‘MATERIAL AND NON-MATERIAL DAMAGE’

of personal data protection by professional secrecy, or any other significant economic or social disadvantage to the natural person concerned”.

With the right set of facts, a claimant, such as an aggrieved employee, consumer, social media account holder, or contractor could allege to have suffered many of the harms in this non-exhaustive list.

Irish data protection actions can now include claims for compensation for stress and emotional suffering, whereas prior to the GDPR, only compensation for financial and other material loss could be recovered in Ireland.

The burden of proof

Where the GDPR has been infringed, there is liability unless a controller or processor can prove it is not the source of noncompliance (article 82 GDPR). Significantly, a litigant does not have to prove fault or negligence to initiate proceedings.

It is likely that data rights requests to controllers and complaints to supervisory authorities will be made to help ground and support any data protection actions taken. Expect to see complaints to supervisory authorities arise in parallel with legal actions.

Forum shopping

Proceedings against a controller or processor may be brought in the courts of the member state where the controller or processor has an establishment, or the courts of the member state where the data subject habitually resides (article 79 GDPR; section 117 DPA). This choice of forum provision means that claimants may tend to select member states based on differences in national laws (such as cost of litigation, and ease and speed of access to the courts)



Live long and litigate


that could have an impact on the number of cases appearing before the Irish courts. There is a *lis pendens* system requiring the courts to suspend proceedings if identical proceedings are before another court (article 81 GDPR).

In Ireland, the Circuit Court and High Court – but not the District Court – have jurisdiction to hear a data protection action and have the power to grant relief by way of injunction, declaration, or compensation for damage suffered by the data subject as a result of the infringement.

Where do we go from here?

The level of actions for breach of an individual’s data protection rights, seeking compensation, remains to be seen. It is equally unknown how the Irish courts will tackle the concept of awarding compensation for breach of data protection laws, especially for non-material damage. Certainly, the self-reporting of personal data breaches to data subjects (required when a personal data breach is likely to result in a ‘high risk’ of adverse effects to an individual’s rights and freedoms) is likely to increase visibility and awareness of data protection issues, and to increase complaints and claims.

Of course, the safest course of action

for controllers and processors is to ensure that appropriate procedures to achieve compliance with the GDPR and the DPA are in place. Compliance is the best defence, and efforts made to achieve compliance, even if these actually fail, are likely to influence the Irish courts when considering the topic of compensation. Compensation may, after all, not be the end goal in many data protection actions; often the data subjects simply want their rights to be honoured and for organisations to rectify behaviour. 

LOOK IT UP

CASES:

- *Collins v FBD Insurance plc* [2013] IEHC 137
- *Google Inc v Judith Vidal-Hall, Robert Hann, Marc Bradshaw v The Information Commissioner* [2015] EWCA Civ 311
- *NT1, NT2 v Google LLC v The Information Commissioner* [2018] EWHC 799

LEGISLATION:

- *Data Protection Act 2018*
- *General Data Protection Regulation*

LITERATURE:

- Elaine Edwards, *The Irish Times*, ‘DPC receives over 1,100 reports of data breaches since start of GDPR rules’ (30 July 2018)
- Pádraig Hoare, *Irish Examiner*, ‘Data watchdog deals with 1,300 GDPR queries’ (6 June 2018)
- *Privacy Laws & Business*, ‘First UK collective action cases in the pipeline’ (20 August 2018)