The Privacy, Data Protection and Cybersecurity Law Review

Third Edition

Editor
Alan Charles Raul

Law Business Research

The Privacy, Data Protection and Cybersecurity Law Review

Third Edition

Editor
Alan Charles Raul

Law Business Research Ltd

PUBLISHER
Gideon Roberton

SENIOR BUSINESS DEVELOPMENT MANAGER
Nick Barette

BUSINESS DEVELOPMENT MANAGER
Thomas Lee

SENIOR ACCOUNT MANAGERS
Felicity Bown, Joel Woods

ACCOUNT MANAGERS
Jessica Parsons, Jesse Rae Farragher

MARKETING COORDINATOR
Rebecca Mogridge

EDITORIAL ASSISTANT
Gavin Jordan

HEAD OF PRODUCTION
Adam Myers

PRODUCTION EDITOR
Anne Borthwick

SUBEDITOR
Anna Andreoli

CHIEF EXECUTIVE OFFICER
Paul Howarth

Published in the United Kingdom
by Law Business Research Ltd, London
87 Lancaster Road, London, W11 1QQ, UK

www.TheLawReviews.co.uk

ISBN 978-1-910813-32-4

Printed in Great Britain by
Encompass Print Solutions, Derbyshire
Tel: 0844 2480 112

THE LAW REVIEWS

THE MERGERS AND ACQUISITIONS REVIEW

THE RESTRUCTURING REVIEW

THE PRIVATE COMPETITION ENFORCEMENT REVIEW

THE DISPUTE RESOLUTION REVIEW

THE EMPLOYMENT LAW REVIEW

THE PUBLIC COMPETITION ENFORCEMENT REVIEW

THE BANKING REGULATION REVIEW

THE INTERNATIONAL ARBITRATION REVIEW

THE MERGER CONTROL REVIEW

THE TECHNOLOGY, MEDIA AND
TELECOMMUNICATIONS REVIEW

THE INWARD INVESTMENT AND
INTERNATIONAL TAXATION REVIEW

THE CORPORATE GOVERNANCE REVIEW

THE CORPORATE IMMIGRATION REVIEW

THE INTERNATIONAL INVESTIGATIONS REVIEW

THE PROJECTS AND CONSTRUCTION REVIEW

THE INTERNATIONAL CAPITAL MARKETS REVIEW

THE REAL ESTATE LAW REVIEW

THE PRIVATE EQUITY REVIEW

THE ENERGY REGULATION AND MARKETS REVIEW

THE INTELLECTUAL PROPERTY REVIEW

THE ASSET MANAGEMENT REVIEW

THE PRIVATE WEALTH AND PRIVATE CLIENT REVIEW

THE MINING LAW REVIEW

THE EXECUTIVE REMUNERATION REVIEW

THE ANTI-BRIBERY AND ANTI-CORRUPTION REVIEW

THE CARTELS AND LENIENCY REVIEW

THE TAX DISPUTES AND LITIGATION REVIEW

THE LIFE SCIENCES LAW REVIEW

THE INSURANCE AND REINSURANCE LAW REVIEW

THE GOVERNMENT PROCUREMENT REVIEW

THE DOMINANCE AND MONOPOLIES REVIEW

THE AVIATION LAW REVIEW

THE FOREIGN INVESTMENT REGULATION REVIEW

THE ASSET TRACING AND RECOVERY REVIEW

THE INSOLVENCY REVIEW

THE OIL AND GAS LAW REVIEW

THE FRANCHISE LAW REVIEW

THE PRODUCT REGULATION AND LIABILITY REVIEW

THE SHIPPING LAW REVIEW

THE ACQUISITION AND LEVERAGED FINANCE REVIEW

THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

THE PUBLIC-PRIVATE PARTNERSHIP LAW REVIEW

THE TRANSPORT FINANCE LAW REVIEW

THE SECURITIES LITIGATION REVIEW

THE LENDING AND SECURED FINANCE REVIEW

THE INTERNATIONAL TRADE LAW REVIEW

THE SPORTS LAW REVIEW

THE INVESTMENT TREATY ARBITRATION REVIEW

THE GAMBLING LAW REVIEW

THE INTELLECTUAL PROPERTY AND ANTITRUST REVIEW

THE REAL ESTATE, M&A AND PRIVATE EQUITY REVIEW

THE SHAREHOLDER RIGHTS AND ACTIVISM REVIEW

www.TheLawReviews.co.uk

ACKNOWLEDGEMENTS

The publisher acknowledges and thanks the following law firms for their learned assistance throughout the preparation of this book:

ALLENS

ASTREA

BAKER & MCKENZIE - CIS, LIMITED

BOGSCH & PARTNERS LAW FIRM

CMS CAMERON MCKENNA GRESZTA I SAWICKI SP.K

DUNAUD CLARENC COMBLES & ASSOCIÉS

ELIG, ATTORNEYS-AT-LAW

GIANNI, ORIGONI, GRIPPO, CAPPELLI & PARTNERS

JUN HE LAW OFFICES

LEE & KO

MATHESON

NNOVATION LLP

SANTAMARINA Y STETA, SC

SIDLEY AUSTIN LLP

SIQUEIRA CASTRO – ADVOGADOS

SK CHAMBERS

SUBRAMANIAM & ASSOCIATES

URÍA MENÉNDEZ ABOGADOS, SLP

VIEIRA DE ALMEIDA & ASSOCIADOS, SP RL

WALDER WYSS LTD

WINHELLER RECHTSANWALTSGESELLSCHAFT MBH

CONTENTS

Chapter 14

IRELAND

Andreas Carney and Anne-Marie Bohan[1]

I OVERVIEW

The data protection regime in Ireland is governed by the Data Protection Acts 1988 and 2003 (DPA), which transposed European Directive 95/46/EC on data protection (Directive) into Irish law. In addition, there are numerous sector-specific regulations in areas such as employment,[2] electronic communications,[3] health data[4] and genetic data.[5] Ireland protects privacy and data protection rights fundamentally at a constitutional level in Articles 40.3.1, 40.3.2 and 40.5 of the Irish Constitution.[6] These rights are balanced against the freedom of expression protected in Article 40.6, and none is regarded as absolute.[7]

---

1 Andreas Carney and Anne-Marie Bohan are partners at Matheson.

2 SI No. 337 of 2014 – Data Protection Act 1988 (Commencement) Order 2014 and SI No. 338 of 2014 – Data Protection (Amendment) Act 2003 (Commencement) Order 2014. These make it unlawful for employers to require employees or applicants for employment to make an access request seeking copies of personal data that are then made available to employers or prospective employers. This provision also applies to any person who engages another person to provide a service.

3 SI No. 336/2011 – European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011 (E-Privacy Regulations). This deals with specific data protection issues relating to use of electronic communication devices, and particularly with direct marketing restrictions.

4 SI No. 82/1989 – Data Protection (Access Modification) (Health) Regulations, 1989. This outlines certain restrictions in the right of access relating to health data.

5 SI No. 687/2007 – Data Protection (Processing of Genetic Data) Regulations 2007. This outlines restrictions in respect of processing genetic data in relation to employment.

6 *Kennedy v. Ireland* [1987] IR 587; *Schrems v. Data Protection Commissioner* [2014] IEHC 310.

7 *Herrity v. Associated Newspapers (Ireland) Limited* [2008] IEHC 249; *X (an infant) v. Sunday Newspapers Ltd (trading as 'The Sunday World')* [2014] IEHC 696.

Ireland is a signatory to the 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, the Charter of Fundamental Rights of the European Union, and the European Convention on Human Rights and Fundamental Freedoms.

II THE YEAR IN REVIEW

It has been an eventful year for data protection in Ireland. The Court of Justice of the European Union (CJEU) struck down the US-EU Safe Harbor Framework in October 2015 following a reference from the Irish High Court. This decision precipitated the EU Commission and US Department of Commerce agreement in July of this year on a new framework for trans-Atlantic data transfers in the form of the EU–US Privacy Shield. While the Privacy Shield has its critics, it now offers another means of legitimately transferring personal data to the US.

The ability of US authorities to legitimately access personal data held in Ireland was tested in *Microsoft Corporation v. United States of America* in which US authorities sought to compel Microsoft to disclose e-mails located in their Dublin-based data centre as part of a narcotics investigation. While an initial decision ruled in favour of the US authorities, the Second US Circuit Court of Appeals overturned that decision and determined that the relevant US statute[8] being relied on by the authorities did not have extra-territorial effect and so did not empower them to require the production of personal data held in Ireland. This decision was largely welcomed, as it gave a level of certainty to those data controllers who strategically host personal data only within Ireland and other European Economic Area (EEA) Member States.

The year also saw the Office of the Data Protection Commissioner (ODPC) reopen an office in Dublin and also increase its headcount. The ODPC's annual report for 2015 shows a slight decrease in the number of complaints opened for investigation[9] and breach notifications made to the office, as well as highlighting prosecutions undertaken. According to the ODPC, the largest single category of complaints related to data subject access rights, which accounted for over 60 per cent of the total number of complaints in 2015.

III REGULATORY FRAMEWORK

i Privacy and data protection legislation and standards

As well as conferring rights on individuals, the DPA also place obligations on those who collect and process personal data. The DPA seek to regulate the collection, processing, keeping, use and disclosure of personal data. The DPA place responsibilities on both data controllers and, to a lesser extent, on data processors.

The E-Privacy Regulations provide for a number of protections and offences in relation to electronic communications, and, in particular, direct marketing via electronic means.

8 Electronic Communication Privacy Act 1986.

9 The ODPC Report notes 932 complaints that were opened for investigation in 2015 and 960 such complaints in 2014.

The key definitions under the DPA are as follows:

a personal data: data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller;

b sensitive personal data: personal data as to:
- the racial or ethnic origin, the political opinions or the religious or philosophical beliefs of the data subject;
- whether the data subject is a member of a trade union;
- the physical or mental health or condition or sexual life of the data subject;
- the commission or alleged commission of any offence by the data subject; or
- any proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings;

c processing: in relation to information or data, the performing of any operation or set of operations on the information or data, whether by automatic or other means, including:
- obtaining, recording or keeping the information or data;
- collecting, organising, storing, altering or adapting the information or data;
- retrieving, consulting or using the information or data;
- disclosing the information or data by transmitting, disseminating or otherwise making it available; or
- aligning, combining, blocking, erasing or destroying the information or data;

d data controller: a person who, either alone or with others, controls the contents and use of personal data;

e data processor: a person who processes personal data on behalf of a data controller, but this does not include an employee of a data controller who processes such data in the course of his or her employment; and

f data subject: an individual who is the subject of personal data.

ii General obligations for data handlers

Obligations of data controllers

The general obligations on data controllers are as follows:

Transparency

Data subjects must be provided with information relating to the processing of their data. This includes:

a the identity of the data controller or their representative, the data processor, or both;

b the purposes for which the data are intended to be processed; and

c any other information that is necessary, having regard to the specific circumstances in which data are to be processed, including but not limited to details of recipients or categories of recipients of the personal data and information as to the existence of the right of access and the right to rectify data.

Lawful basis for processing[10]

At least one of the following is required for personal data to be lawfully processed:

a consent of the data subject (specific, freely given, informed); or

b the processing is necessary:

- for the performance of a contract to which the data subject is a party;
- to take steps at the request of the data subject prior to entering into a contract;
- for compliance with a legal obligation to which the data controller is subject (other than an obligation imposed by contract);
- to prevent injury or other damage to the health of the data subject or serious loss or damage to property of the data subject, or to otherwise to protect his or her vital interests where the seeking of the consent of the data subject is likely to result in those interests being damaged;
- for compliance with a legal obligation, including the administration of justice; for the performance of a function conferred on a person by law; for the performance of a function of the government or a minister of the government; or for the performance of any other function of a public nature that is performed in the public interest; or
- for the purposes of legitimate interests pursued by the data controller (or a third party to whom the personal data are disclosed), provided that the rights of the data subject are not unduly prejudiced.

Purpose limitation

Personal data should only be obtained for one or more specified, explicit and legitimate purposes, and should not be further processed in a manner incompatible with those purposes.

Proportionality

Personal data collected must be adequate, relevant and not excessive in relation to the purposes for which they are collected or are further processed.

Retention

Personal data should not be kept for longer than is necessary for the purpose for which they were obtained. If the purpose for which the information was obtained has ceased and the personal information is no longer required, the data must be deleted or disposed of in a secure manner.

Rights of data subjects

The general rights of data subjects are as follows:

Access to data

Data subjects have the right to, free of charge, find out if an organisation or an individual holds information about them. This includes the right to be given a description of the personal data and to be told the purposes for which the data are held. A request for these data must be made in writing by the data subject and the individual must receive a reply within 21 days according to the DPA.

10 Sensitive personal data must also pass an additional legitimate basis for processing.

Data subjects have the right to obtain a copy, within 40 days of a request, of any personal data that relate to them that are held either on a computer or in a structured manual filing system, or that are intended for such a system.

A number of exceptions to the right of access exist under the DPA, including legal privilege, research data, data that comprise an opinion given in confidence (subject to certain limitations) or data used for the investigation of offences.

Correction and deletion

Data subjects have the right to request in writing to have their data either deleted or corrected where the data are not obtained lawfully or are inaccurate. The data controller or processor must respond within a reasonable amount of time and no later than 40 days after the request. There is no express right of a data subject to request the deletion of their information if they are being processed lawfully.

Objection to processing

Data subjects have the right to object to processing that is likely to cause damage or distress. This right applies to processing that is necessary for the purposes of legitimate interests pursued by the data controller to whom the personal data are or will be disclosed, or processing that is necessary for the performance of a task carried out in the public interest or in the exercise of official authority.

Objection to marketing

Data subjects have the right, by written request, to require a data controller to cease processing data for that purpose, and where they are only retained for that purpose, they have the right to have it erased. The data controller must do this within 40 days.

Under the E-Privacy Regulations, data subjects have the right to have their 'opt-out' preference recorded in the National Directory Database, which constitutes an objection to direct telephone marketing to them.

Complaint to relevant data protection authority or authorities

Data subjects have a right of complaint to the ODPC in relation to the treatment of their personal data. The ODPC must investigate such complaints unless it considers them to be 'frivolous or vexatious'.

Registration

It is obligatory for the following types of data controller to register with the ODPC if they hold personal data:

a government bodies and public authorities;
b banks, financial and credit institutions and insurance undertakings;
c data controllers whose business consists wholly or mainly of direct marketing;
d data controllers whose business consists wholly or mainly in providing credit references;
e data controllers whose business consists wholly or mainly in collecting debts;
f internet access providers, telecommunications networks and service providers;
g data controllers that process genetic data (as specifically defined in Section 41 of the Disability Act 2005); and
h health professionals processing personal data related to mental or physical health.

Data processors that process personal data on behalf of a data controller in any of the categories listed above must also register.

Exemptions

Generally, all data controllers and processors must register unless an exemption applies, either under Section 16(1)(a) or (b) of the DPA or under SI No. 657 of 2007. Under Section 16(1)(a) or (b) of the DPA, the following are excluded from registration:

a organisations that only carry out processing to keep, in accordance with law, a register that is intended to provide information to the public;

b organisations that only process manual data (unless the personal data have been prescribed by the ODPC as requiring registration); and

c organisations that are not established or conducted for profit, and that are processing personal data related to their members and supporters and their activities.

Additionally, pursuant to SI No. 657 of 2007, the Irish Minister for Justice and Equality has specified that the following data controllers and data processors are not required to register (provided they do not fall within any of the categories noted above in respect of which no exemption may be claimed):

a data controllers who only process employee data in the ordinary course of personnel administration and where the personal data are not processed other than where it is necessary to carry out such processing;

b solicitors and barristers;

c candidates for political office and elected representatives;

d schools, colleges, universities and similar educational institutions;

e normal commercial activity that by definition requires the processing of personal data (e.g., keeping details of customers and suppliers). This exemption does not include health professionals who process personal data relating to physical or mental health;

f companies that process personal data relating to past or existing shareholders, directors or other officers of a company for the purpose of compliance with the Companies Acts;

g data controllers who process personal data with a view to the publication of journalistic, literary or artistic material; and

h data controllers or data processors who operate under an approved data protection code of practice.

If an exemption does apply, however, it is limited only to the extent to which personal data are processed within the scope of that exemption.

The ODPC is obliged not to accept an application for registration from a data controller who keeps 'sensitive personal data' unless the ODPC is of the opinion that appropriate safeguards for the protection of the privacy of the data subjects concerned are being, and will continue to be, provided by the controller.

Where the ODPC refuses an application for registration, it must notify the applicant in writing and specify the reasons for the refusal. An appeal against such decision can be made to the circuit court.

iii Technological innovation and privacy law

Cloud computing

The ODPC has issued guidance on issues that arise from processing data in the cloud. The data controller must be satisfied that the cloud service provider will only process the data in accordance with the data controller's instructions. The data controller must also be satisfied that appropriate security measures have been taken by the cloud provider. These measures should cover continued access to the data by the data controller, prevention of unauthorised access to the data, adequate oversight of any sub-processors, procedures in the event of a data breach, and the right to remove or transfer data. The data controller's obligations in this respect can be satisfied by a detailed technical analysis incorporating an audit of the cloud provider or by third-party certification of the cloud provider to approved international standards.

A data controller must also assess the location of the data and must ensure that personal data are not transferred outside the EEA except in compliance with the DPA, for example, where the transfer is to an EU-approved country or pursuant to EU Model Contract Clauses or binding corporate rules (BCRs).

Finally, the data controller must ensure that a written contract is in place with the cloud provider.

Biometrics

The ODPC has published guidance on the use of biometric data both in the workplace and in schools, colleges and other educational institutions. The key issue in relation to biometric data is proportionality. The data controller must assess whether the biometric system is necessary and if there are less invasive alternatives available. Proportionality will depend on a number of factors, including the nature of the workplace or educational institution, the intended purpose of the system, efficiency and reliability. In the employment context, the ODPC's stated position is that consent is not generally satisfactory, as it can be argued that it is not freely given in view of the typically imbalanced nature of the employer–employee relationship. Employers should seek to rely on the 'legitimate interest' ground for processing biometric data, but must ensure the right balance is struck between their interests and the employees' rights. In the context of educational institutions, the ODPC recommends that consent is the only way of legitimising the processing of personal data. A clear and unambiguous right to opt out of the biometric system must be given. It is important that data subjects are made aware of the purpose of processing the biometric data.

The ODPC also highlights the importance of security in relation to biometric data, taking into account, in particular, the state of technological development, the cost of implementing security measures, the nature of the data being protected and the harm that might result through the unlawful processing of the data. The ODPC recommends that the personal data are deleted as soon as the employee or student permanently leaves.

The ODPC guidance recommends that employers and educational institutions conduct a privacy impact assessment prior to implementing a biometric system. This should take into account the need for such a system, the type of system required, the effect on data subjects and any less invasive options available.

iv Specific regulatory areas

Health data

The Data Protection (Access Modification) (Health) Regulations, 1989 provide that health data shall not be supplied to data subjects unless a health professional is first consulted, and that access to the data is not likely to cause serious harm to the mental or physical health of the data subject.

The ODPC has published guidance in the area of research in the health sector. The ODPC is of the opinion that anonymisation of patient data is the optimal position for health research. Where this is not possible, or access to patient identifiable information is required, health research should be conducted on the basis of informed and freely given explicit consent.

The Health Identifiers Act 2014 was enacted in July 2014 (although it has only been partially commenced). It establishes a unique health identifier for each patient and provides that this shall be personal data for the purposes of the DPA. The Act provides for limitations on accessing and processing health identifiers and offences for non-compliance.[11]

Electronic communications marketing

Under the E-Privacy Regulations, using publicly available communications services to make any unsolicited calls or send unsolicited e-mails for the purpose of direct marketing is restricted.

Direct marketing by fax

A fax may not be used for direct marketing purposes with an individual who is not a customer, unless the individual in question has previously consented to receiving marketing communications by fax.

Direct marketing by phone

In summary, to contact an individual by phone for the purposes of direct marketing, the individual must have given his or her consent to receiving direct marketing calls (or to the receipt of communications to his or her mobile phone, as the case may be). In certain cases, it will be necessary to consult the National Directory Database prior to placing calls for marketing purposes.

Direct marketing by e-mail or text message

To validly use these methods to direct market an individual, the individual concerned must have consented to the receipt of direct marketing communications via these methods.

The legislation provides for an exception whereby an existing customer may be taken to have consented on what is known as a 'soft opt-in' basis provided that certain requirements are met, and that the service or product that is being marketed is either the same or very similar to the product previously sold to that person.

11 Sections 21–25 of the Health Identifiers Act 2014.

IV INTERNATIONAL DATA TRANSFER

Personal data may not be transferred outside the EEA unless one of the following applies:

a the transfer is authorised by law;

b consent to the transfer is given by the data subject;

c the transfer is necessary for the performance of a contract to which the data subject is party;

d the transfer is necessary to conclude a contract with someone other than the data subject, where it is in the data subject's interests;

e the transfer is necessary for reasons of substantial public interest;

f the transfer is necessary for obtaining legal advice for legal proceedings;

g the transfer is necessary to prevent injury or damage to the data subject;

h the personal data to be transferred are an extract from a statutory public register established by law for public consultation; or

i the transfer is done through one of the mechanisms described in items (a), (b) or (c) below.

Even where one of the above elements exists, the ODPC retains the power to prohibit the transfer of personal data abroad to any country inside or outside the EEA.

In addition to the methods outlined above, the three methods by which Irish-based businesses typically transfer personal data outside the EEA are as follows:

a Use of 'model clauses' between the data controller and the person or organisation to whom they intend to pass the information to abroad. These are contractual clauses approved by the European Commission and that assure an adequate level of protection for the personal data. They do not usually require the approval of the ODPC; however, it can approve transfers based on contractual clauses that do not directly conform to the European model clauses.

b Transfer to a country that is on the European Commission 'adequate standard of protection' list, or US organisations that have agreed to be bound by the rules of the Privacy Shield agreement (essentially a streamlined version of EU data protection law).

c A further method that is less frequent is using BCRs, whereby personal data can be transferred to other companies within a group and based abroad, as long as certain legally enforceable rules exist within the group whereby they must give the data an adequate level of protection. This method is less frequently used because of the expense and time involved in having these rules approved by the ODPC (which is a requirement in order to be able to rely on them).

V COMPANY POLICIES AND PRACTICES

While the DPA do not provide specifically for the appointment of a data protection officer, when registering with the ODPC, both data controllers and data processors must give details of a 'compliance person' who will supervise the application of the DPA within the organisation in relation to personal data that are collected.

Operators of websites are required to have privacy statements in place. This is required by both the DPA, which require data controllers to supply certain information to data subjects, and the E-Privacy Regulations, which require certain information to be supplied

when information is stored or retrieved from a person's terminal equipment, including the use of cookies. The privacy policy must contain the identity of the data controller, the purpose for which personal data will be processed and the parties to whom the data will be disclosed. Data subjects must also be informed of their rights of access, rectification and erasure under the DPA. The ODPC also recommends including information such as the retention period and complaint resolution mechanism. The ODPC recommends placing a link to the privacy statement in a reasonably obvious position on each page of websites.

Although not strictly required, it is recommended that data controllers implement a security policy. The ODPC recommends that this include data collection and retention, access control, a 'movers, leavers and joiners' policy and an incident response plan.

VI DISCOVERY AND DISCLOSURE

Where data are sought for use in civil proceedings in a foreign country, Irish companies may be compelled under a subpoena from an Irish court to provide them. This happens frequently between EU countries, but it is also possible for a request from outside the EU to succeed.

In relation to requests from foreign law enforcement agencies, there is a legal framework in place that allows for the law enforcement agencies of foreign signatories of certain Hague Conventions to seek the disclosure of data held by Irish companies by the Irish police, who then issue a warrant for it. Where the request is made by the law enforcement agencies of countries that are not signatories, this is determined by the Department of Justice and Equality on a case-by-case basis. Generally, where proper undertakings are given by the agency making the request, it will be granted, and Irish companies will be compelled to disclose the data.

Part 3 of the Criminal Justice (Mutual Assistance) Act 2008 provides for various forms of mutual legal assistance to foreign law enforcement authorities. Part 3 relates to requests for mutual assistance between Ireland and other EU Member States for cooperation in the policing of telecommunications messages for the purposes of criminal investigations. The Minister for Justice can also now request that tapping of communications be undertaken in an EU Member State for an Irish-based criminal investigation, and also outlines how requests from other EU countries to Ireland for such interceptions should be processed.

The ODPC has not, as yet, issued official guidance in relation to foreign e-discovery requests or requests for disclosure from foreign law enforcement agencies. However, it is clear from statements by the government expressed prior to the most recent decision in the *Microsoft Warrant* case that the government advocates the use of existing mutual legal assistance treaties as a means of providing assistance in legal cases or law enforcement investigations.

VII PUBLIC AND PRIVATE ENFORCEMENT

i Enforcement agencies

The DPA confer specific rights on the ODPC and explicitly state that the ODPC shall be the supervisory authority in Ireland for the purpose of the Directive. The ODPC is responsible for ensuring that individuals' data protection rights are respected, and that those who are in control of or who process personal data carry out their responsibilities under the DPA.

Powers of the ODPC

Investigations

The ODPC must investigate any complaints that it receives from individuals in relation to the treatment of their personal data unless it considers them to be 'frivolous or vexatious'. The ODPC may also carry out investigations of its own accord. In practice, these usually take the form of scheduled privacy audits. However, it should be noted that the ODPC is not prevented from conducting 'dawn raid' types of audits if it decides to do so.

Power to obtain information

The ODPC has the power to require any person to provide it with whatever information it needs to carry out its functions. In carrying out this power in practice, the ODPC usually issues the person with an information notice in writing. It is an offence to fail to comply with such an information notice (without reasonable excuse), although there is a right to appeal any requirement specified in an information notice to the circuit court.

Power to enforce compliance with the DPA

The ODPC may require a data controller or data processor to take whatever steps it considers appropriate to comply with the terms of the DPA. In practice, this may involve blocking personal data from use for certain purposes, or erasing, correcting or supplementing the personal data. This power is exercised by the ODPC issuing an enforcement notice. It is an offence to fail to comply with an enforcement notice (although there is also a right of appeal against such a notice as there is for an information notice referred to above).

Power to prohibit overseas transfer of personal data

Under Section 11 of the DPA, the ODPC may prohibit the transfer of personal data from Ireland to an area outside of the EEA. In exercising this power, the ODPC must have regard to the need to facilitate international transfers of information.

Powers of 'authorised officers'

The ODPC has the power to nominate an authorised officer to enter and examine the premises of a data controller or data processor, to enable the ODPC to carry out its functions. An authorised officer has a number of powers, such as the power to enter the premises and inspect any data equipment there; to require the data controller or data processor to assist him or her in obtaining access to personal data; and to inspect and copy any information.

Enforcement

The ODPC may bring summary legal proceedings for an offence under the DPA. However, in contrast to the position in certain other jurisdictions such as the UK, the ODPC does not have the power to impose fixed monetary penalties.

Sanctions

While most of the penalties for offences under the DPA are civil in nature, breaches of data protection can also lead to criminal penalties. Summary legal proceedings for an offence under the DPA may be brought and prosecuted by the ODPC. Under the DPA, the maximum fine on summary conviction of such an offence is set at €3,000. On conviction on indictment (such a conviction in Ireland is usually reserved for more serious crime), the maximum penalty is a fine of €100,000.

The E-Privacy Regulations specify the sanctions for breaches of electronic marketing restrictions, which on summary conviction are a fine of up to €5,000 (per communication) or, on conviction on indictment, maximum fines ranging from €50,000 for a natural person to €250,000 for a body corporate.

The ODPC exercises its powers of enforcement on a regular basis, including through conducting inspections of organisations. During the course of 2015, 51 audits and inspections were carried out, and four entities were prosecuted for a total of 24 offences.

ii Recent enforcement cases

Excessive use of CCTV

In 2015, the ODPC addressed a number of cases where companies were using CCTV systems in a manner incompatible with the DPA and the ODPC's guidance. While no fines were imposed, the ODPC issued a number of case studies on the topic.

Marketing offences

A number of companies were prosecuted in 2015 for making unsolicited marketing calls and communications. In one case, a fine of €1,000 was imposed. Orders to make charitable donations ranging from €1,000 and up to €35,000 were also made (this approach is sometimes applied by courts as an alternative to levying a fine).

iii Private litigation

The DPA provide a statutory duty of care on the part of data controllers and processors in favour of data subjects. Thus, an individual can sue under the law of torts for a breach of any obligations under the DPA. The High Court has held that it is necessary for a data subject to show harm has resulted from a breach before any right to compensation will arise under this section.[12]

VIII CONSIDERATIONS FOR FOREIGN ORGANISATIONS

The DPA apply to data controllers in respect of the processing of personal data only if:

a the data controller is established in Ireland, and the data are processed in the context of that establishment; or

b the data controller is established neither in Ireland nor in any other state that is a contracting party to the EEA Agreement, but makes use of equipment in Ireland for processing the data otherwise than for the purpose of transit through the territory of Ireland. Such a data controller must, without prejudice to any legal proceedings that could be commenced against the data controller, designate a representative established in Ireland.

Each of the following shall be treated as established in Ireland:

a an individual who is normally resident in Ireland;

b a body incorporated under the laws of Ireland;

12 *Collins v. FBD Insurance plc* [2013] IEHC 137.

c a partnership or other unincorporated association formed under the laws of Ireland; and

d a person who does not fall within any of the above, but who maintains in Ireland an office, branch or agency through which he or she carries on any activity, or a regular practice.

IX CYBERSECURITY AND DATA BREACHES

The ODPC has published the Personal Data Security Breach Code of Practice (Code), which contains specific data security breach guidelines. This Code is non-binding in nature and does not apply to providers of publicly available electronic communications services in public communications networks in Ireland, which are subject to a mandatory reporting obligation under the E-Privacy Regulations.

The following guidelines are provided for in the Code:

a when a data breach occurs, the data controller should immediately consider whether to inform those who will be or have been impacted by the breach;

b if a breach is caused by a data processor, he or she should report it to the data controller as soon as he or she becomes aware of it;

c if the personal data was protected by technological measures (such as encryption) to such an extent that it would be unintelligible to any person who is not authorised to access it, then the data controller may decide that there is no risk to the personal data (and so no notification to the data subject is necessary);

d any incident that has put personal data at risk should be reported to the ODPC as soon as the data controller becomes aware of it. There are some limited exceptions to this provided for in the Code; for example, this is not required where:

- it affects fewer than 100 data subjects;
- the full facts of the incident have been reported without delay to those affected; and
- the breach does not involve sensitive personal data or personal data of a financial nature; and

e if the data controller is unclear about whether to report the incident, the Code advises that the incident should be reported to the ODPC. The Code advises that the controller should make contact with the ODPC within two working days of the incident occurring.

Once the ODPC is made aware of the circumstances surrounding a breach or a possible breach, it will decide whether a detailed report or an investigation (or both) is required.

Regarding cybersecurity, the government is in the process of implementing the National Cyber Security Strategy 2015–2017, which established the National Cyber Security Centre (NCSC) within the Department of Communications, Energy and Natural Resources and outlines the government's plan to address the risks posed by cybercrime to the digital economy and society. The objectives include:

a improving the resilience and robustness of the critical information infrastructure in crucial economic sectors;

b engaging with international partners to ensure that cyberspace remains open, secure, unitary and free;

c raising awareness of the responsibilities of businesses and individuals;

d ensuring that Ireland has a comprehensive and flexible legal and regulatory framework in place to combat cybercrime; and

e building capacity to engage in the emergency management of cyber incidents.

The NCSC aims to build on the work of the Computer Security Incident Response Team, which was established in 2011. The NCSC also intends to introduce legislation to transpose the EU Network and Information Security Directive (which was approved in 2016), the Budapest Convention on Cybercrime and Directive 2013/40/EU on attacks against information systems.

In September 2016, the Central Bank of Ireland, the regulator for financial institutions, published Cross Industry Guidance in respect of Information Technology and Cybersecurity, which relates to IT governance and risk management by regulated financial institutions in Ireland.

X OUTLOOK

The main feature of the short to mid-term Irish data protection landscape is the coming into effect of the General Data Protection Regulation (GDPR) in May 2018. With the final text of the GDPR now published, businesses are starting to familiarise themselves with the new regime that the GDPR will bring about. We are already seeing controllers and processors alike looking to implement aspects of the GDPR, notably privacy by design in new product and service offerings that they plan to roll out between now and May 2018.

The next phase of proceedings regarding data transfers has already started in the Irish courts. The ODPC is seeking a ruling from the CJEU on whether, following the *Schrems* decision, the transfer of data to the US based on model clauses is permissible. It is expected that the Irish courts' decision as to whether to make the referral will be issued in 2017.

In its most recent Annual Report, the ODPC lists its next priorities as including the expansion of its capacity and capability, and working closely with all stakeholders, and particularly with the Article 29 Working Party, towards the implementation of the GDPR.

Appendix 1

ABOUT THE AUTHORS

ANDREAS CARNEY

Matheson

Andreas Carney is a partner in the technology and commercial contracts group and a member of our data protection and privacy group. His core practice areas comprise outsourcing and other material service arrangements, data protection and IT. He works closely with clients from a diverse spread of industry sectors.

Andreas has advised extensively on IT infrastructure projects, including software and systems development, systems implementation and integration, systems support and maintenance, hardware supply, cloud services and co-location and other data centre arrangements. He also regularly works with clients in respect of their IT products and services, including social media, e-commerce and online consumer matters.

His data protection work is wide-ranging, and includes strategic compliance advice, outsourced data processing arrangements, assisting clients in achieving privacy by design in new products and services, handling cross-border data flows, managing data security breaches, dealing with data subject access requests and representing clients on regulatory issues arising with the Irish Data Protection Commissioner.

He regularly speaks and publishes on topics within his areas of expertise, and is a committee member of the Ireland Group of the Society of Computers and Law.

ANNE-MARIE BOHAN

Matheson

Anne-Marie Bohan is a partner in both the asset management and investment funds group and the FinTech group at Matheson, and is head of the outsourcing group. She advises on all aspects of outsourcing, information technology law and e-commerce law, with specific focus on the requirements of financial institutions and financial services providers in these areas.

Anne-Marie has extensive experience in drafting and negotiating contracts for the development, sale, purchase and licensing of hardware, software and IT systems for both suppliers and users of IT within the financial services industry and across a broad range of other industries. She has also acted in some of the largest value and most complex IT

and telecommunications systems and services outsourcing contracts, including advising on the largest and highest value financial services outsourcing to date, in Ireland. Anne-Marie's practice also includes advising a broad range of clients on data protection and privacy issues, including employee data protection issues.

Anne-Marie has written numerous articles on electronic commerce, internet, security issues, data protection and copyright law, and contributed the Ireland chapter to *Outsourcing Contracts – a Practical Guide* in 2009. She has also spoken at conferences on IT and electronic commerce issues, including electronic signatures, internet security, e-commerce and data protection. She also contributed the Irish chapter to *Getting the Deal Through: e-Commerce* in both 2002 and 2003, and has lectured as part of the Law Society of Ireland, diploma in electronic commerce. Anne-Marie was a member of the Matheson team that advised the Department of Public Enterprise on the drafting of the Electronic Commerce Act 2000.

MATHESON
70 Sir John Rogerson's Quay
Dublin 2
Ireland
Tel: +353 1 232 2000
Fax: +353 1 232 3333
andreas.carney @matheson.com
anne-marie.bohan@matheson.com
www.matheson.com