Irish Communication Review

Volume 16 | Issue 1 Article 9

June 2018

Data Protection and Privacy for Media and Individuals Under Irish and EU Law

Sarah Kearney
sarah.kearney@lawlibrary.ie

Data protection and privacy for media and individuals under Irish and EU law

Sarah Kearney

Abstract

Recent public discussion has seen an increasing emphasis placed on data protection and privacy. An accord must be struck between the individual's right to privacy and an organisation's right to examine an individual's personal information for its given commercial, contractual or social media activities. This paper examines the evolution of data protection and regulation in Irish and EU law, Illustrating that data protection applies in relation to the publication of material in the media, even if it may still be set aside in the case of public interest. It concludes that the Irish and European Courts place considerable significance on the protection of the right to privacy and data protection as demonstrated by the recent jurisprudence and cases referred to the Courts of Justice of the EU. Furthermore, it is suggested that the introduction of the General Data Protection Regulation and the Data Protection Act 2018 should lessen the Irish media's uncertainties on how to comply with data protection.

Introduction

In the current age of the internet and social media platforms, evident in many facets of private and commercial life, there is an ever-increasing emphasis placed on data protection and privacy. On attempting to strike an accord between such

liberties, it is necessary to examine an individual's right to privacy and to safeguard information from being disseminated to third party organisations with an organisation's right to examine an individual's personal information for its given commercial, contractual or social media activities[1]. The awareness of the protection of rights such of this nature have possessed recognition since the enacting of the Constitution, with subsequent Common Law established by the Irish Courts[2] and, indeed on a European footing since the enacting of the Universal Declaration of Human Rights.

European legislation presently dictates the purpose of data protection laws pursuant to Article 8(2) of the Charter of Fundamental Rights of the European Union states that: '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...'

The Data Protection Acts 1988 to 2018 form the statutory basis for data protection law in Ireland. Since the Office of the Data Protection Commissioner (ODPC) was given statutory empowerment, the transparency of complaints such as the categories of databases containing any European citizen's personal data (those individuals otherwise known as 'Data Subjects') places emphasis, for example, on awareness of the obligation of registration placed on certain controllers and processors who are participating in collecting such personal data. The Commissioner refers to the principles of data protection for controllers being the adherence to the obtaining and processing of information fairly; keeping it only for one or more specified, explicit and lawful purposes; using and disclosing it only in ways compatible with these purposes; keeping it safe and secure; keeping it accurate; complete and up-to-date; ensuring that it is adequate; relevant and not excessive; retaining it for no longer than is necessary

[1] See generally Lambert, 'Data Protection Law in Ireland', (2nded.) Clarus Press, 2016 and Kelleher, 'Privacy and Data Protection Law in Ireland', (2nd ed.) Bloomsbury Professional 2015.

[2] *McGee v Attorney General* [1974] IR 284 first examined the concept of the right to privacy as a Constitutional right. Wherein the Supreme Court espoused 'it is scarcely to be doubted in our society that the right to privacy is universally recognised and accepted with possibly the rarest of exceptions, and that the matter of martial relationship must rank as one of the most important of matters in the realm of privacy.'

for the purpose or purpose; and giving a copy of his or her personal data to that individual on request[3].

The latest Annual Report of the Data Protection Commissioner of Ireland 2017[4], examines the evolution of types of complaints made to the Office of the Date Protection Commissioner (ODPC). Interestingly, it appears that the total complaints received in 2017 was 2,642, up from 1,479 in 2016 (a 79% increase) with the largest single category being access rights which made up 1,372 (or 52%) of the total. The main goals are listed as building 'the capacity and capabilities of the DPC to reflect our enhanced role under the new GDPR and ePrivacy regime, close collaboration and partnership with EU and International data protection authority counterparts, and regulatory bodies in other sphere, drive better data protection awareness and compliance through strategic consultation and effective oversight and enforcement. These are discussed, in part, below.

Irish jurisprudence

The Irish Superior Courts have referred questions of significant importance to the Court of Justice of the European Union resulting in some seminal decisions within the area of data protection law.

In *Digital Rights Ireland limited v Ireland*[5] the Applicant, the owner of a mobile phone which it used since 2006, challenged national measures requiring retention of data relating to electronic communications sought a declaration of the invalidity of Directive 2006/24. This Directive required telephone communications service providers to retain traffic and location data for a period specified by national law to prevent, detect, investigate and prosecute crime and safeguard security. Whilst the retention of content was not permitted. It did allow for the identification of the 'source of a communication and its destination, the date, time, duration and type of a communication, users' communication equipment, and location of mobile equipment including name and address of

[3]See the 'Eight Rules of Data Protection' at https://www.dataprotection.ie/docs/A-Guide-for-Data-Controllers

[4] See https://www.dataprotection.ie/docimages/documents/DPC%20Annual%20Report%202017.pdf

[5] C-293/12 and C-594-12, Digital Rights Ireland Limited v Ireland, 8th April 2014

subscriber, calling telephone number, number called and IP address for internet users'.

The Applicant successfully argued that the Directive in its use as a means of communication was in breach of the individual's right to private life and, did in fact constitute processing of personal data guaranteed by the Code of Federal Regulations and the European Charter of Fundamental Rights.

In *Schrems -v- Data Protection Commissioner* C-362/14[6] the compatibility of the mass transfers of personal data to the United States of America was examined with the compatibility of European Law to do so. The applicant, an Austrian national residing in Austria, was a user of Facebook which he had concluded a contract with Facebook Ireland (a subsidiary of Facebook Inc.) located in the United States. The commercial practice dictated that Facebook Ireland's users' personal data transferred to the servers in the United States of Facebook Inc. and further processed.

The Applicant sought to prohibit Facebook Ireland from transferring his personal data to the United States, which (it was suggested) did not ensure adequate protection against the surveillance activities engaged in there by public authorities. The Defendant rejected the complaint on grounds that there was no evidence that it had been accessed by the National Security Agency and that the Commission decision 2000/520 had found that the USA ensures an adequate level of protection in the 'Safe Harbour' program.

The CJEU found that this practice was an interference with the fundamental right to respect for private life of persons whose personal data is or could be transferred from the Europe to the United States (without limiting the interference with any pursuit of legitimate objectives such as national security) '… legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life. Likewise, legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to

[6]Judgment of the Court (Grand Chamber) of 6 October 2015, Maximillian Schrems v Data Protection Commissioner

obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection.'

After the delivery of the *Schrems* decision, the 'Safe Harbour' regime was struck down by the CJEU and a new framework for the transfer of personal data from the EU to the US, the 'Privacy Shield', was adopted. Thereafter, the Data Protection Commissioner referred a question to the High Court on the validity or otherwise of European Commission decisions approving data transfer channels known as Standard Contractual Clauses (SCCs). These empower the Commission to decide on the adequacy of protection for personal data in respect of transfers which are binding on Members States. A decision of this calibre will have significant impact on international trade agreements and privacy rights of European citizens. The Data Protection Commissioner was successful in attaining a preliminary reference form the Irish High Court in March 2017 to be considered by the CJEU.In coming to the same conclusion Justice Costello espoused that there existed 'well founded concerns… that the laws of the United States do not ensure this continuity of a high level of protection and that the standard contractual clauses do not ensure that data transferred to the United States enjoys a high level of protection to which data subjects in the European Union are entitled by virtue of the provisions of the Directive as read in the light of the Charter[7]'. At the time of writing, a judgment from the Court of Justice of the EU in '*Schrems II*' is still extant. Interestingly, the CJEU has recently ruled on a parallel legal point that whilst Schrems may bring an individual action in Austria against Facebook Ireland, as the assignee of other consumers' claims, he cannot benefit from the consumer forum for the purposes of a collective action[8].

A subsequent EU-US 'Umbrella Agreement', which sets out a high-level data protection framework for EU-US law enforcement cooperation was given legislative footing on 1st February 2017.This agreement covers all personal data of Data Subjects exchanged between the EU and the US for the purpose of prevention, detection, investigation and prosecution of criminal offences, including terrorism.

[7]Data Protection Commissioner v Facebook IrelandLtd [2017] IEHC 545

[8]Case C-498/16 Maximilian Schrems v Facebook Ireland Limited

In the wake of fundamental decisions like the latter, and the legal complexities that exist with transferring personal data to jurisdictions outside of the EU, it is of no surprise that more comprehensive legislation has been drafted.

At the dawn of GDPR's implementation, Max Schrems under his non-profit organisation, 'None of Your Business', lodged complaints against Google, Facebook, Instagram and WhatsApp, arguing they were acting illegally by forcing users to accept intrusive terms of service or lose access. Regarding the policing of the adequacy of data privacy notices and the issue of 'forced consent', perhaps judgment in '*Schrems III*' will cast light on same in due course.

The General Data Protection Regulation

The legislative framework that surrounds the law on data protection, its collection, handling, storage, and processing has been significantly reformed with introduction of the General Data Protection Regulation (hereinafter 'the Regulation'). The framework replaces the European Data Protection Directive 95/46/ EC which it has been suggested[9] by experts and precedent has been implemented inconsistently across Europe. The deadline for the implementation across the Member States was the 25th of May 2018.

The Regulation is applicable to all Member States and European citizens' personal data. Thus, the Regulation has a significant impact on all organisations (as well as self-employed, sole traders) that retain any personal data of private individuals. It is important to note that the legislative protection extends regardless of where the personal data is collected, stored, or processed. As such, the implementation of the Regulation is applicable to all organisations that collect and store personal data of European Citizens whether inside or outside of the European Union. Therefore, the compliance with the Regulation itself has extra-territorial applicability effect, and should be borne in mind even if you do not have a formal presence within the European Union where the activities relate to offering goods or services, to European citizens (this is regardless of

[9]See 'Reform of Data Protection Legal Framework' available on http://ec.europa.eu/justice/data-protection/reform/index_en.htm which notes:
'The Regulation is an essential step to strengthen citizens' fundamental rights in the digital age and facilitate business by simplifying rules for companies in the Digital Single Market. A single law will also do away with the current fragmentation and costly administrative burdens, leading to savings for businesses of around €2.3 billion a year'.

whether same requires the payment of a charge or fee). It is also applicable in the commercial monitoring of behaviour that takes place within the European Union. Any non-European Data Controllers processing the data of European citizens will possess a positive obligation to appoint a representative in Europe.

Some notable changes that the Regulation has introduced includes stricter rules on informed consent, the data subjects will retain further rights on the control and use[10] of their data. If a data breach occurs which 'result in a risk for the rights and freedoms of individuals' then there is a further obligation on all organisations of notification to Data Subjects within 72 hours of such a breach. There is the potential for substantial penalties for serious infringements of non-compliance with the Regulation placed on data controllers. The maximum penalty of €20 million or 4% of annual global revenue can be imposed, whichever is greater (or an organisation can be fined 2% of annual global revenue for not having their records in order).

A future function of the Regulation is the empanelling of a European Data Protection Board. The Board is composed of the head of one supervisory authority of each Member State and of the European Data Protection Supervisor, or their respective representatives. This allows for independent voting rights on policy and procedure of the newly enacted Regulation across all Member States.

Perhaps the most notable change with the Regulation, of commercial interest, is the designation of a Data Protection Officer (DPO) under Article 35 thereof.

The appointment of a DPO in Ireland requires that an individual 'shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39'. The role of the DPO among other duties is to comply

10

The rights of control include, by are not limited to access to information whether personal data concerning them is being processed, its location and/or purpose. A data subject additionally has the 'right to be forgotten' for erasure of same data: the controller or processor should endeavour to consider 'the public interest in the availability of the data' when considering such requests. And, the right to data portability whereby the data subject can request to receive and/or transmit their personal data to another controller.

Perhaps the most important introduction is the concept of 'privacy by design' which encourages the minimisation of data collection, control and process of personal data that is 'absolutely necessary' for the completion of an organisation's commercial functionality.

with internal record keeping requirements. The latter expertise and qualities shall be commensurate with the sensitivity, complexity and how voluminous the data pertains to be. Under the Data Protection Act 2018[11] the functions of a data protection officer include 'informing and advising the controller, and the employees of the controller who carry out processing, of their obligation' under law, monitoring the compliance and the policies of the controller in relation to the protection of personal data, 'including the assignment of responsibilities in the controller in relation to the protection of personal data, the raising of awareness and the training of staff involved in processing operations in that regard, and any audit activity related to the protection of personal data', carrying out of a data protection impact assessment, and acting as the contact point for data subjects, etc.

The European Parliament proposal text suggests that a DPO be 'mandatory for all enterprises that process special categories of data, including information such as health data or religious and political beliefs'. Additionally, the European Commission proposal text recommends the position being mandatory where the organisation with 250 employees, while the Parliament text calls for 'those processing the personal data of over 5000 data subjects in any 12-month period'. The latter proposals have not been specifically addressed in the Regulation and assumedly will be adjudicated on subjectively when the Regulation is implemented. According to the DPA 2018, the appointment of a DPO is a requirement where the core activities of the organisation involve large scale processing (or a defined public body) and/or when special categories or personal data relating to criminal convictions are processed. Otherwise, revised legislative guidelines are not definitive of the appropriate circumstances in which to appoint a DPO, this will have to be access by the individual organisations.

Within the Irish jurisdiction, the areas of privacy and freedom of expression are both well enshrined in the Constitution. Indeed, in a society where technology is accelerating at an increasing rate there must be safeguards created, for example, when the data controller is a public body.

Additionally, the Regulation places a positive obligation on controllers in relation to security awareness 'the controller and the processor shall implement

[11] See section 84(5) of the Data Protection Act 2018

appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

a) the pseudonymisation and encryption of personal data;
b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing'.

Critically another societal consideration is the rights in which the Irish Press should consider when contemplating material and data protection obligations prior to publication.

Expectations of the media having regard to Data Protection Law

The Court of Justice of the European Union[12], in safeguarding the importance of freedom of speech, has held that 'journalist activities' should be interpreted broadly and cover the disclosure to the public of information, opinions or ideas by any means (with the expectation of advertisements). Certain individuals may invoke the journalism exemption in their capacity for example, as a blogger (and not a professional journalist) if they are posting information or ideas for public consumption online[13]. If the blog or comment is not intended as public interest journalism but rather social, recreational internet use then 'domestic purposes' exemption may be sought.

The astonishingly malleable influence which online platforms possess with international political affairs is becoming ever-apparent: particularly in the wake of the latest US and French presidential elections.

What are the legal requirements which journalists must endeavour to comply with whilst balancing the principles of free press with data protection law?

The Data Protection Acts allows for journalists to safeguard privacy and to redact the identity of individuals who are confidential sources. Irish legislation, further provides that personal data that are processed for 'journalistic purposes or for

[12] C-73/07 Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy, 16th December 2008

[13]The Law Society and others v Kordowski[2011] EWHC 3182 (QB).

the purposes of academic, artistic or literary expression, shall be exempt from compliance… having regard to the importance of the right of freedom of expression and information in a democratic society, compliance with the provision would be incompatible with such purposes.'[14]

The DPA 2018, subject to the rules of the applicable Court or in circumstances where the Court directions otherwise or if the in-camera rule applies, authorises 'the disclosure, for the purpose of facilitating the fair and accurate reporting of the proceedings, to a bona fide member of the Press or broadcast media and at the member's request, of information contained in a record of proceedings before a court for which the Committee is the rule-making authority.'

In Ireland, the ODPC examined the News of the World cases and commented that '… data protection applies even in relation to the publication of material in the media. However, in such cases, the issue to be considered in the first instance is whether a general public interest could be deemed to apply to the publication of the material. If it does, then the general requirements of data protection are set aside. However, if no public interest could legitimately be claimed, then the media must have due regard to their data protection obligations'[15].

The English Judiciary has recently examined the balancing exercise of the media's freedom of speech with the individuals' right to private life. The application involved a claim for damages and an injunction for misuse of private information, harassment and breaches and threatened breaches of the Data Protection Act 1998 (DPA 1998). The Court in finding there was no incompatibility with the Directive espoused: -

'It is well recognised in both domestic and European jurisprudence that in the field of journalism, protection of freedom of expression requires particular importance to be attached to protection from pre-publication restraint, and that protection of the private rights of individuals may adequately be secured by the ability to sue for damages after publication[16].'

[14] Section 43 of the Data Protection Act 2018

[15] https://www.dataprotection.ie/docs/Case-Study-6-News-of-the-World:-Limits-of-the-Media-Exemption/463.htm

[16] *Stunt v Associated Newspapers Ltd* [2017] EWHC 695 (QB) see paragraph 51

The UK authority, which is of persuasive authority for Irish Courts, emphases the ability to have access to the Courts for an action in defamation. The benefit (if any) of redress, and the possibility of availing of damages for reputational damage, being available after publication is matter for the person alleging same.

Conclusion

The introduction of the General Data Protection Regulation and the Data Protection Act 2018, lessens the Irish press's uncertainties on how to comply with data protection and, its obligations. The exercise of mass surveillance and data retention is a topical area, especially within the Irish legal landscape with the recent scandal of Cambridge Analytica, to name one example. It is abundantly clear that the Irish Courts place significance on the protection of the right to privacy, and data protection, demonstrated by the recent jurisprudence and cases referred to the Courts of Justice of the EU.