DATA PROTECTION AND THE EXERCISE OF THE JUDICIAL FUNCTION IN IRELAND

Abstract: This paper aims to clarify the applicable data protection law when courts are acting in their judicial capacity. The provisions of the General Data Protection Regulation and of the Law Enforcement Data Protection Directive apply to courts with some considerable exceptions to the rights of data subjects. This does not exempt courts from fulfilling their obligations as data controllers, and the importance this might have for their practice and procedures merits a thorough examination this paper hopes to be the basis for.

*Author: Giacomo Bonetto, LLM (UCD), is a stagiaire in the cabinet of Advocate General Hogan at the Court of Justice of the European Union and formerly a Judicial Assistant to the Hon Ms Justice Baker in the Supreme Court.**

Introduction

The courts established under the Constitution are obliged to exercise their constitutional function subject only to the law.[1] The right to data protection affects the courts as it does every other fundamental right in the sense that the courts themselves, as other branches of government, are obliged to respect it when fulfilling their function under the Constitution, although courts enjoy immunity from suit in respect of that exercise. This paper is concerned in particular with, and purports to outline in summary, the foundation of the obligations that the Data Protection Act 2018 (the Data Protection Act) has imposed upon the judiciary to ensure the data protection principles are guaranteed in the course of the administration of justice, whilst restricting the rights of data subjects in order to safeguard judicial independence and court proceedings.

The General Data Protection Regulation (the Regulation) finds its legal basis in article 16(2) of the Treaty on the Functioning of the European Union (TFEU),[2] and provides a uniform data protection regime for all EU Member States.[3] In Ireland, the aspects of the Regulation which require implementation have been dealt with by the enactment of the Data Protection Act.[4] Recital 20 of the Regulation explicitly states that its provisions apply to the 'activities of courts and other judicial authorities'. The Law Enforcement Data Protection Directive

* I want to express my profound gratitude for the helpful suggestions and advice of the Hon. Ms Justice Marie Baker. The views expressed are entirely and solely my own.

[1] Article 35 of the Constitution.

[2] 'The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data […] by the Member States when carrying out *activities which fall within the scope of Union law*, and the rules relating to the free movement of such data.' (Emphasis added).

[3] European Parliament and Council Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC OJ [2016] L 119/1.

[4] For example, the age of consent to the processing of personal data was left to be decided to each Member State (see s 29 of the Data Protection Act).

(the Directive),[5] as transposed by national law,[6] outlines the data protection regime applicable when personal data is processed for the specific purpose of the prevention, investigation etc. of criminal offences, by specific controllers, ie the 'competent authorities'. Courts qualify as competent authorities for the purposes of the Directive when they process personal data relating to criminal offences for criminal justice purposes.[7]

The scope of the Regulation and of the Directive does not include the processing of personal data when the processing activity falls outside the competence of EU law.[8] It would seem therefore that, *prima facie*, the performance of the judicial function by the courts insofar as it constitutes processing of personal data would be excluded from the scope of the Regulation when national courts do not apply EU law.[9] However, the scope of the exceptions to the data protection rights provided for by the Regulation itself, as implemented by the Data Protection Act, has implicitly extended the applicability of the rest of the data protection regime to the exercise of the judicial function in general, even when Courts do not apply EU law. It might constitute a disproportionate restriction of the right to data protection if the judiciary were exempted *tout court* from the data protection principles as well as from the data protection rights when processing personal data in matters which do not require the application of EU law.

The applicable principles and data subject rights related to the processing of personal data governed by the Directive are similar to those outlined by the Regulation, as are the restrictions to the data protection rights established by the Data Protection Act in respect of both types of processing activities (those governed by the Regulation and those governed by the Directive). This article will focus on the regime laid down by the Regulation and how it affects courts acting in their judicial capacity, but it must be borne in mind that a detailed analysis is also warranted as to when courts can be qualified as 'competent authorities' under the Directive, which may raise specific and different issues from those discussed in general herein.[10]

Therefore, one must ask the usual questions: what is the personal data processed? Who is the controller? Are there any processors? What are the statutory obligations they must each fulfil? What are the rights of a data subject? What are the remedies available to a data subject? In other words, what are the data protection obligations of the courts in the course of, and in connection with, court proceedings? A brief answer to each of these questions will outline the data protection regime in the courts. It must be stressed at the outset that the Data Protection Act refers to 'courts' and does not consider the individual judicial office holder. It may be of interest in the future to conduct a thorough analysis on the implications stemming from that. First, however, we must examine the intricate interaction between the

[5] European Parliament and Council Directive (EU) 2016/680 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA O.J. L/119, 4.5.2016.

[6] For Ireland, see Part 5 of the Data Protection Act.

[7] Recital 20 of the Directive.

[8] See Article 2(2)(a) of the Regulation and Article 2(3)(a) of the Directive.

[9] This differentiation is necessary because the principle of effectiveness of EU law mandates that there must exist a sufficient remedy to guarantee rights under EU law.

[10] According to its Recital 80, the Directive 'applies also to the activities of national courts and other judicial authorities'.

right to data protection as laid down in the Charter of the Fundamental Rights of the EU (the Charter) and the exercise of the judicial function.[11]

The fundamental right to data protection

The enshrinement of the right to data protection in article 8 of the Charter, immediately after the right to privacy in article 7, can be clearly seen as an elevation of the right to data protection to the status of a fundamental right of itself,[12] although the right to data protection was born ancillary to other fundamental rights, in particular to the right to privacy.[13] The Lisbon Treaty established that the Charter has the same legal value as the Treaties of the European Union. In Ireland, while a general right to privacy has long since been recognised as having constitutional status, albeit as an unenumerated constitutional right,[14] the recognition of a standalone fundamental right to data protection seems to derive solely from the Charter.

After having provided for a general recognition of the right to data protection of natural persons in its first paragraph, article 8 of the Charter goes on in its second paragraph to outline the content of the right, which includes rights vested in the data subjects (the right of access and rectification in particular) and statutory duties of controllers (that processing must be lawful, fair and for specified purposes).[15] The content of the right to data protection is further developed by EU law, mostly by the Regulation and the Directive, as further implemented in national legislation. The rights vested in the data subjects and the principles of data protection which impose statutory obligations upon data controllers and processors can exist separately from each other. It is essential to understand why this is possible, as we shall presently see that in the context of the performance of the judicial function, whilst the right to access, to erasure, etc., are restricted for the purposes of safeguarding the independence of the judiciary and court proceedings, courts must nonetheless abide to the implementation of the data protection principles.

The right to the protection of personal data of natural persons in the Charter gives rise to an immediate question: a right to protection against what? In a world where control and possession of information has become one of the greatest assets of private wealth and public power,[16] for example, in relation to national security, it seems that there might be a simple but very general answer to that question – protection against the possibility that the information be misused and against the diminution of the actual capacity of the person to whom such information relates to actually control it. This is independent from the actual

[11] Charter of Fundamental Rights of the European Union OJ 2012 C 326/02.
[12] Orla Lynskey, 'Deconstructing Data Protection: The "Added-Value" of a Right to Data Protection in the EU Legal Order' (2014) 63(3) *International and Comparative Law Quarterly* 569.
[13] Viktor Mayer-Schönberger, 'Generational Development of Data Protection in Europe' in Philip E. Agre and Marc Rotenberg (eds), *Technology and Privacy: The New Landscape* (Cambridge (MA), MIT Press 1997).
[14] In respect to, particularly the right to marital privacy since 1973 (see the judgment of the Supreme Court in *McGee v Attorney General* [1974] IR 284).
[15] 'Everyone has the right to the protection of personal data concerning him or her. 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.'
[16] See Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Profile Books 2019).

risks to the rights and freedoms of individuals posed by that misuse. Whilst this is just one of the various theories suggested as underpinning the identification of data protection as a fundamental right, it seems to be the most appealing one, although that is not always accepted in the academic world.[17]

Information is non-excludable, ie unsusceptible of appropriation, except by grant of exclusive right.[18] Rights in information are non-transferable, in the same way as an author has a copyright moral rights.[19] Data protection rights such as the right to access to personal data, to erasure and the right to be forgotten are indeed rights in information and could be argued to constitute a form of a grant of an exclusive right. However, the existence of such rights alone would not achieve the objective that the creation of the right to data protection is keen to ensure, namely the protection against risks posed to individuals by the misuse of their information. The real thrust of the data protection right rests in the statutory obligations imposed on data controllers. This conclusion is consistent with the judgment of the Court of Justice of the EU ("the Court of Justice") in *Digital Rights Ireland*,[20] in which the Court of Justice dealt with the essence of the right in order to exercise a balance with national security interests.

By way of example, the redaction of certain details from draft judgments is sought as a means to achieve a balance between the constitutionally protected principle that justice is to be administered in public[21] and other fundamental rights. Redaction is sometimes required by statute whereby redaction of the names of the parties is expressly mandated, such as in s 26 of the International Protection Act 2015 of asylum seekers, where the right to life or health would otherwise be exposed to risks, or in family law matters under s 40 of the Civil Liability and Courts Act 2004, for the purposes of guaranteeing *inter alia* the right to marital privacy and the best interests of minors. These provisions could be *also* said to constitute an implementation of the right to data protection which the State is obliged to vindicate by its obligations under EU law.

A redaction of judgments for the sole purpose of implementing the right to data protection is not, however, explicitly mandated by statute, and it is left to the discretion of the courts in accordance with the strict requirements established in *Gilchrist v Sunday Newspapers Ltd.*[22] In defamation cases, it can be seen why the balance favours the open justice principle. Whilst it seems *prima facie* paradoxical that judgments in defamation actions are published without redaction, there is no risk from the vindication of the reputation or the right to good name outlined in an unredacted judgment, because reputation and good name are intrinsically related to their public sphere. But how about litigation in relation to personal insolvency cases for instance? Can data protection as exception to the principle of open justice

[17] Maria Tzanou, *The Fundamental Right to Data Protection. Normative Value in the Context of Counter-Terrorism Surveillance* (Bloomsbury 2017) 41.
[18] Justine Pila and Paul Torremans, *European Intellectual Property Law* (OUP 2016).
[19] ibid.
[20] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resoruces and Others and Kärntner Landesregierung and Others* [2014] EU:C:2014:238, [40]. The Court of Justice was asked to rule on the validity of the Data Retention Directive. They held that the Data Retention Directive provided that certain principles of data protection and data security had to be respected by providers of publicly available electronic communications services or of public communications networks, and that it thus did not violate the essence of the right to data protection, although it declared the Data Retention Directive invalid on the grounds of proportionality.
[21] Article 34 of the Constitution.
[22] *Gilchrist v Sunday Newspapers Ltd* [2017] IESC 18, [2017] 2 IR 284.

established by law (eg under the principle of data minimisation) be of aid where privacy has failed?[23] Are there cases where judgments must be redacted under data protection law regardless of the actual risk posed to rights or freedoms of others, purely on the basis of the right to data protection? The answer to this question is more complex and requires an analysis of how data protection interacts with the exercise of the judicial function.

The exercise of the judicial function

As noted above, the scope of this paper is limited to the assessment of the obligations of the courts under the Data Protection Act when they act in a judicial capacity. It does not deal with the event that personal data are processed, eg in relation to activities of the Board of the Courts Service by its judicial members, or the activities of the recently established Judicial Council.[24] Although, the fact that such processing is not done by courts acting in a judicial capacity may not exclude *a priori* the applicability of the restriction to data subject rights for safeguarding the independence of the judiciary as s 158(3) of the Data Protection Act does not extend the restriction of data protection rights to the processing activities of 'courts acting in their judicial capacity', but to the extent to which it is proportionate to safeguard judicial independence and court proceedings, without any reference to the activity being performed in a judicial capacity,[25] or other restrictions to the rights of the data subjects.[26] There may still exist the need to safeguard judicial independence even when processing activities are not done by courts acting in their judicial capacity. Processing of personal data by members of the judiciary outside their judicial capacity, however, raises peculiar issues, particularly with respect to the lawfulness and scope of processing, which will be a matter within the remit of the Data Protection Commission, and warrants a detailed analysis outside the scope of this paper.

It is thus necessary to clarify when a court is acting in its judicial capacity for the purposes of the application of the Data Protection Act. The wording, as noted above, is adopted in s 157 for the purposes of identifying the jurisdiction of the *ad hoc* supervisory authority for data protection in the judiciary, the 'Assigned Judge', but the Data Protection Act omits to define 'courts acting in their judicial capacity'. Rule 3 of the Data Protection Act (S 158(3) Rules 2018 ("the Data Rights Rules")) implements the restriction to the rights of data subjects provided by s 158(1) of the Data Protection Act, which will be analysed below, also refers to the 'performance of a judicial function' when it broadly defines processing activities of courts when acting in a judicial capacity, but omits to define it. Rule 3 refers to data processing 'for the purposes of or in connection with proceedings, or the performance of a judicial function, or (as the case may be) the performance by a court officer in civil proceedings of limited functions of a judicial nature conferred on that officer by law'.

The first consideration must be that the establishment of the *ad hoc* data protection supervisory authority for the judiciary is mandated by article 55(3) of the Regulation, which provides that 'supervisory authorities shall not be competent to supervise *processing operations of courts acting in their judicial capacity'* (emphasis added), and therefore directly excludes, in

[23] The balance with the open justice principle has been quite clearly not in favour of privacy: see the *dicta* of Laffoy J in *Roe v The Blood Transfusion Service Board* [1996] 3 IR 67.
[24] Judicial Council Act 2019.
[25] However, the implementation of s 158(3) by the Rules considers the restriction of data subject rights only to the processing activities of courts when acting in their judicial capacity.
[26] Such as the exercise of a task otherwise imposed on a judge by law.

Ireland, the jurisdiction of the Data Protection Commission in relation to 'processing operations of the courts when acting in their judicial capacity'. The language of the Regulation has been transposed almost with no change by the Data Protection Act when it established the *ad hoc* supervisory authority for the judiciary: 'The judge ("assigned judge") for the time being assigned for that purpose by the Chief Justice shall be competent for supervision of data *processing operations of the courts when acting in their judicial capacity*' (emphasis added).[27] The rationale for the exclusion of the jurisdiction of national supervisory authorities from the processing of personal data by courts when acting in their judicial capacity was expanded upon in Recital 20 of the Regulation:

> The competence of the supervisory authorities should not cover the processing of personal data when courts are acting in their judicial capacity, in order to safeguard the independence of the judiciary in the performance of its judicial tasks, including decision-making. It should be possible to entrust supervision of such data processing operations to specific bodies within the judicial system of the Member State, which should, in particular ensure compliance with the rules of this Regulation, enhance awareness among members of the judiciary of their obligations under this Regulation and handle complaints in relation to such data processing operations.

It seems that the concepts of 'courts' and of 'acting in a judicial capacity' are *not* to be construed as autonomous concepts of EU law. The provisions of the Regulation where the concept is used (article 55, noted above, and also article 37(1)(a), which excludes the obligation of courts acting in their judicial capacity to designate a data protection officer), are concerned with balancing the right to data protection and the right of fair process, as guaranteed by judicial independence. Judicial independence is an established requirement under EU law as Member States must ensure that an effective remedy is available to vindicate rights under EU law, which would not be effective in the event that judicial independence is not guaranteed.[28]

Recently, in *Associação Sindical dos Juízes Portugueses,*[29] the Court of Justice considered the factors to be taken into account in assessing whether a body is a 'court' for the purposes of the application and effectiveness of EU law, and interestingly, it relied upon its judgment in *Margarit Panicello*,[30] which was concerned with the meaning of 'court or tribunal' for the purposes of the making of preliminary references under article 267 TFEU. The factors identified as indicative were, *inter alia*, whether the body in question is established by law, whether it is permanent, whether its jurisdiction is compulsory, whether its procedure is *inter partes*, whether it applies rules of law, and whether it is independent.[31] As far as the obligation to guarantee independence of courts or tribunals under EU law is concerned, the focus is on whether the body which is to be qualified as a 'court or tribunal' for the purposes of assessing the implementation of that obligation by a Member State is applying EU law when

[27] Section 157(1) of the Data Protection Act.

[28] Whether the Data Protection Act sufficiently implements that obligation is a discrete matter from the meaning of 'court' in article 55 of the Regulation and its Irish implementation.

[29] (Case C-64/16) *Associação Sindical dos Juízes Portugueses* EU:C:2018:117.

[30] (Case C-503/15) *Margarit Panicello* EU:C:2017:126, [27].

[31] The requirement of independence of a court when deciding a matter of EU law has been recently considered in (Joined Cases C-585/18, C-624/18 and C-625/18) *A.K. (Independence of the Disciplinary Chamber of the Supreme Court)* EU:C:2019:982, where the Court of Justice dealt with the interpretation of the Equality Framework Directive 2000, in relation to the lowering of the retirement age of judges of the Sąd Najwyższy, the Polish Supreme Court, and the early retirement of some of them due to the entry into force of new national legislation.

determining a dispute, and not necessarily 'exercising its judicial capacity'. That is a different and broader scope than the exercise of the judicial function which is an attribute of sovereignty and a function of government.[32] The Regulation, on the other hand, focusses on the exercise of the judicial function, which necessarily varies in Member States. This is arguably confirmed in recital 97 of the Regulation, which relates to the obligation to nominate a data protection officer, and reiterates that the exception is mandated for 'courts or independent judicial authorities *when acting in their judicial capacity'* (emphasis added).[33]

The word 'courts' in s 157 of the Data Protection Act refers only to the courts established under Article 34 of the Constitution to fulfil the judicial function by the Courts (Establishment and Constitution) Act 1961 and the Courts (Supplemental Provisions) Act 1961, to include the Circuit and District Court, but not quasi-judicial statutory bodies[34] such as the Labour Court,[35] established under the Industrial Relations Act 1946, or the Tax Appeals Commission, established under the Finance (Tax Appeals) Act 2015,[36] although they have been qualified as 'courts' for the purposes of article 267 TFEU.[37] This restrictive interpretation of the Data Protection Act has been adopted by the Labour Court and the Tax Appeal Commission, both of which have indicated the Data Protection Commission is the competent supervisory authority.[38] Considering that the jurisdiction of quasi-judicial statutory bodies is limited,[39] and that their decisions are subject to statutory appeals and/or judicial review,[40] the independence in the exercise of the judicial function guaranteed by excluding the jurisdiction of supervisory authorities only from the judicial review of, or statutory appeal against, those decisions before the courts may be argued to be a sufficient implementation of the Regulation. Furthermore, an extension of the literal meaning of the provisions to all quasi-judicial statutory bodies seems not warranted by the canons of statutory interpretation.[41]

---

[32] As stated by Kennedy C.J. in *Lynham v. Butler (No 2)* [1933] IR 74, [99].

[33] Judicial authorities other than courts could be the administrative tribunals established in civil-law Member States.

[34] The term is used to include a vast plethora of independent bodies which have been instituted from time to time under article 37 of the Constitution.

[35] In *Zalewski v Workplace Relations Commission* [2020] IEHC 178, [218], Simons J recently clarified the following regarding the Workplace Relations Act 2015: 'the decision-making under the WRA 2015 lacks one of the essential characteristics of the administration of justice, namely the ability of a decision-maker to enforce its decisions.'

[36] In *The State (Calcul International Ltd) v Appeal Commissioners* (Unreported, High Court, 18 December 1986), [19], Barron J held that the Commissioners were not exercising powers of a judicial nature because they had 'no power to enforce their decisions'. On 21 March 2016, the Tax Appeal Commission replaced the Office of the Appeal Commissioners. Appeals can no longer be reheard before a Circuit Court Judge but a statutory appeal can be brought to the High Court on a point of law only. Section 949AM of the Taxes Consolidations Act 1997, as inserted by the Finance (Tax Appeals) Act 2015, provides that the Revenue Commissioners shall give effect to any determination unless the determination has been appealed to the High Court and that the assessment or the amended assessment made in the determination shall be final and conclusive.

[37] Their capacity to make preliminary references under Article 267 TFEU has been confirmed by the Court of Justice in (Case C-191/03) *North Western Health Board v Margaret McKenna* EU:C:2005:513 and in (Case C-344/15) *National Roads Authority v Revenue Commissioners* EU:C:2017:28 respectively.

[38] Explicitly in 'Privacy Policy' (Labour Court, 9 November 2019) <www.labourcourt.ie/en/contact-us/data-protection/data-protection-privacy-policy-nov-2019.pdf>, and implicitly in 'Annual Report 2019' (Tax Appeals Commission), p 10 <www.taxappeals.ie/_fileupload/AnnualReports/Annual%20Report%202019%20-%20English.pdf> Accessed 15 October 2020.

[39] Article 37 of the Constitution.

[40] See *Kennedy v Hearne* [1988] IR 81.

[41] See the Interpretation Act 2005.

As regards the meaning of the phrase 'acting in their judicial capacity', Recital 20 of the Regulation suggests that it should not be limited to 'decision making' activities of courts, in other words, to the adjudication on the respective rights of the parties,[42] which is the essence of the judicial function,[43] but should also encompass all those 'judicial tasks' which may be ancillary to that. This wide interpretation is supported by the purpose of the provision, namely the protection of judicial independence. Whilst the principle that justice is to be administered in public does not encompass decisions made by judges in relation to eg the composition of the courts and the listing of a matter on the diary of the court, activities which do not amount to 'administration of justice' but simply to 'administrative procedures',[44] those activities nonetheless constitute judicial tasks ancillary to the exercise of the judicial function. The case law concerning the scope of judicial immunity from suit,[45] on contempt of court,[46] and on judicial privilege, which are strictly connected with the safeguarding of judicial independence, is more useful in this respect and tends to extend the respective principles to cover ancillary activities to the judicial function. A broad interpretation of the meaning of 'judicial capacity' to encompass ancillary matters to the exercise of the judicial function seems therefore to be warranted.

The Data Rights Rules seem to have adopted the view that data processing activities exercised on behalf of courts acting in their judicial capacity are to be considered within the meaning of 'courts acting in their judicial capacity' for the purposes of the Data Protection Act and that they are therefore outside the remit of the Data Protection Commission.[47] This approach seems to be well founded. Data processing activities of registrars and other court officers, such as listing a matter for hearing or keeping the files in the court records, whether made under the explicit direction of a judge or in the course of the usual business of a court, can be said to be delegated activities over which the judge maintains control, as statutorily specified by the Court Officers Act 1926,[48] and without which the exercise of the judicial function could be seriously impaired in practice. Moreover, these activities are subject to the same immunity, and are protected by the law on contempt of court and judicial privilege.[49] Section 7 of the Offences Against the State Act 1939 may also support a broad interpretation of 'courts' as including the court officers acting under the direction of the court.[50] It is unclear however whether certain court officers that perform activities which cannot readily

[42] *Walsh v Property Registration Authority* [2016] IECA 34, [23].
[43] In *McDonald v Bord na gCon* [1965] IR 217 the Supreme Court approved the five criteria that Kenny J. had outlined in the High Court for the identification of the judicial power.
[44] *Application of Singer* (1963) 97 ILTR 130.
[45] *Shell E & P Ireland Ltd. v McGrath* [2006] IEHC 108, [2007] 1 IR 671, at p. 688.
[46] *Skeffington v Rooney* [1997] 1 IR 22.
[47] See, for example, Rule 3 of the Data Protection Act (section 158(3)) Rules 2018 (S.I. No. 658/2018): 'Save as otherwise provided in these Rules, these Rules shall apply to the processing of personal data *by, for or on behalf of* a court when acting in a judicial capacity' (emphasis added).
[48] Section 65: '(1) Nothing in this Act shall prejudice or affect the control of any judge or justice over the conduct of the business of his court. (2) When an officer attached to any court is engaged on duties relating to business of that court which is for the time being required by law to be transacted by or before or under or pursuant to the order of a judge or judges of that court he shall observe and obey all directions given to him by such judge or judges. (3) All proofs and all other documents and papers lodged in or handed in to any court in relation to or in the course of the hearing of any suit or matter shall be held by or at the order and disposal of the judge or the senior of the judges by or before whom such suit or matter is heard.'
[49] See, for example, *Halsbury's Laws of England*, 'Contempt of Court' Volume 24 (2019) para 2(2) – 7. (note 2): 'an assault committed or threat made in the precincts of the court is a contempt in the face of the court where it is directed at *a person having a duty to discharge in the court*.' (emphasis added).
[50] Section 7 makes it an offence to prevent or obstruct 'the exercise or performance by any member of the legislature, the judiciary, or the executive or by any officer or employee (whether civil (including police) or military) of the State of any of his functions, powers, or duties'.

be said to support judicial activity such as the Office of Wards of Court, the Taxing Master, and the Master of the High Court are considered 'courts' for the purposes of the Data Protection Act.[51]

The safeguard of judicial independence and court proceedings

Due to the constitutional principle that justice is to be administered in public,[52] (which is part of the fundamental right to fair trial) one must, in principle, expect that privacy is not a starting point, as the law would not allow the redaction of the names of the parties, or the witnesses, or order that the matter be heard *in camera* to protect the right to privacy or to good name,[53] unless the exceptions to the constitutional principle that justice must be administered in public have been provided for by statute (eg Family Law Act 2004) or where courts exercise their common law power under the exceptional circumstances envisaged in *Gilchrist v Sunday Newspapers Ltd*.[54] However, as mentioned above, the right to data protection is an autonomous fundamental right and a separate balancing exercise must be carried out.[55] The balance with the right to fair trial is focussed in particular on the need to safeguard the independence of judges and the administration of justice more generally, which includes the principle that justice is to be administered in public.

The Regulation itself has operated a balancing exercise between the right to a fair trial and the right to data protection and has provided for two mandatory derogations from the data protection regime for the purpose of safeguarding judicial independence and court proceedings in relation to the data processing activity of courts when acting in their judicial capacity. The first derogation, considered above, is the exclusion from the jurisdiction of national supervisory and is directly mandated by article 55(3) of the Regulation. The rationale for the exclusion is arguably that the exercise of the judicial function could be undermined if the court were rendered accountable to national supervisory authorities, which are independent statutory bodies. The second derogation, which is provided for by article 37(1)(a) of the Regulation, is the exclusion of the courts when acting in their judicial capacity from the obligation to appoint a data protection officer, an independent figure as well, the requirement for which could also undermine the activities of courts exercising their judicial function, should they fear the intervention of the data protection officer in any aspect or their activities.

The exclusion of the obligation to avail of a data protection officer to safeguard judicial independence and court proceedings has been considered by article 23(1)(f) of the Regulation

[51] These issues deserve a thorough and comprehensive analysis which is beyond the limited scope of this article.
[52] Article 34 of the Constitution.
[53] In *Re Ansbacher (Cayman) Ltd* [2002] 2 IR 517, [529], McCracken J held that 'No case has been cited to me in which a right to good name or a right to privacy can justify anonymity in court proceedings. A request for such anonymity was expressly refused by Laffoy J. In Roe v The Blood Transfusion Service Board [1996] 3 I.R. 67, although that case was heard before Irish Times Ltd v Ireland [1998] 1 I.R. 359. However, the rationale for refusing anonymity as set out in that case seems to me to remain perfectly valid'.
[54] *Gilchrist v Sunday Newspapers Ltd* [2017] IESC 18, [2017] 2 IR 284. The court was concerned specifically with the granting of proceedings to be held *in camera* to protect the right to live of witnesses who were part of a protection scheme process but O'Donnell J formulated the principles in a quite general manner which seems to be applicable to the protection of other fundamental rights, including privacy and data protection.
[55] It could nonetheless be argued that when the outcome of the balance is in favour of the right to data protection, that may constitute a backdoor for the protection of the right to privacy in the context of the administration of justice.

as a basis of one of the restrictions to the right to data protection whose implementation is left, however, to the discretion of the Member States:

> Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society […].

What is meant by 'legislative measure' is expanded upon by recital 41 of the Regulation. It does not necessarily require a legislative act adopted by parliament.

Any restriction will have to comply with the provisions of article 23(2) of the Regulation that the restriction be necessary and proportionate.[56] The reason for the restriction, and how and when it may apply should be readily understood by the data subjects.[57] Article 52 of the Charter provides also that any restriction of the rights and freedoms provided for by the Charter must 'respect the essence of those rights and freedoms'. Thus, '[s]ubject to the principle of proportionality', the restrictions are to be made 'only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.'[58] In its judgment in *Digital Rights Ireland,*[59] the Court of Justice held the Data Retention Directive invalid as it violated, inter alia, the proportionality requirement.[60] The Court carried out an analysis of concepts such as the essence of the

---

[56] '[A]ny legislative measure referred to in paragraph 1 shall contain specific provisions at least, where relevant, as to:

(a) the purposes of the processing or categories of processing;
(b) the categories of personal data;
(c) the scope of the restrictions introduced;
(d) the safeguards to prevent abuse or unlawful access or transfer;
(e) the specification of the controller or categories of controllers;
(f) the storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing;
(g) the risks to the rights and freedoms of data subjects; and
(h) the right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction.'

[57] Recital 8 of the Regulation. This can be achieved through a tailored data protection notice.

[58] Article 52 (Scope of the Guaranteed Rights) of the Charter is as follows: "'. Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others. 2. Rights recognised by this Charter which are based on the Community Treaties or the Treaty on European Union shall be exercised under the conditions and within the limits defined by those Treaties. 3. In so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention. This provision shall not prevent Union law providing more extensive protection.'

[59] *Digital Rights Ireland* (n 21). Its conclusions have been confirmed in relation to the requirements that must be met by national legislation in Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB v Post-och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others* EU:C:2016:970.

[60] EU Parliament and Council Directive 2006/24/EC of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC [2006] OJ L/105 obliged Member States to implement legislation laying down the obligation on the providers of publicly available electronic

fundamental right to data protection and the necessity and proportionality of the restrictions which are arguably relevant when the restrictions to the right to data protection are applied to safeguard judicial independence and court proceedings.

In Ireland, s 158 of the Data Protection Act has implemented article 23(1)(f) of the Regulation and has provided for a restriction of the rights of data subjects as will be considered below. Subsection 6 of s 158 has established an *ad hoc* panel consisting of three judges nominated by the Chief Justice and empowered it to make rules to implement the restrictions[61] "to the extent that the restrictions are necessary and proportionate to safeguard judicial independence and court proceedings." The Rules have been made under S.I. No. 658/2018, the Data Rights Rules mentioned above, which entered into force on 1 August 2018.[62] Whilst the Data Protection Act has implemented the Regulation and restricted the rights of data subjects in respect of the processing of their personal data in order to safeguard judicial independence and court proceedings, the obligations of data controllers outlined in the Regulation remain fully applicable to processing activities of courts, even though data protection rights are restricted. In other words, whilst a data subject will see, eg, his right to access to his personal data restricted to safeguard judicial independence and court proceedings, the data protection principles of, eg, keeping personal data secured and confidential, could not be said to undermine judicial independence or court proceedings, and such obligations apply in their entirety to the courts.

Processing of personal data in the administration of justice

The data protection legislation applies only to information capable of being characterised as personal data. Furthermore, a processing activity of the information must occur, and the personal data so processed must form, or be intended to form, part of a filing system.[63] Both the definitions of 'processing' and of 'personal data' under article 2(1) of the Regulation have been consistently interpreted broadly by the Court of Justice, so as to include, in essence, any activity performed in relation to information which can lead, directly or indirectly, to the identification of a natural person.[64] The concept of identifiability, namely whether there are means which are reasonably likely to be used, in addition to information which is not per se sufficient to identify the natural person,[65] has also been interpreted broadly by the Court of Justice.[66]

As stated in the data protection notice for the courts, available on the website of the Courts Service,[67] courts process a broad range of personal data which can include names and contact

communications services or of public communications networks to retain certain data generated or processed by them for the purposes of the investigation, detection and prosecution of serious crime. See *Digital Rights* (n 21) [65].

[61] Section 158(3) of the Data Protection Act provides that the panel 'may make such rules as it considers necessary for the purpose of ensuring the effective application of a restriction under that subsection.'

[62] Data Protection Act (Section 158(3)) Rules 2018 (S.I. 658/2018).

[63] Article 2(1) of the Regulation.

[64] However, cf *Nowak v Data Protection Commissioner* [2020] IECA 174.

[65] Recital 26 of the Regulation.

[66] Case C-582/14 *Patrick Breyer v Bundesrepublik Deutschland* EU:C:2016:779, [43]. The case concerned dynamic IP addresses, which change each time there is a new Internet connection and which do not allow to establish a link with a given computer but only with the additional information provided by an Internet Service Provider.

[67] 'Processing of personal data by or on behalf of courts acting in a judicial capacity' (Courts Data Protection Notice) <www.courts.ie/courts-data-protection-notice> Accessed 27 August 2020.

information, but also information which may be detailed and, sometimes, highly sensitive.[68] The categories of personal data that are processed by courts depend on the nature of the proceedings concerned (eg criminal or civil proceedings), the content of pleadings (eg, a bankruptcy petition or an application for custody of a minor) and other court documents lodged, exchanged or issued in connection with, and of evidence given and submissions made in, those proceedings.[69] Courts receive personal data in the context of court proceedings from a number of different sources.[70] The types of personal data received by the courts, and the consequences of the provision of personal data or failure to provide such data, will depend on the general law, the rules of evidence and the rules of court.[71]

Information is normally disclosed in open court by the parties in person or on their behalf by counsel or witnesses, and it seems problematic that the information so disclosed is recorded in an anonymous way, so that it would not fall within the broad definition of personal data outlined above.[72] Litigants are thus not the only relevant data subjects, as whomsoever is rendered identifiable in open court following the disclosure of information and data protection obligations could be entitled to protection in respect to his or her personal data. The information concerning natural persons opened to court is normally recorded by means of digital audio recording, deposit of files in the court records and notes taken by court officials. Each and every such recording is likely to have personal data forming part of a filing system, whether or not that is an official court record. The difference between a filing system which is or is not a court record will be apparent in respect to the exercise of residual data protection rights under the Data Rights Rules.

Processing of personal data in the context of the administration of justice is not, however, limited to the disclosure of personal data in open court and the recording of personal data by courts and court officials — it extends to the further processing of the information by courts after the hearing. Before delivering its decision, whether it be *ex tempore* or a written reserved judgment, a court would normally rise to assess the matter in chambers. It is arguable that personal data will be processed in that context and the judge's notes might be organised in a way that the data contained therein form part of a filing system. Furthermore, in order to fulfil their obligation that justice is to be administered in public,[73] it has become the practice of the Superior Courts to direct that written judgments be uploaded onto the website of the Courts Service. This has, in effect, created an online database accessible by members of the public, in which disclosure of personal data of the litigants and witnesses to the public must comply with data protection obligations.

Responsibility for the implementation of obligations under data protection law rests mainly on the data controller who is, in essence, the natural or legal person that determines the

[68] ibid. This concerns, for example: racial or ethnic origin, political opinions, religious beliefs, trade union membership, genetic or biometric data, health data.
[69] ibid.
[70] ibid. These sources include: parties to proceedings (a plaintiff, a defendant), or their legal advisors; a witness giving evidence before the court; a person who is not a party to proceedings, but who is required to provide discovery (a pre-trial procedure); and other publicly available information (for example, from other reported cases).
[71] ibid.
[72] Recital 26 of the Regulation clarifies that 'The principles of data protection should […] not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.'
[73] In *Nash v DPP* O'Donnell J. held that 'The delivery of judgment is a part of the administration of justice in public and normally comprehends making the text of a judgment publicly available'.

purposes and means of the processing of personal data. The identification of a data controller within the Regulation,[74] which is to be interpreted broadly, is a matter of fact.[75] This depends on whether a legal or natural person determines the purposes and means of processing and if the entity actually benefits from the processing.[76] The latter factor will delineate if there is a factual influence of the entity over the processing activity.[77] In *re Mount Carmel Medical Group (South Dublin) Ltd*, Keane J held that there can be 'no discretion either to artificially delimit the number of persons against whom those rights can be asserted or to nominate only certain persons within that definition for that purpose'[78]. However, article 4(7) of the Regulation states that 'where the purposes and means of [the processing of personal data] are determined by […] Member State law, the controller or the specific criteria for its nomination may be provided for by […] Member State law'. The Data Protection Act has empowered the Superior Courts Rules Committee, the Circuit Court Rules Committee, and the District Court Rules Committee established under the Courts of Justice Act 1936 to implement Rules of Court in respect of the processing of personal data that are contained in a court record.[79] The Act has established an *ad hoc* committee empowered to implement Rules in respect of the processing of personal data which are not contained in a court record.[80] The Processing Rules do not contain a definition of 'controller', and the fact that they generally refer back to the Regulation for definitions not contained therein seems to *prima facie* suggest that whether the holder has an influence over how and by whom the data is processed and held is the key criterion. [81]

[74] Article 4(7) of the Regulation defines 'controller' as 'the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data'.

[75] *Re Mount Carmel Medical Group (South Dublin) Ltd* [2015] IEHC 450, [2015] 1 IR 671, [700]. The centrality of the factual influence of a controller over the processing operations has been recently emphasised by the European Data Protection Supervisor in relation to data processing within the ambit of the EU institutions: 'EDPS Guidelines On The Concepts of Controller, Processor and Joint Controllership Under Regulation (EU) 2018/1725' (European Data Protection Supervisor, 7 November 2019), p 7 <https://edps.europa.eu/sites/edp/files/publication/19-11-07_edps_guidelines_on_controller_processor_and_jc_reg_2018_1725_en.pdf> Accessed 27 August 2020.

[76] Case C-40/17 *Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW* eV EU:C:2019:629, [78]-[81].

[77] EDPS (n 77), p 7.

[78] *Re Mount Carmel Medical Group* (n 77), [701].

[79] Respectively, the Data Protection Act (Section 159(1)) Rules 2018 (S. I. 659/2018) ("the Superior Courts Records Data Processing Rules"); the Data Protection Act (Section 159(2)) Rules 2018 (S.I. 661/2018) ("the Circuit Court Records Data Processing Rules"); and the Data Protection Act (Section 159(3)) Rules 2018 (S.I. 663/2018) ("the District Court Records Data Processing Rules").

[80] Section 158(6) of the Data Protection Act: 'a panel of three judges nominated by the Chief Justice for the purposes of this section', ie the same panel of judges who have implemented the Data Rights Rules mentioned above in relation to the implementation of the restrictions to the rights of the data subjects in relation to personal data processed by or on behalf of courts acting in their judicial capacity. See also Section 159(4): 'The panel referred to in section 158(6) may make processing rules in respect of personal data—

(a) that are not personal data to which subsection (1), (2) or (3) applies, and

(b) in respect of which a court, when acting in its judicial capacity, is a controller.'

[81] Rule 3(2) of the Data Protection Act (Section 159(1)) Rules 2018 (S. I. 659/2018); Rule 3(2) of the Data Protection Act (Section 159(2)) Rules 2018 (S.I. 661/2018); Rule 3(2) of the Data Protection Act (Section 159(3)) Rules 2018 (S.I. 663/2018) all provide that: 'In these Rules, save as expressly provided otherwise, terms defined in the [Regulation] or the [Directive] shall have the meanings given to them in the Data Protection Regulation or, as the case may be, the [Directive].'

Since the purpose of processing personal data in the context of the exercise of the judicial function is established by law,[82] and the means of so doing are also established by law,[83] it is arguable that the law, through either the various statutes establishing the courts or the Constitution itself, has also established that courts are the 'controller' of personal data processed in the context of the exercise of the judicial function, as courts must process personal data for that purpose, and the judicial function remains theirs and theirs alone.[84] The main focus in order to establish whether a court acts as data controller therefore becomes whether it is, in fact, exercising its judicial function. In this regard, the above considerations on what may constitute 'courts acting in their judicial capacity' remain central. The issue that courts may be held to be joint controllers together with the Courts Service, as opposed to the qualification of the Courts Service as the processor of personal data on behalf of a court acting in its judicial capacity, has been recently considered by Judge Comerford in the Dublin Circuit Court, in respect of the publication of judgments on the Courts Service website.[85]

The concept of 'data processor' identifies the entities which firms employ to outsource parts of their activities in order to process personal data for or on behalf of the controller. Liability for the processing in a manner compliant with legislation remains on the controller.[86] In the context of the courts, a processor is any legal officer (potentially, even a solicitor),[87] directed to deal with personal data disclosed for the purposes of court proceedings and which will be held in a filing system (whether or not a court record). This is, it seems, the view taken in the Processing Rules, which defines processor as:

> a processor of personal data of which a [court] is the controller and includes without limitation, any court officer, any member of the staff of the Courts Service for the time being employed in a court office and any contractor of the Courts Service (including any employee or person working under the direction

[82] (n 39). As stated in the Data Protection Notice, the lawful basis of processing is to be found 'in the Constitution, by statute (for example, the Courts of Justice Acts 1924 as amended, the Courts (Supplemental Provisions) Acts 1961 as amended and, in the case of a Special Criminal Court, Part V of the Offences against the State Act 1939 as amended) and otherwise by law'.

[83] The Constitution is clear in Article 34.1: 'justice shall be administered in courts established by law by judges appointed in the manner provided by this Constitution'.

[84] The exercise of the judicial function by bodies which are not courts established by law is severely restricted by the Constitution.

[85] *Courts Service v Data Protection Commissioner* (Unreported, Dublin Circuit Court, Comerford J, 3 February 2020). A High Court judgment was delivered, stamped 'no redaction needed' and published shortly thereafter on the Courts Service website without redacting the name of the first notice party in the proceedings as mandated in a previous order of the High Court judge himself: this issue was the subject matter of a data protection complaint to the (then) Data Protection Commissioner ("DPC") by the first notice party ("the data subject"). The DPC decided that the Courts Service are in joint controllership, together with the relevant judge, of personal data contained in unofficial versions of judgments uploaded by the Courts Service onto their website and that any such upload in breach of a court order directing anonymisation is a breach of data protection obligations of the Courts Service as data controller ("the DPC's decision"). The DPC's decision was appealed to the Circuit Court pursuant to section 26 of the Data Protection Acts 1988 to 2014 ("the 1988 Act") and the DPC's findings were upheld by the Circuit Court judge without deciding the joint controllership issue. See also Colm Keena, 'Courts Service Breached Data Law by Publishing Man's Name' (Irish Times, 7 February 2020) <www.irishtimes.com/news/crime-and-law/courts-service-breached-data-law-by-publishing-man-s-name-1.4164590> accessed 22 August 2020.

[86] See article 28 of the Regulation.

[87] However, one must bear in mind that anyone in the precincts of the Court may be directed to do or not to do something in relation to personal data and could potentially be identified as 'processor' for the purposes of the Data Protection Act if all the other requirement for the applicability of data protection legislation are met.

> of such contractor) who is processing personal data of which a [court] is the controller.[88]

The Regulation obliges both controller and processor to set out their respective obligations and responsibilities in a contract or some other legal document.[89] In the case of processing activities of courts acting in their judicial capacity, this legal document is the Processing Rules mentioned above.[90] As regards the obligations of processors, the Rules contain broadly similar, if not identical, provisions. In particular, the processor must: act only on a direction given by or on behalf of the court concerning the processing; assist the court in ensuring compliance with the court's obligations under applicable data protection law; maintain all personal data in accordance with the duration of the processing; make available to the court concerned all information necessary to demonstrate compliance; implement such technical and organisational security measures as required by data security obligations; inform the president of the court concerned immediately if an instruction received from the court infringes data protection law;[91] notify the president of the court concerned immediately after becoming aware of any personal data breach.

Data protection obligations of courts

The Courts themselves, and court officers acting on their behalf as processors, are therefore obliged to implement data protection legislation, in particular the data protection principles.[92] When personal data disclosed in open court is filed in the court records, or in the case of the publication of judgments or other material upon the website of the Courts Service, it does not seem to be enough that courts simply 'delegate' to the parties the responsibility of complying with data protection obligations.[93] Whereas it may be argued that parties and courts are joint controllers in respect of the personal data disclosed in open court, the different stages of the processing activity are clearly severable. The obligations of a controller are imposed on the court once the data is processed, for example, after the data is disclosed in court. It would seem to be an inadequate solution to characterise the parties to a case as processors on behalf of the judiciary or sole controllers merely on account of having disclosed data in court.

I will now set out, in summary form, the most relevant principles of processing which courts and those acting on their behalf are obliged to implement when acting in their judicial capacity, insofar as they do not correspond to any of the restricted rights under article 23 of the Regulation:

---

[88] S.I. No. 665/2018 - Data Protection Act (Section 159(4)) Rules 2018, s3(1).

[89] Article 28(3) of the Regulation provides that: 'Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller.'

[90] As clarified by the Explanatory Memorandum attached to the rules: 'These rules, made under section 159 […] of the Data Protection Act, govern, for the purposes of Article 28(3) of [the Regulation and Article 22(3) of [the Directive], the processing by a processor of personal data […]'.

[91] The ground-breaking consequences of this obligation and its compatibility with s 65 of the Courts Officers Act 1926 and the independence of the judiciary merit a whole and in-depth analysis that is outside the scope of this paper.

[92] Article 5 of the Regulation.

[93] See para 7 of the Supreme Court Practice Direction SC19 "Conduct of proceedings in Supreme Court".

- Data security and confidentiality: personal data must be processed ensuring appropriate technical and security measures are in place, including protection against unauthorised or unlawful processing and against accidental loss.[94] Courts rely on the Courts Service and its contractors to provide adequate security measures.[95] Adequate training of all personnel, including judges, seems to be essential in order to fulfil the principle. No matter which format (hard copy or soft copy electronic database) or typology of filing system (a court record or not), the security obligation must be fulfilled. In this respect it seems to be the case that although the courts are not legally obliged to do so,[96] in the event of a data breach which exposes the rights and freedoms of an individual to a high risk, it would be good practice if the courts consider whether the circumstances warrant the sending of a notification to the natural persons, especially if the data breach is likely to result in a high risk to the rights or freedoms of individuals.

- Data retention:[97] the Processing Rules have interestingly differentiated between the retention period of personal data, which form part of a court record,[98] and that of personal data which do not form part of a court record. As regards the former, the retention period is very broadly defined as the period necessary for the purposes of the determination of court proceedings to which the personal data relate, including any appeal and enforcement action, prior to the transfer of the court record in accordance with the provisions of the National Archives Act 1986. As regards the latter, the retention period is described by the Processing Rules as 'such period as the judge or, as the case may be, the court concerned shall require.'[99] This, in practice, should not however exceed the retention period outlined in the courts data protection notice, namely 'for as long as necessary to enable the courts to perform their functions under the Constitution and law, to ensure the administration of justice and to facilitate the efficient management and operation of the courts.'[100]

- Purpose limitation: 'personal data should be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible.'[101] An example of this principle in the context of the administration of justice is the disclosure of information related to court proceedings to lawful recipients. Specific Rules ("Data Disclosure Rules") have been made pursuant to section 159(7) of the Data Protection Act.[102] Subject to the provisions of statute, the relevant rule of court, any practice direction of the court concerned and any order of that court, members of the press, who have sufficient proof of their status, for the purpose of facilitating the fair and

[94] Article 5(1)(f) of the Regulation.
[95] The provision of adequate measures is, as seen above, one of the processors' obligation.
[96] As we will see, the right of the data subjects to be notified of data breaches does not exist.
[97] Article 5(1)(e) of the Regulation.
[98] A court record is defined by the Processing Rules as 'a record of a superior court of record'.
[99] Rule 4(6) of the Data Protection Act (Section 159(4)) Rules 2018 (S.I. 665/2018).
[100] (n 68).
[101] Article 5(1)(b) of the Regulation.
[102] S.I. No. 660 of 2018 (Superior Courts), S.I. No. 662 of 2018 (Circuit Court), S.I. No. 664 of 2018 (District Court).

accurate reporting of a hearing in the proceedings can ask to have court records disclosed to them. As regards members of the public, whilst their access to the court records have been severely limited,[103] those in attendance at court will hear information disclosed, and are allowed to take written or shorthand notes. Electronic recording remains strictly forbidden.[104] Personal data contained in a judgment or decision of a court, or a list or schedule of proceedings or hearings (for example, the legal diary) is also made accessible to the public. Importantly, the Rules provide that nothing 'authorises the use of any information in any document included in a court record which has not been opened or is not deemed to have been opened at a hearing before the court concerned'.[105]

- Data minimisation: personal data must be 'adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.'[106] In the context of the administration of justice, this principle may be relevant, *inter alia*, in respect of the publication of judgments onto the website of the Courts Service. When parties disclose information or give evidence in open court, they themselves decide the extent to which personal data is disclosed. However, as regards the reasoning for a judge's decision, the principle should be implemented when the judgment is directed to be published on the website of the Courts Service. It could be a good practice that judgments be reviewed, even with the help of the parties themselves, before distribution, in order to avoid unnecessary processing of data.

Data protection rights of the data subjects in the administration of justice

In order to safeguard the right to data protection, as there is no statutorily established exception to the principle that justice is to be administered in public, apart from, indirectly, the principles of data protection outlined above, parties or witnesses have no entitlement to have their names anonymised, nor does there exist any entitlement to have court proceedings conducted *in camera*.[107] It seems difficult to envisage a case in which the exceptional circumstances indicated in *Gilchrist v Sunday Newspaper* would warrant the triggering of the common law jurisdiction to direct that proceedings be held *in camera,* purely on the basis of the right to data protection, without establishing a high risk to another right or freedom of individuals. This is because the balance between the right to data protection and the right to fair trial has already been achieved by the Regulation and its implementation in the Data Protection Act, with the outcome of restricting the data protection rights of data subjects, as we will presently see.

---

[103] Since 29 April 2019: 'Access to court files in the Superior Courts' (High Court Practice Decisions) '[t]he files maintained in the […] offices of the Superior Courts shall not be made available to any person attending at any of those offices. For the avoidance of doubt this includes the parties to the proceedings and the solicitors on record" (Practice Direction HC86 "Access to court files in the Superior Courts' <www.courts.ie/content/access-court-files-superior-courts-1> accessed 27 August 2020.

[104] See 'Use of cameras and electronic devices in court' (High Court Practice Directions) <www.courts.ie/content/use-cameras-and-electronic-devices-court-3> accessed 27 August 2020.

[105] S.I. No. 664/2018 - Data Protection Act (Section 159(7): District Court) Rules 2018, s 4(1).

[106] Article 5(1)(c) of the Regulation.

[107] This might contrast the current trend in Europe. See, for example, the new practice of the Court of Justice <https://curia.europa.eu/jcms/upload/docs/application/pdf/2018-06/cp180096en.pdf> last accessed 21 October 2020.

The Data Protection Act has restricted the specific rights vested in the data subject to the extent that such restriction is necessary for the safeguarding of judicial independence and court proceedings. The extent of the restriction has been outlined by the Data Rights Rules mentioned above. Rule 4 establishes the general rule that all the rights are restricted when personal data are processed by or on behalf of courts acting in their judicial capacity,[108] except for the extent specified by rules 5 to 7 of the Data Rights Rules.[109] This implies that the following are all subject to an absolute restriction: the right to erasure (right to be forgotten),[110] the right to restriction of processing,[111] the right to notification obligation regarding rectification, erasure, or restriction,[112] the right to data portability,[113] the right to object,[114] the right against automated decision making,[115] and the right to be notified of data breaches when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.[116]

The most relevant restrictions to the rights of the data subjects, as operated by the Data Rights Rules are, in summary:

- Right to information:[117] data subjects must be aware that their personal data is being processed by the controller. To that end, they have to be informed about who is to process their personal data and how it is to be processed. Rule 5 provides that this right in relation to processing activities of courts acting in their judicial capacity is fulfilled 'by way only of general notice published on behalf of the courts in their capacity as data controllers on the Courts Service website'. Rule 5 then goes on to detail the contents of the said notice.[118]
- Right of access: data subjects have the right to obtain, in intelligible form and without expense, all personal data about them held by a controller.[119] Rule 6(1) of the Data Rights Rules limits the extent of that right only to the personal data contained in court records where a provision of statute, rules of court, or the practice of the court so permits.[120] As regards recording of proceedings not contained in court records, Rule 6(2) provides that the right exists, subject to an application made to the court concerned, in accordance with the relevant

[108] See Rule 3 which importantly limits the scope of the Data Rights Rules to courts acting in their judicial capacity, as opposed to the Data Protection Act, which mentions the restriction in relation to, more broadly, the safeguard of judicial independence and court proceedings.
[109] Rule 4 reads as follows: 'In accordance with section 158(1) of the 2018 Act and for the purposes of section 158(3) of the 2018 Act, save to the extent specified in rules 5 to 7 of these Rules, Articles 12 to 22 and 34 (and Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22) of the Data Protection Regulation and sections 87, 90, 91, 92 and 93, and section 71 insofar as it relates to those sections, of the 2018 Act shall not apply to the processing of any personal data referred to in rule 3 of these Rules.'
[110] Article 17 of the Regulation.
[111] Article 18 of the Regulation.
[112] Article 19 of the Regulation.
[113] Article 20 of the Regulation.
[114] Article 21 of the Regulation.
[115] Article 22 of the Regulation.
[116] Article 34 of the Regulation.
[117] Articles 12 to 14 of the Regulation.
[118] Courts Data Protection Notice (n 68).
[119] Article 15 of the Regulation.
[120] Practice Direction HC86 (n 106).

rules of court.[121] This provision therefore leaves ample discretion to the court concerned.

- Right to rectification:[122] data subjects have the right to have inaccurate data rectified or corrected.[123] Rule 7 of the Data Rights Rules provides that in respect of processing activities of courts acting in their judicial capacity the right exists subject to an application made to the court concerned, in accordance with the relevant rules of court.[124] Rule 7, similar to Rule 6(2) in respect of access requests for personal data not contained in court records, leaves ample discretion to the court concerned.

A broad analysis of the Data Rights Rules enacted under the Data Protection Act for the purposes of implementing the restrictions to the rights of the data subjects – implementation which is required to be proportionate and necessary to safeguard judicial independence and court proceedings – shows that the Rules Committee seems to have incorporated those rights within the pre-existent court procedural rules. That is arguably a practical way to safeguard judicial proceedings. Whether that implementation is 'necessary and proportionate' with the objective is outside the scope of this paper.

The supervisory authority for processing activities of courts acting in their judicial capacity

Ireland is one of the few countries in Europe that has established by statute an *ad hoc* supervisory authority competent for the processing activities operations of courts when acting in their judicial capacity. Section 157(1) of the Data Protection Act reads as follows: 'The judge ("assigned judge") for the time being assigned for that purpose by the Chief Justice shall be competent for supervision of data processing operations of the courts when acting in their judicial capacity.' The Assigned Judge, since August 2018, has been Baker J.[125]

The interpretation of the wording 'processing operations of courts acting in their judicial capacity' has been dealt with above and those considerations are useful in order to understand the jurisdiction of the Assigned Judge. It seems appropriate here to focus on the nature of the role and on the related powers which have not been explored so far in practice or in the literature. The role could be seen as some form of hybrid between a data protection

[121] 'A data subject may seek access to any part of a note or recording made of proceedings only by making an application to the court concerned subject to and in accordance with the provisions of Order 123, rule 9 of the Rules of the Superior Courts (in the case of the Supreme Court, Court of Appeal or High Court), Order 67A, rule 8 of the Circuit Court Rules (in the case of the Circuit Court) or, as the case may be, Order 12B, rule 5 of the District Court Rules (in the case of the District Court).'

[122] Article 16 of the Regulation.

[123] Denis Kelleher and Karen Murray, *EU Data Protection Law* (Bloomsbury 2018), para 9.19.

[124] 'An application by a data subject for the rectification without undue delay of inaccurate personal data processed by or on behalf of a Court which is contained in a judgment or order of the court may be made by means only of an application subject to and in accordance with the provisions of Order 28, rule 11 of the Rules of the Superior Courts (in the case of the Supreme Court, Court of Appeal or High Court), Order 65, rule 3 of the Circuit Court Rules (in the case of the Circuit Court) or, as the case may be, Order 12, rule 16 or Order 45E, rule 3 of the District Court Rules (in the case of the District Court), and only by a person entitled to make such application in accordance with the rule of court concerned.'

[125] 'Right to lodge a complaint about the use of your personal data by or on behalf of a court acting in a judicial capacity' (Data Protection Complaints Procedure) <www.courts.ie/data-protection-complaints-procedure> accessed 16 October 2020.

officer with limited powers, and an actual data protection supervisory authority, since the Assigned Judge has the duty to assess data protection complaints.

Section 157(2) describes the tasks of the Assigned Judge, without specifying her powers, and establishes a right of data subjects to lodge a complaint, which must include the right to have that complaint decided by her:

> 'The assigned judge shall, in particular—
>
> (a) promote awareness among judges of the provisions of the Data Protection Regulation, the Directive and any enactment, rule made under section 158(3) or other rule of law that gives further effect to the Data Protection Regulation or effect to the Directive, and ensure compliance with those provisions, and
>
> (b) handle, and investigate to the extent appropriate, complaints in relation to data processing operations of the courts when acting in their judicial capacity.'

The powers of the Assigned Judge must be carefully exercised in conjunction with the principle of judicial immunity from suit and the independence of each judge acting in a judicial capacity. Even a declaration that a judge has breached a data protection obligation may be contrary to such principle. The complaint procedure before the Assigned Judge is arguably within the realm of administrative decisions and is probably subject to judicial review, although that would imply in turn that there are remedies against courts in relation to data protection obligations, in breach of the principle of judicial immunity.

Conclusion and caveat

Courts have an obligation to ensure that justice is to be administered in accordance with data protection law, to the extent to which it is applicable to them. They have jurisdiction in the inherent power of the court to manage its proceedings, and it is therefore important that the practice of the courts does not leave sole responsibility to the parties to ensure that data opened or otherwise provided to courts is compliant with data protection obligations. The important role in the administration of justice played by the Courts Service could operate as a shield against the breach of the principle of judicial immunity from suit. It seems to be the case in the administration of justice that processors play the most important role in the fulfilment of data protection obligations. This seems to be in line with the broad data protection obligations of processors outlined in the Processing Rules emanated under the Data Protection Act.

The operation of the separate regime for data protection established to reconcile the objectives of protection of the rights of data subjects and the independence of the judiciary is still in its infancy. It remains to be seen how the rules and principles will play out in practice. The number of complaint and requests to the Assigned Judge is relatively small and it is not yet possible to form a view as to the likely future difficulties and developments. Nonetheless, the existence of a separate regime has been the subject of much discussion at European level and is an important element of the maintenance of the rule of law.