DATA MATTERS: DATA PROTECTION ISSUES

*Authors: Judge Marie Quirke, judge of the District Court.**

Abstract: This article explores the range of issues judges may find themselves dealing with following the enactment of the Data Protection Act 2018 (itself implementing Regulation (EU) 2016/679 – The General Data Protection Regulation). These issues include a new cause of civil action, changes to civil procedure, the role the Circuit Court plays in hearing appeals of decisions of the Data Protection Commission and the role that the Circuit Court plays in sanctioning administrative measures taken by the Data Protection Commission.

Introduction

The legal landscape as it relates to Data Protection Law has changed drastically since the enactment of Regulation (EU) 2016/679 ('the GDPR') and the corresponding domestic legislation, the Data Protection Act 2018 ('the 2018 Act'), which gives effect to the GDPR. This landscape is not dissimilar to the hills of Donegal in that there are many and several manifestations. If viewed together, the hills and aspects of Data Protection law may blend together seamlessly, but each hill will possess its own twists, turns and challenges.

The GDPR became law by way of direct effect on 25 May 2018 and, in tandem with this, the 2018 Act was enacted on 24 May 2018 with most provisions being commenced on 25 May 2018 via the Data Protection Act 2018 (Commencement) Order 2018 (S.I. No. 174 of 2018). Parts 5 and 6 of the 2018 Act also incorporate Directive (EU) 2016/680 ('the Law Enforcement Directive') which sets out how data is to be processed by authorities/data controllers who are competent for the prevention, investigation, detection or prosecution of criminal activities or execution of criminal penalties, where personal data is being processed for these purposes. The application of the Law Enforcement Directive is outside the scope of this paper.

Personal Data – A Primer

In order to fully consider the impact of the 2018 Act and the GDPR on the business of the Circuit Court, it is worth exploring the concept of personal data. In 2006, British mathematician and architect of the Tesco Clubcard, Clive Humby pronounced that 'data is the new oil'. While this particular analogy may have some attraction when considering the monetisation of personal information by commercial entities, it is somewhat of a flawed analogy. Sholtz notes that the analogy fails to properly encompass the moral, legal and personal aspects of personal data.[1] It is submitted that a more useful analogy is to compare the large-scale storage and use of personal data to that of the nuclear industry in that if poorly handled, the resultant leaks and externalised costs can be catastrophic.[2]

The GDPR provides a very broad definition of 'personal data' in Article 4(1): 'Any information relating to an identified or identifiable natural person'

* With thanks to Robert Brophy BL of the Research Support Office of the Courts Service

[1] Lauren Scholz, 'Big Data is Not Big Oil: The Role of Analogy in the Law of New Technologies' (2020) 85 Tennessee Law Review.

[2] Cory Doctorow, 'Personal data is as hot as nuclear waste' (The Guardian 15 January 2008).

Further to this broad definition, the CJEU has adopted an expansive approach to the concept finding that, for example, IP addresses and answers given as part of a professional examination constituted personal data.[3] Further examples are found in the recitals to the GDPR and include genetic material and online identifiers such as cookies.[4]

Data may also become personal data where, when combined with another piece of information, it can be used to identify a natural person.[5] An example of this would be a company which places a tracking device in its fleet of vehicles. The tracking data, in and of itself, is not personal data, but by virtue of the fact that the company's employees are driving the vehicles, the tracking data becomes personal data pertaining to the company's employees.

Personal data may not be processed unless it is done so under one of six possible legal bases detailed at Article 6 GDPR:

1. Consent;
2. Contractual necessity;
3. Compliance with a legal obligation to which the controller is subject to;
4. Vital interests of a natural person;
5. Necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; or
6. Necessary for pursuance of the legitimate interests of the controller except where such interests are overridden by the rights of the data subject.

It is a common misconception that consent is the only basis for processing personal data. In actuality, consent as a basis presents issues to a data controller in that consent can be withdrawn unilaterally by the data subject, and therefore it may, in many cases, be the least preferable basis.[6] For consent to be validly given, it must be freely given, and the data subject must be informed of the nature of the processing 'in plain language'.[7] Further to this, the concept of 'special category data' is detailed in Article 9 GDPR. This is data which:

1. Reveals racial or ethnic origin;
2. Reveals political opinions;
3. Reveals religious or political beliefs;
4. Reveals trade union membership;
5. Constitutes genetic data or biometric data for the purposes of uniquely identifying a natural person i.e. facial images or finger prints; or
6. Concerns a persons health or sexual orientation.

The processing of special category data is explicitly forbidden unless one (or more) of ten exceptions detailed in Article 9(2) GDPR are satisfied:

1. Explicit consent;
2. Necessary for employment, social security, social protection law or for a collective agreement with necessary safeguards;

[3] Case C-582/14 *Breyer v. Bundesrepublik Deutschland* and Case C-434/16 *Nowak*.
[4] Recital 34 GDPR and Recital 30 GDPR respectively.
[5] Article 9(1) GDPR.
[6] Article 7(3) GDPR.
[7] Recital 42 GDPR.

3. Necessary to protect the vital interest of the data subject, where the data subject is incapable of providing consent;
4. Forms part of legitimate activities of a non-profit body with a political, philosophical, religious or trade union aim;
5. The data was already made 'manifestly' public by the data subject;
6. For legal proceedings and the administration of justice;
7. For public interest;
8. For medical reasons;
9. For public interest in the area of public health; or
10. For archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

The Importance of Data Protection Rights

The importance of data protection rights has been recognised in recent years by a series of legislative measures. Article 16 of the Treaty on the Functioning of the European Union gave the European Union a mandate to legislate for data protection rights at treaty level. Further to this, Article 8 of the Charter of Fundamental Rights of the European Union establishes this as a fundamental right which shall be controlled by an independent authority:

1) Everyone has the right to the protection of personal data concerning him or her.
2) Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3) Compliance with these rules shall be subject to control by an independent authority.

By establishing the right to data protection as a standalone right, the EU went further than the European Court of Human Rights who have recognised the right only as an adjunct to the right to privacy.

While Article of the Charter defined the right to data protection, the GDPR put flesh on the bones of this right and enumerated these rights as follows:

1. The right of access.[8]
2. The right to be informed.[9]
3. The right of rectification.[10]
4. The right of Erasure / Right to be forgotten.[11]
5. The right of data portability.[12]
6. The right not to be subjected to a decision based solely on automated processing.[13]

[8] Article 15 GDPR.
[9] Articles 13 & 14 GDPR.
[10] Articles 16 & 19 GDPR.
[11] Article 17 & 19 GDPR.
[12] Article 20 GDPR.
[13] Article 22 GDPR.

7. The right to object to processing.[14]
8. The right to restriction of processing.[15]

Further to this, the GDPR introduced a number of principles for the lawful processing of data.

1. Lawfulness, fairness and transparency;
2. Purpose limitation;
3. Data minimisation;
4. Accuracy;
5. Storage limitation;
6. Integrity and confidentiality; and
7. Accountability.

Civil Issues - Data Protection Actions

The first time the Irish Superior Courts had to consider damages flowing from a violation of a data subject's rights was in *Collins v. FBD Insurance plc*.[16] This case was decided under the Data Protection Directive (Directive 95/46/EC), the Data Protection Act 1988 and the Data Protection (Amendment) Act 2003.

To briefly summarise the facts, Mr. Collins held a motor insurance policy through FBD. Mr. Collins' van was stolen and FBD sought to repudiate the policy due to non-disclosure of a material fact. FBD had engaged a private investigator to examine the claim and the investigator had discovered that Mr. Collins had a criminal conviction for a theft offence. It later transpired that the information gleaned about this criminal conviction was inaccurate and had been obtained other than in a manner prescribed by the District Court rules.

Following two complaints to the Data Protection Commission, the Commissioner found that FBD had breached Mr. Collins' data protection rights in four ways:

1. Failing to comply with an access request within the statutory 40-day time period;
2. Failing to disclose that information in its possession about Mr Collins had been released to a third party (a private investigator);
3. Failing to have a contract in place with the private investigator, a statutory requirement to ensure the data subjects rights are protected; and
4. Failing to obtain the information relating to Mr Collins' criminal conviction in a proper manner.

Following the Commissioner's decision, the plaintiff took a Circuit Court action against the defendant insurance company seeking relief inter alia under s.7 of the Data Protection Act 1988 and 2003. This provision imposes a duty of care upon data controllers and processors towards data subjects 'for the purposes of the law of torts and to the extent that that law does not so provide'. The Circuit Court awarded Mr. Collins €15,000. The order of the Circuit Court did not identify the claim(s) in respect of which the damages were awarded.

[14] Article 21 GDPR.
[15] Article 18 GDPR.
[16] [2013] IEHC 137.

This is of particular importance as other reliefs were pleaded including damages for breach of contract and discrimination under the Equal Status Acts 2000 and 2008. There is no report of this judgment available. On appeal, the High Court found that s.7 of the Data Protection Act 1988 and 2003 did not allow for recovery of damages without proof of actual loss or damage. Further to this, it was found that 'the statute does not provide for strict liability and for me to interpret s.7 of the Data Protection Acts as enabling a claimant to benefit from an award of damages for non-pecuniary loss, would be for me to expand the scope of s.7 beyond that provided for in the Act or required by the Directive'[17].

The principle from *Collins* that non-pecuniary loss was not recoverable under s.7 was upheld by the Supreme Court in *Murphy v. Callinan*, with Baker J noting:

> The Data Protection Act 2018 implementing GDPR permits an individual to seek compensation from the court for breaches of data subject rights even in the absence of any material damage or financial loss. But s. 7 of the 1988 Act, on which the plaintiff relies, whilst it did expressly create a duty of care on a data controller in regard to personal data, did not make the breach of data subject rights actionable without proof of negligence or a causative connection to an alleged material damage or other loss.[18]

The GDPR has brought significant developments in how a plaintiff may recover damages. Up until this point, there were no reported Irish judgments where the plaintiff succeeded in obtaining damages. Article 82(1) of the GDPR states: '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.' S.117 of the 2018 Act transposes this provision into Irish law and allows for the recovery of damages, declaratory relief and injunctive relief for breaches of data subject rights. This provision was considered by the Court of Appeal in the in the case of *Shawl Property Investments Ltd v A. & B.*, where Whelan J noted that 'it is necessary to have regard to the principle of proportionality in evaluating claims for breaches of [the GDPR].'[19] It was further noted that 'nothing stated in s.117 or indeed the Act itself suggests that a data protection action is a tort of strict liability.'[20] This case concerned the dismissal of the second defendant/appellant's counterclaim in the High Court which pleaded, *inter alia*, reliefs under the s.117 of the Data Protection Act 2018. The Court of Appeal found that this particular element of the counterclaim could proceed, so while the comments of Whelan J are of some guidance, they are strictly *obiter* and do not alter the previous position in relation to damages for breaches of data protection rights in Ireland. The case has been remitted to the High Court for determination, but has not, at the time of writing, been listed for hearing.

Clarity as to the scope of loss which may be recovered in a data protection action may come from an Austrian case which was referred to the CJEU on 12 May 2021 and has yet to be determined. In *UI v. Osterreichische Post AG*, a reference to the CJEU was made, requesting clarification on three issues:

1. Does the award of compensation under Article 82 GDPR also require, in addition to infringement of provisions of GDPR, that an applicant

[17] *Collins v. FBD Insurance plc* [2013] IEHC 137 [4.4].
[18] *Murphy v. Callinan* [2018] IESC 59 [42].
[19] *Shawl Property Investments Ltd v A. & B.*[2021] IECA 53 [133].
[20] ibid [114].

must have suffered harm, or is the infringement of provisions of GDPR in itself sufficient for the award of compensation?

2. Does the assessment of the compensation depend on further EU Law requirements in addition to the principles of effectiveness and equivalence?
3. 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 of the infringement of at least some weight that goes beyond the upset caused by that infringement?[21]

It is anticipated that this case will be determined during 2022. When the courts are called upon to assess data protection actions, they may arise in proceedings where other reliefs are pleaded. For example, in *Collins*, other reliefs were pleaded including damages for breach of contract and discrimination under the Equal Status Acts 2000 and 2008. It is not unreasonable that a data protection action could also feature claims for breach of contract, breach of privacy, breach of a duty of care and breach of confidence.

A further development in civil litigation that has been brought about by the GDPR is the concept of a class action under Article 80. This provision (implemented by s.117(7) of the 2018 Act) allows for a data protection action to be brought on behalf of a data subject by a non-profit body. In relation to the recent Facebook data breach, Digital Rights Ireland CLG has indicated that it will pursue a class action under Article 80 GDPR and is seeking concerned parties to join the action.[22] The CJEU has since held that consumer protection associations may bring representative actions in relation to infringements of personal data protection.[23] Further to his, Article 80(2) GDPR must be interpreted as not precluding national legislation which allows a consumer protection association to take such an action where the association may lack a mandate conferred upon it for that particular purpose.[24]

Civil Issues - Quantum

Under s.117 of the 2018 Act, jurisdiction for data protection actions is held by the Circuit Court concurrently with the High Court. S. 117(5) limits the amount recoverable in the Circuit Court to the current monetary jurisdiction in tort as prescribed by law, which currently stands at €75,000. The only reported Irish judgment which concerns quantum in a data protection action is *Collins* where a sum of €15,000 was awarded. However, this decision is of limited assistance as (a) the award was overturned by the High Court and (b) the order of the Circuit Court did not particularise this sum in circumstances where reliefs were also sought under the Equal Status Acts.

Comparators from other jurisdictions may give some guidance as to the appropriate level of damages to be awarded. In the *Austrian Post* case, which has been referred to the CJEU, a data subject (privacy lawyer Dr. Christian Wirthensohn) made a subject access request to the

[21] Case C-300/21: Request for a preliminary ruling from the Oberster Gerichtshof (Austria) lodged on 12 May 2021—*UI v Österreichische Post AG*. OJ C320, pp 25–26.
[22] Digital Rights Ireland, 'We're Suing Facebook. Join Us' <https://www.digitalrights.ie/facebook/> Accessed 1 June 2022.
[23] *Meta Platforms Ireland Ltd v. Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V.* (Case C-319/20).
[24] ibid [84].

Austrian Post Office in relation to this data. He found that they had estimated his likely political affiliation.[25] He was particularly aggrieved as the political affiliation ascribed to him was for a party known for extreme views. He then took a civil data protection action under Article 82 of the GDPR on the basis that his political beliefs are 'special category data' under Article 9 of the GDPR. The Austrian court of first instance found in his favour and awarded damages of €500 (a sum of €2,500 plus costs had been sought). This decision was overturned on appeal on the basis that the plaintiff had failed to sufficiently prove that he had suffered non-material damage. A further appeal in this case led to the above reference being made to the CJEU which has yet to be determined.

The German courts have shown a particular reluctance to order compensation under Article 82 without strong evidence of loss. The Local Court of Diez found on 7 November 2018 that damages were not justified in cases where the plaintiff had received spam email, in breach of his data subject rights.[26] In this case, the plaintiff had sought damages of €500. In the Netherlands, the Administrative District Court of Overijssel awarded damages of €500 where a data subjects Freedom of Information request was shared amongst government authorities in unredacted format. On appeal the Dutch Council of State overturned this decision.[27] Cases from the UK may provide more useful guidance as to the appropriate level of damages to be awarded for breach of data subject rights on account of the similarities between the Irish and UK legal systems. In *Halliday v. Creation Consumer Finance Ltd*, the defendant finance company's reporting of the debt due to the relevant UK credit rating agency was technically incorrect.[28] The plaintiff claimed that this misreporting constituted a breach of the finance company's data protection obligations. The lower courts dismissed the claim but it was appealed. The Court of Appeal stated that the breach was a 'limited', 'mechanical', 'single episode case', and there was no damage to Mr. Halliday's reputation nor evidence of any malice attributable to the defendant. In terms of quantum, the court concluded that the plaintiff had suffered nominal pecuniary damage (£1) and awarded a 'modest' award of compensation of £750 for the 'distress' caused to the plaintiff. The court commented: 'It is not the intention of the legislation to produce some kind of substantial award. It is intended to be compensation [for loss suffered].'[29] While *Halliday* dealt with minor breaches of a data subject's rights, the UK Supreme Court in Lloyd v. Google LLC considered the issue of non-material damage.[30] The case was brought as a representative action by a consumer rights advocate and the sum of £750 per member of the representative class was suggested as the appropriate level of quantum, per *Halliday*. However, the UK Supreme Court rejected the claim as it was held that s.13 of the Data Protection Act 1998 required proof of actual damage for the claimant to succeed.

Costs implications may arise where a data protection action is heard in the Circuit Court but damages are awarded on a scale which would ordinarily place the action within the monetary jurisdiction of the District Court, which is currently a maximum of €15,000. It has been suggested that if damages were to be awarded on a District Court scale but costs incurred on a Circuit Court basis –

[25] Case C-300/21 *UI v. Osterreichische Post AG*.
[26] GDPR Hub, 'AG Diez 8 C 130/18 7.11.2018' (22 March 2022) <https://gdprhub.eu/index.php?title=AG_Diez_8_C_130/18_7.11.2018> Accessed 1 June 2022.
[27] GDPR Hub, 'RvS - 201905087/1/A2' (15 September 2020) <https://gdprhub.eu/index.php?title=RvS_-_201905087/1/A2> Accessed 1 June 2022.
[28] [2013] EWCA Civ 333.
[29] ibid [36].
[30] [2021] UKSC 50.

> 'a situation arises whereby any modest damages award is only a small fraction of the parties' legal costs, this would raise a wider concern as to whether litigation is the most cost-effective way of resolving these disputes, and indeed this may call into question the appropriateness of the litigation process as an "effective" judicial process envisaged by the European legislators.'.[31]

Orders 60 of the Circuit Court Rules sets out the procedures applicable to data protection action.

Civil Issues – Discovery and Data Protection Rights

Outside of data protection actions, the data protection rights of a natural person may be engaged in civil litigation, in particular when issues of discovery arise in an action. The right of access to personal data is enshrined in both Article 15 of the GDPR and s.91 of the 2018 Act. The right of access is central to the rights of a data subject in that many other rights ostensibly flow from the premise that the subject is entitled to access their personal data. For example, a subject may not be able to effectively vindicate their rights to rectification or erasure if they are denied access to the very data that they wish to rectify or erase. The CJEU in Opinion 1/15 emphasised the importance of the right of access in this regard:

> Furthermore, as regards Article 7 of the Charter, the Court has held that the fundamental right to respect for private life, enshrined in that article, means that the person concerned may be certain that his personal data are processed in a correct and lawful manner. In order to carry out the necessary checks, that person must have a right of access to the data relating to him which is being processed.[32]

Further to providing copies of a subjects personal data, the following information must be provided pursuant to Article 15(1) of the GDPR as part of a Data Subject Access Request ('DSAR'):

a) the purposes of the processing;
b) the categories of personal data concerned;
c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
f) the right to lodge a complaint with a supervisory authority;
g) where the personal data are not collected from the data subject, any available information as to their source;

[31] Trevor Murphy, 'The Justiciability of Data Protection Laws in Ireland: a New Dawn of Civil Litigation?' Commercial Law Practitioner 2020, 27(11), 238-256, 253.
[32] Opinion 1/15 of the Court (Grand Chamber) 26 July 2017 ECLI 592 para 219.

h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

There are only three grounds on which a data controller may refuse or curtail a DSAR:

1. Where disclosing the data would 'adversely affect the rights and freedoms of others'.[33] Keogh notes that an example of this would be:

   'where data concerning a person other than the data subject is included within the information, to the extent that it would adversely affect the rights of that other person, it is permissible for that information to be redacted i.e. giving the specific name each employee that may have access to the data'.[34]

2. Where the controller has already complied with a DSAR and an identical request is made, unless a reasonable period has elapsed.[35]
3. Where the personal data relates to an expression of opinion about the data subject by another person given in confidence, or on the understanding it would be treated as confidential. This principle is illustrated in *Nowak v. Data Protection Commissioner*, where the High Court held that the Mr. Nowak did not have a right of access to information sent as part of a complaint made to the Chartered Accountant's Regulatory Board in relation to audits that he had carried out whilst employed by an accountancy firm.[36] It was held that this did not constitute personal data and was therefore not subject to the right of access.[37]

Access and Litigation Privilege

Where civil proceedings are instigated and a party seeks documentation to advance or defend a claim, the interplay between an individual's data protection rights and the discovery process may become an issue. This tension is illustrated in the case of *Bus Átha Cliath v. Data Protection Commissioner*, where the plaintiff in a personal injuries action sought CCTV footage under a DSAR.[38] Bus Átha Cliath / Dublin Bus refused on the basis that as litigation had commenced, the CCTV footage was subject to litigation privilege and therefore discovery was the proper means to obtain the CCTV footage. The Data Protection Commissioner issued an enforcement notice, ordering Dublin Bus to comply with the Subject Access Request and this was appealed to the Circuit Court which found in favour of the DPC. Bus Átha Cliath / Dublin Bus brought a further appeal to the High Court. Here, Hedigan J held that the right of access was a fundamental and distinct right, which exists separately from discovery. It was held there was no exemption to data protection law where litigation was ongoing and the decision of the DPC was upheld. It should be noted that this case was decided under the Data Protection Directive but the right of access was not changed in any material way with the advent of the GDPR.

[33] Article 15(4) GDPR.
[34] Laura L Keogh, *Data Protection Compliance* (Clarus Press 2019) 91.
[35] Recital 63 GDPR.
[36] [2018] IEHC 117.
[37] ibid [24].
[38] [2012] IEHC 339.

In *Dudgeon v. Supermacs Ireland Ltd* , an appeal was brought against a Circuit Court order denying the plaintiff discovery of the CCTV footage of an accident on the defendant's premises.[39] Ultimately, Barr J found that discovery of the CCTV footage was unnecessary on the facts of the case as the CCTV footage would only be used to ascertain the credibility of the plaintiff as a witness. No mention was made in the judgment of the plaintiff's right to obtain the CCTV under a DSAR.

Discovery - Possession, power or procurement

The courts have begun to consider how, in making an order for discovery, certain information may be in the 'possession, power or procurement' of an individual by way of their right of access.[40] In *Susquehanna International Group Ltd v. Needham* , the plaintiff sought an order for discovery of certain categories of documents against the defendant.[41] The plaintiff contended that those documents were necessary in support of the plaintiff's claim for breach of contract. The defendant contended that the documents asked to be disclosed were wide ranging. The primary issue between the parties was that the plaintiff wanted the disclosure of the documents that could have been available to the defendant pursuant to a data subject access request.

Baker J granted an order for the discovery of the documents sought by the plaintiff. The court, however, modified the said request in relation to certain categories. The Court held that it could order the discovery of documents, which was the matter of data subject access request, if the person concerned had the legal entitlement to procure or obtain those documents. The court found that in the present case, the defendant had a legal enforceable right that he could exercise to obtain the relevant documents from the head office of his company. This case pre-dates the introduction of the GDPR, with the data protection rights of the defendant being considered under the provisions of Directive 95/46/EC and the Data Protection Acts 1988-2003.

The relationship between a subject access request and discovery was again considered in *Avoncore Ltd and Canmont Ltd t/a Douglas Shopping Centre v. Lesson Motors Ltd, Adam Opel GmbH, Opel Automobile GmbH and Vauxhall Motors Ltd*[42] In a discovery application, a previous order for discovery was amended to clarify that 'the discovery includes documents which the Driver is in a position to obtain by right from [their insurer], including, but not limited to, by way of a data subject access request under the Data Protection Acts.'[43]

Enforcement of a DSAR and Discovery Order

In contrasting the right of access to the discovery process, *Kelleher* notes that:

> Access to a subject's personal data is one of their fundamental rights, whilst orders for discovery are an interlocutory stage in the court process but in practice controllers tend to treat access requests quite differently to orders for discovery, probably because a discovery order is directly supervised by a judge by whom immediate remedies may be imposed. A litigant unhappy with

[39] [2020] IEHC 600.
[40] O.31, r.12 of the Rules of the Superior Courts.
[41] [2017] IEHC 706.
[42] [2022] IEHC 34.
[43] ibid [333].

> the response given to such an order can easily apply to court;[44] in contrast a subject who is unhappy with the response to their access request must first complain to the DPC, who must seek to resolve the complaint amicably, before making a decision which may then be appealed to the Circuit Court.[45]

It should be noted that the above quote deals with the regime under the Data Protection Directive and now s.117 of the 2018 Act allows a subject to proceed directly to litigation, without having to have recourse to a complaint, where their right of access has been infringed upon. The point, however, remains that the enforcement of a discovery order may prove easier as there will already be proceedings in being and the matter can be heard as an interlocutory application.

Judicial Issues – Administrative Decisions of the Data Protection Commission

Article 58(4) GDPR provides that:

> The exercise of the powers conferred on the supervisory authority pursuant to this Article shall be subject to appropriate safeguards, including effective judicial remedy and due process, set out in Union and Member State law in accordance with the Charter.

S.155 of the 2018 Act grants the Circuit Court jurisdiction to hear a number of applications in relation to administrative decisions of the Data Protection Commission ('the DPC'):

1. An appeal against an administrative fine imposed by the DPC;[46]
2. An application by the DPC to confirm an administrative fine;[47]
3. An application brought by an authorised officer of the DPC to compel a person to comply with a DPC investigation;[48]
4. An application brought by an authorised officer of the DPC to compel a person to comply with an oral hearing conducted by the DPC.[49]

The above applications shall be made to a judge of that Court for the circuit in which the person to whom the application relates ordinarily resides or, if a controller or processor, has an establishment or, at the option of the person, by a judge of the Circuit Court for the time being assigned to the Dublin circuit.

An appeal against an administrative fine imposed by the DPC must be brought within 28 days of the notification of the decision to impose the fine. The Circuit Court is allowed to consider any evidence adduced even if this evidence was not originally presented to the DPC. On appeal, the Circuit Court may confirm, annul or replace the decision with such other decision as the court considers just and appropriate, including a decision to impose a

[44] O.31, r.21 Rules of the Superior Courts.
[45] Denis Kelleher, *Privacy and Data Protection Law in Ireland* (2nd edn, Bloomsbury Professional 2015) para 13.30.
[46] S. 142 Data Protection Act 2018.
[47] S. 143 Data Protection Act 2018.
[48] S. 138 Data Protection Act 2018.
[49] Paragraph 5 of Schedule 3 to the Data Protection Act 2018.

different fine or no fine at all. It should be noted that if an appeal is brought in the Circuit Court against an administrative fine which is within the ordinary monetary jurisdiction of the court (€75,000), it appears that the court may vary this fine up to €1 million.[50]

In considering any appeal, the court is mandated to act in accordance with Article 83 GDPR. This obliges the court to consider, *inter alia*:

1. The nature, gravity and duration of the infringement;
2. The intentional or negligent character of the infringement;
3. Any actions taken by the controller in mitigation;
4. Any previous infringements on the part of the controller;
5. The degree of responsibility of the controller for the infringement;
6. The degree of co-operation by the controller;
7. The categories of personal data involved in the infringement;
8. The manner in which the infringement came to the attention of the supervisory body;
9. Any previous measures imposed on the controller;
10. Any codes of conduct relevant to the controller;
11. Any other relevant aggravating or mitigating factor such as financial gains or losses.

No appeal brought under s.142 of the 2018 Act has been fully determined at the time of writing. An appeal brought by the Department of Social Protection due to be heard in December 2021 was settled before the scheduled hearing date.[51] Further to this, whilst WhatsApp Ireland Ltd indicated a desire to appeal an administrative fine of €225 million, the statutory appeal has been adjourned generally pending the determination of separate judicial review proceedings.[52]

S. 143 of the 2018 Act imposes obligation on supervisory authority to bring an action to the Circuit Court to confirm an administrative fine. The first instance of this procedure being used was when the Circuit Court confirmed a fine of €75,000 issued against Tusla.[53] The Circuit Court, in October 2021, confirmed a fine of €450,000 on Twitter International Company.[54] No appeals have been brought against these decisions. It should be noted that the fine in this case far exceeds the ordinary monetary jurisdiction of the Circuit Court.

Judicial Issues – Appeals of Substantive Decisions of the Data Protection Commission

[50] S. 142(5) Data Protection Act 2018.
[51] Department of Social Protection, 'Agreement between the Department of Social Protection and the Data Protection Commission' (Gov.ie, 10 December 2021) <https://www.gov.ie/en/publication/5088f-psc/> Accessed 1 June 2022.
[52]Courts Service Online, 'Whatsapp Ireland Ltd -v- Data Protection Commission & Ors 2021/816 Jr' <https://www.csol.ie/ccms/web/high-court-search/case-details/2021/816/JR> Accessed 1 June 2022.
[53]Data Protection Commission, 'Data Protection Commission Fine on Tusla Child and Family Agency Confirmed in Court' (4 November 2020) <https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-fine-tusla-child-and-family-agency-confirmed-court> Accessed 1 June 2022.
[54] Data Protection Commission, 'Confirmation of Fine – Twitter International Company' (18 Octobe 2021) <https://dataprotection.ie/en/news-media/press-releases/confirmation-fine-twitter-international-company> Accessed 1 June 2022.

Article 78(1) GDPR states that: 'Without prejudice to any other administrative or non-judicial remedy, each natural or legal person shall have the right to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them.' S. 150 of the 2018 Act transposes Article 58 GDPR and grants the Circuit Court concurrent jurisdiction with the High Court to determine appeals of substantive decisions of the Data Protection Commission. This provision is silent as to when the Circuit Court is the appropriate jurisdiction for an appeal of a substantive decision. This may be contrasted to s.117 of the 2018 Act, which in granting concurrent jurisdiction to the Circuit and High Courts in relation to data protection actions, aligns the amount recoverable in the Circuit Court with that court's ordinary monetary jurisdiction. Previously, appeals against a substantive decision could only be brought in the Circuit Court.[55] Appeals taken under s.150 may be appealed to the High Court (in the case of an appeal brought first to the Circuit Court) and the Court of Appeal (in the case of an appeal brought first to the High Court) only on a point of law.[56] From a procedural perspective, Orders 60 and 64B of the Circuit Court Rules outline the procedural aspects of an appeal against a substantive decision of the Data Protection Commission. All appeals must be brought within 28 days of service of the decision of the Data Protection Commission.[57] In considering an appeal, the Circuit Court may annul the decision of the Data Protection Commission, substitute its own decision or dismiss the appeal.[58]

The Circuit Court must consider, in hearing an appeal against a substantive decision of the Data Protection Commission, the appropriate level of curial deference that must be shown towards the Commission as an expert body. To this end, the decision in *Nowak v. Data Protection Commissioner* is instructive.[59] In *Nowak*, O'Donnell J (as he then was) considered the appropriate test to apply when considering an appeal brought under s.26 of the Data Protection Act 1988:

> It can be said that if an error is sufficiently clear and serious to be detectable by a non-expert court after scrutiny, then that is justification for overturning the decision, even though the court may lack more specific expertise. In my view, the Orange standard is the appropriate standard to apply.[60]

The test in *Orange* was first outlined by Keane CJ in *Orange Communications Ltd v. The Director of Telecommunications Regulation and anor (No. 2)* and states:

> [A]n applicant will succeed in having the decision appealed from set aside where it establishes that, taking the adjudicative process as a whole, the decision reached was vitiated by a serious and significant error or a series of such errors. In arriving at a conclusion on that issue, the High Court will necessarily have regard to the degree of expertise and specialised knowledge available to the first defendant.[61]

[55] S. 26 Data Protection Act 1988.
[56] S. 150(11) Data Protection Act 2018.
[57] S. 150(1) Data Protection Act 2018, s.150(5) Data Protection Act 2018.
[58] S. 150(2) Data Protection Act 2018, s.150(6) Data Protection Act 2018.
[59] [2016] IESC 18.
[60] ibid [30].
[61] [2000] 4 IR 159 184-185.

This test was subsequently approved by Finnegan P in *Ulster Bank Investment Funds Ltd v. Financial Services Ombudsman*.[62] There is nothing in the 2018 Act to suggest that the test in *Orange* is to be displaced or modified when appeals are brought against substantive decisions of the DPC. Therefore, the Circuit Court must exhibit curial deference towards the technical expertise of the DPC in deciding an appeal and only seek to annul, modify or substitute a decision where it is clear that a serious error of law or fact was made by the DPC.

Finally, the court has a general discretion to hear an appeal otherwise than in public,[63] and where issues of privilege arise.[64]

Conclusion

Under the 2018 Act, the Circuit Court has been vested with significant responsibilities regarding the enforcement of key aspects of the GDPR. With these responsibilities, a number of issues arise in relation to the jurisdiction of the Circuit Court to hear matters. As the *de facto* court of first instance for the private enforcement of data protection rights, through data protection actions, the Circuit Court must deal with a 'new' type of claim where the issue of quantum remains very much in question. In the absence of a judgment of the Superior Courts, it may well be for the Circuit Court to lay down a marker in relation to the size of an award of damages arising out of a breach of a person's data protection rights. This then presents a further issue in relation to the costs of an action that may well be within the ordinary monetary jurisdiction of the District Court.

A further development of the jurisdiction of the Circuit Court may be found in the expanded jurisdiction that the court has in relation to administrative fines. The ability of the Circuit Court to vary an administrative fine which begins within its current monetary jurisdiction (€75,000) up to €1 million is a novel departure which ostensibly expands the jurisdiction of the court beyond its ordinary monetary jurisdiction. By way of comparison, where the Central Bank issues an administrative fine pursuant to the Central Bank Act 1942 (as amended), the High Court enjoys exclusive jurisdiction to affirm the fine.

In relation to appeals of substantive decisions of the DPC, the Circuit Court, by virtue of the authorities of *Orange* and *Nowak* is bound by a test which belongs more to the sphere of judicial review than that of an ordinary civil appeal. While this is not a unique feature to appeals taken under the 2018 Act,[65] it places considerations of administrative law which were traditionally within the sole jurisdiction of the High Court into the sphere of the Circuit Court. Having considered all of the foregoing, the Circuit Court may have become the epicentre of data matters. Only time will tell.

[62] [2006] IEHC 323.
[63] S. 156 Data Protection Act 2018.
[64] S. 151(5) Data Protection Act 2018.
[65] For example, appeals of decisions of the Workplace Relations Commission may be brought to the Circuit Court.