The GDPR and Employment Litigation

Declan Harmon BL

Barrister-at-Law at The Bar of Ireland

The GDPR: Five years a-growing

1. The General Data Protection Regulation ("**GDPR**") is now a little over five years in force, having commenced in May 2018. At that time, there was much uncertainty regarding how actions brought before the courts in Ireland arising out of alleged infringements of the GDPR and / or the Data Protection Act 2018 ("**the 2018 Act**") would be determined. As two learned authors noted at the time:

> *As there have [been] no published decisions in this jurisdiction on the subject, nor even any news reports of Circuit Court awards, it is unclear as to what level of damages might be awarded to a claimant for a breach of their data protection rights. Anecdotally, data protection law practitioners are aware that cases are either not yet ready for hearing, or have settled prior to hearing. The absence of guidance from the Courts makes settlement more difficult. It is likely that when decisions start to issue, regard will be given to factors such as whether the breach was deliberate, the sensitivity of the data involved, the degree of distress caused, and any previous breach or administrative fine previously imposed on the data processor or controller.*[1]

2. Whether or not one is filled with joy in celebration of the fifth birthday of the GDPR, it is timely to reflect on the developments in GDPR and data protection related litigation, particularly since some (but by no means all) of the issues arising in such cases have been clarified by recent decisions of both the Court of Justice of the European Union ("**CJEU**") and domestic courts.

Why does this matter to employment practitioners?

3. Readers may be wondering "*Why should I care?*". Put simply, the scope and scale of data that may be collected and processed within the context of the employment relationship is

[1] Hogan and O'Doherty, *Data Protection Claims: Law and Practice*, paper delivered to the Employment Bar Association Annual Conference, November 2020, at paragraph 82.

such that an employer may hold more personal data on an employee than any other data controller. In addition, that data will often be sensitive in nature.

4. If one considers that an employer may frequently:

    - hold an employee's CV or educational records,
    - keep their banking information for payroll purposes,
    - receive health data for occupational health reasons, and
    - create daily records through the use of CCTV cameras in the workplace,

    then it is easy to see the many touchpoints in the employment relationship where an employer is acting as a data controller in respect of the employee's personal data.

5. Employment practitioners and clients should also care about this area because it has created additional ways within which contentious issues in the workplace can be litigated and expands the venues within which that litigation takes place.

6. Issues which would not have given rise to a justiciable claim pre-GDPR may now do so and this is something which employees, employee representatives, employers and practitioners need to contend with.[2] On a practical note, the costs of defending such claims can frequently exceed the damages being claimed, giving rise to difficult cost / benefit decisions for defendants. Anecdotally, it is understood that many employers are not insured for such claims under their traditional liability policies, or have such a high excess on their policy that they effectively end up self-insuring.

A refresher on the law

7. The statutory provisions introduced in the GDPR and the 2018 Act will likely be well known to practitioners at this stage and so it is not intended to do any more than summarise and recap on them here.

8. Article 79 of the GDPR provides, *inter alia*:

[2] This paper will confine itself to the civil litigation provisions arising from the GDPR and the 2018 Act. Of course, there is a parallel regulatory and supervisory function (including the imposition of fines) performed by the Data Protection Commission to which aggrieved data subjects may also have recourse but which is beyond the scope of this paper.

Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority[3] …, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation.

9. Article 82 of the GDPR provides, *inter alia*:

Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.

10. While the GDPR is directly effective and, therefore, does not require transposing legislation, the 2018 Act contains provisions for the practicalities of how what are termed "data protection actions" are to be conducted.

11. Most particularly, section 117 of the 2018 Act provides, *inter alia*, that:

- A data subject may bring a data protection action without prejudice to any other remedy available to her (including her right to lodge a complaint with the Data Protection Commission),
- A data protection action shall be deemed to be an action founded on tort,
- The Circuit Court has concurrent jurisdiction with the High Court to hear data protection actions,
- The court hearing a data protection action shall have the power to grant to a plaintiff one or more than one of the following reliefs:
  (a) relief by way of injunction or declaration, or
  (b) compensation for damage suffered by the plaintiff as a result of the infringement of a relevant enactment, and
- "Damage" includes material and non-material damage.

[3] In Ireland, this is the Data Protection Commission.

12. The provisions of the relevant articles of the GDPR and of section 117 of the 2018 Act merit some comment.

13. First, it is clear that a data subject does not have to make a binary choice between bringing a data protection action or making a complaint to the Data Protection Commission (or, indeed, taking any other action).

14. Secondly, the fact that "damage" includes both material and non-material damage is very significant in the Irish context because it altered the position from that which was understood to exist under the previous legislation, as interpreted most particularly by the High Court in *Collins v. FBD Insurance*[4], whereby a claimant was required to show material damage in order to recover.

15. Thirdly, damages are not the only remedy available and an "effective judicial remedy" may also take the form of declaratory relief or an injunction (whether interlocutory or permanent).

16. Fourthly, the Circuit Court is the lowest court imbued with jurisdiction to deal with data protection actions. This has given rise to significant concern on the part of defendants to such actions since even relatively minor claims where damages could be expected to be within the District Court jurisdiction had to be issued in the Circuit Court, with the attendant additional costs. This situation has been altered by section 77 of the Courts and Civil Law (Miscellaneous Provisions) Act 2023, which amends the 2018 Act to give the District Court jurisdiction in such actions. This provision has not been commenced at the time of writing of this paper (October 2023) and it is understood that the necessary amendments to the District Court Rules are awaited before commencement.

17. However, even when the District Court does attain jurisdiction, it is by no means certain that this will result in plaintiffs opting to issue their cases in that Court given that the injunctive and, in particular, declaratory reliefs provided for in section 117 of the 2018 Act are routinely pleaded, which the District Court would not have the equitable jurisdiction to grant.

The interpretation of the GDPR across Europe – a journey to Luxembourg

[4] [2013] IEHC 137.

18. So far, so (relatively) simple. However, the job faced by courts around Europe in interpreting Articles 79 and 82 of the GDPR has been anything but simple. This is, perhaps, unsurprising given the unprecedented scope of the GDPR and the right that it gives to directly initiate proceedings for an infringement of its provisions.

19. It is also unsurprising that some of the most fraught questions have been those touching on the issues of how to interpret "non-material damage" and the conditions upon which liability will be imposed on a data controller such that damages might be awarded. At the beginning of 2023, at least six preliminary references on questions related to those issues were before the CJEU from courts across the EU.

20. Very significant guidance in this area has now been provided by the CJEU in its judgment in the case of *UI v. Österreichische Post AG*[5] ("***Österreichische Post***"). In this case, UI sought compensation for the non-material damage he claimed to have suffered as a result of the processing by the defendant postal company of data relating to the political affinities of persons resident in Austria, in particular UI himself, even though he had not consented to such processing.

21. In the request for a preliminary ruling, the CJEU had been asked three questions by the Austrian Oberster Gerichtshof (Supreme Court):

    - Does the award of compensation under Article 82 of the GDPR also require, in addition to infringement of provisions of the GDPR, that an applicant must have suffered harm, or is the infringement of provisions of the GDPR in itself sufficient for the award of compensation?
    - Does the assessment of the compensation depend on further EU law requirements in addition to the principles of effectiveness and equivalence?
    - Is it compatible with EU law to take the view that the award of compensation for non-material damage presupposes the existence of a consequence or effect of the infringement of at least some weight that goes beyond the upset caused by that infringement?

22. While the questions may have been clunky, the answers given by the CJEU were clear:

[5] Case C-300/21, judgment of the Court (Third Chamber), 4th May 2023.

- Article 82 of the GDPR must be interpreted as meaning that the mere infringement of the provisions of that regulation is not sufficient to confer a right to compensation.
- Article 82 must be interpreted as precluding a national rule or practice which makes compensation for non-material damage, within the meaning of that provision, subject to the condition that the damage suffered by the data subject has reached a certain degree of seriousness.
- Article 82 must be interpreted as meaning that for the purposes of determining the amount of damages payable under the right to compensation enshrined in that article, national courts must apply the domestic rules of each Member State relating to the extent of financial compensation, provided that the principles of equivalence and effectiveness of EU law are complied with.

23. In analysing *Österreichische Post,* it can be said that it provided something for plaintiffs, something for defendants and something for another day.

24. Plaintiffs will take comfort from the fact that the idea of being required to exceed a threshold level of seriousness before being able to recover non-material damages has been rejected by the CJEU. This was a departure by the Court from the opinion of the Advocate General in the case, who had suggested that "mere upset" would not attract an award of damages[6].

25. Defendants will take comfort from the fact that the CJEU has rejected the proposition that the infringement of a provision of the GDPR alone is not enough to attract damages. A plaintiff must prove that damage has been suffered by them as a result of the infringement, even if that might simply be done by the evidence of the plaintiff asserting that they had suffered upset or distress as a result of the infringement.

26. Those who had been hoping for clearer guidance from the CJEU on how damages, particularly for non-material damage, are to be assessed were left disappointed. The Court has left it up to national courts to apply their domestic rules relating to the extent of financial compensation. This is subject to the conditions that those rules are not, in situations

[6] Case C-300/21, Opinion of Advocate General Campos Sánchez-Bordona, 6th October 2022.

covered by EU law, less favourable than those governing similar domestic situations (principle of equivalence) and that they do not make it excessively difficult or impossible in practice to exercise the rights conferred by EU law (principle of effectiveness).

27. In addition, it is easy to see how questions of equivalence and effectiveness of EU law will return again to the CJEU for consideration. It is unlikely that this is the last time the CJEU will be asked to provide guidance on this matter.

28. Another interesting area where the CJEU will soon be giving guidance relates to the question of a data controller's liability for a data hacking attack. This will be of interest to employers given the number of high profile hacking attacks on payroll and other systems in recent times.[7]

29. In *VB v. Natsionalna agentsia za prihodite*[8] ("***VB***"), the Varhoven administrativen sad (Supreme Administrative Court of Bulgaria) asked the CJEU questions relating to the criteria for attributing responsibility to a data controller for a hacking attack carried out by a nefarious third party. The background to the case is that, in 2019, a hacker gained unauthorised access to the information system of the National Revenue Agency of Bulgaria and various tax and social security information of millions of persons, both Bulgarian nationals and foreign nationals, had been published on the internet.

30. The National Revenue Agency had pleaded that it had fulfilled its GDPR obligations by implementing the appropriate technical and organisational measures to ensure the security of personal data it held. In addition, a lower court had found that the plaintiff had the burden of proving that the data controller had failed to implement appropriate measures.

31. In his opinion[9], Advocate General Pitruzzella stated the mere existence of a personal data breach is not in itself sufficient to conclude that the technical and organisational measures implemented by the data controller were not appropriate to ensure the protection of the personal data concerned.

[7] See for instance: https://www.irishtimes.com/transport/2023/06/06/aer-lingus-among-victims-of-global-cyberattack-that-has-compromised-employee-data/.
[8] Case C-340/21
[9] Case C-340/21, Opinion of Advocate General Pitruzzella, 27th April 2023.

32. However, he also stated that when verifying whether the technical and organisational measures implemented by the controller of personal data are appropriate, the court hearing the action must carry out a review which extends to a specific analysis of both the content of those measures and the manner in which they were applied, as well as their practical effects. Importantly, the Advocate General's opinion was that the burden of proof was on the data controller to demonstrate that the measures it had implemented were appropriate.

33. Also of significance was the Advocate General's opinion that the fact that the infringement of the GDPR was committed by a third party does not in itself constitute a ground for exempting the controller from liability and "the controller must demonstrate that it is not in any way responsible for the infringement".[10]

34. The Advocate General also had some interesting comments on the issue of damages. His opinion was that detriment consisting of the fear of a potential misuse of a data subject's personal data in the future, the existence of which the data subject has demonstrated, may constitute non-material damage giving rise to a right to compensation, provided that the data subject demonstrates that she has individually suffered actual and certain emotional damage.

35. Of course, the Advocate General's opinion is not binding and we await the judgment of the Court. It is worth bearing in mind that the Court did not follow the Advocate General's opinion in *Österreichische Post*. However, if the Court does follow the Advocate General in *VB* it will be very significant, I would suggest, for the following reasons:

    - It establishes that the mere existence of a personal data breach is not in itself sufficient to establish that a data controller is liable for a data breach.
    - However, the burden of proof in establishing that appropriate technical and organisational measures were followed will lie with the data controller.
    - If the threshold is for the data controller to prove that "it is not in any way responsible for the infringement", that will be a heavy burden for a defendant to discharge. It will likely involve expert technical evidence, which will drive up costs that may be unlikely to ever be recovered, even in a claim that is successfully defended. This is particularly relevant in claims where any damages recovered are

[10] Paragraph 84 of the Opinion, emphasis added.

likely to be small and may encourage defendants to settle on an economic basis even where they may have a good defence.

Developments in the Irish courts

36. Given the uncertainties in how to interpret relevant provisions of the GDPR while the guidance of the CJEU is awaited in the several preliminary references before it, the Circuit Court in the case of *Cunniam v. Parcel Connect Limited t/a Fastway Couriers*[11] imposed a stay on the proceedings pending the determination of relevant preliminary references. This author appeared in the case and so I will not comment further on it. However, it is understood that the decision in that case has led to applications for stays going uncontested in many other proceedings in Circuit Courts across the country.

37. That has not meant that litigation in this area has been completely frozen. In the first written decision of any court in Ireland on the issue, useful guidance on how damages for non-material damage will be assessed was given by the Circuit Court (His Honour Judge John O'Connor) in *Kaminski v. Ballymaguire Foods Limited*[12] ("*Kaminski*"). This case should certainly be of interest to employment practitioners.

38. In *Kaminski*, the Defendant employer showed CCTV footage to some of its employees as part of a meeting between several managers and supervisors. Several clips involving poor food quality and safety practices were shown to the managers and supervisors present at the meeting and the Plaintiff employee appeared in one of the clips of CCTV footage which was shown.

39. The Plaintiff was not present at the meeting in question but he was informed of the CCTV clip subsequently by other employees. The Plaintiff was subjected to some "slagging" by colleagues regarding how he had appeared in the CCTV clip. It is important to note that there was no suggestion of misconduct or bad behaviour on the Plaintiff's part. The Plaintiff was upset and embarrassed by the attention he received and suffered sleep loss.

40. The Court accepted that the Defendant's CCTV policy was not sufficiently transparent and clear that CCTV would be used for training purposes. Accordingly, the Court held that the

[11] [2023] IECC 1.
[12] [2023] IECC 5.

processing of the Plaintiff's personal data in the form of him featuring on CCTV being used for training purposes was unlawful and an infringement of his rights under the GDPR. The Court also accepted that, in the circumstances, the Plaintiff had suffered non-material damage as a result and proceeded to assess the quantum of damages to be awarded.

41. In setting out the factors pertinent in assessing damages for non-material damage, the Court said it was doing so with some caution in the absence of clarification from the Oireachtas, the Superior Courts or the CJEU. However, the Court proffered the following list of factors (which I outline below *verbatim* for clarity):

- *A "mere breach" or a mere violation of the GDPR is not sufficient to warrant an award of compensation.*
- *There is not a minimum threshold of seriousness required for a claim for nonmaterial damage to exist. However, compensation for non-material damage does not cover "mere upset".*
- *There must be a link between the data infringement and the damages claimed.*
- *If the damage is non-material, it must be genuine, and not speculative.*
- *Damages must be proved. Supporting evidence is strongly desirable. Therefore, for example in a claim for damages for distress and anxiety, independent evidence is desirable such as for example a psychologist report or medical evidence.*
- *Data policies should be clear and transparent and accessible by all parties affected.*
- *Employers should ensure their employee privacy notices and CCTV policies are clear to employees.*
- *Where a data breach occurs, it may be necessary to ascertain what steps were taken by the relevant parties to minimise the risk of harm from the data breach.*
- *An apology where appropriate may be considered in mitigation of damages. For example, it may reassure the affected individual that their employment is safe and not at risk.*
- *Delay in dealing with a data breach by either party is a relevant factor in assessing damages.*
- *A claim for legal costs may be affected by these factors.*

- *Even where non-material damage can be proved and is also not trivial, damages in many cases will probably be modest. In the absence of other guidelines, from the Oireachtas or the Superior Courts and / or the Judicial Council, the Court has taken cognisance of the factors as outlined in the Judicial Council Personal Injuries Guidelines 2021 in respect of the category of minor psychiatric damages as instructive guidance, though noting in some cases non-material damage could be valued below €500.*[13]

42. Applying the factors to the circumstances of the case, the Court awarded Mr. Kaminski €2,000 and his Circuit Court costs. While the learned judge was right, in my respectful view, to be cautious given the lack of legislative guidance or binding precedent, it is hard to quibble with the broad thrust of the factors the Court outlined. Anecdotally, it is understood that those factors are being applied or commented favourably upon by Circuit Courts around the country and they have certainly been a factor in settlement negotiations I have experience of since the judgment was handed down.

43. I would suggest that some points are particularly worth highlighting, especially in cases with an employment element:

- The Court placed a high value on the transparency and clarity of workplace policies (e.g. CCTV policies) and it was of significance to the Court in *Kaminski* that the Plaintiff's first language was not English but that he had been provided with policies in English only.
- The Court's quite reasonable desire for supporting evidence of non-material damage is likely to result in medical evidence being proffered in appropriate cases. Defendants may be concerned about their ability to test such evidence in the absence of expert evidence of their own and may, therefore, seek to have plaintiffs medically examined.
- The Court has given a strong indication that it would value an early apology being made in appropriate cases and that such an apology may mitigate the quantum of damages to be awarded. This may require defendants and their advisors to take a

[13] [2023] IECA 5, at paragraph 11.6.

view early on in any litigation or threatened litigation to concede the fact that an infringement has occurred.

- The Court has also strongly indicated that it will take the manner in which the parties have dealt with the infringement into account in any application for costs.

Points to note for the future

44. Five years on from its commencement, GDPR related litigation is firmly established in Ireland. However, the uncertainties of an entirely new sphere of litigation continue to trouble practitioners. The fog is slowly starting to lift in that regard thanks to guidance provided by the CJEU and domestic courts, and this will continue in the year to come.

45. The broad message from the CJEU is that it takes the protection of data subject rights seriously, given that the protection of personal data has the status of a fundamental right. This was clearly seen when the Advocate General's opinion in *Österreichische Post*, which was generally regarded as being favourable to data controllers defending litigation, was not followed by the Court in its ultimate judgment.

46. Employers will continue to be required to ensure strong compliance with the GDPR and the 2018 Act. Those that fail to do so run the risk of facing litigation where the legal costs of defending the claim may be significant, even if any award of damages is modest. *Kaminski* is a good example of a claim in an employment context that would not have been justiciable pre-GDPR now being not just statable but successful.

47. The risks for employers in this field are particularly acute when one considers issues such as hacking incidents where the numbers of employees affected could run into the hundreds or even thousands. If the Advocate General's opinion in *VB* is followed by the Court, then a data controller that is the subject of a hacking attack may face a high bar in disclaiming liability for such an incident.

48. In short, the GDPR is here to stay and, while many may feel that the compliance costs are high, the costs and risks of non-compliance are even higher.

Declan Harmon BL

November 2023