Data Protection & Privacy

Contributing editor
Wim Nauwelaerts

2018

GETTING THE DEAL THROUGH

GETTING THE DEAL THROUGH

Data Protection & Privacy 2018

Contributing editor
Wim Nauwelaerts
Hunton & Williams

Publisher
Gideon Roberton
gideon.roberton@lbresearch.com

Subscriptions
Sophie Pallier
subscriptions@gettingthedealthrough.com

Senior business development managers
Alan Lee
alan.lee@gettingthedealthrough.com

Adam Sargent
adam.sargent@gettingthedealthrough.com

Dan White
dan.white@gettingthedealthrough.com

Law Business Research

THE QUEEN'S AWARDS FOR ENTERPRISE: 2012

Published by
Law Business Research Ltd
87 Lancaster Road
London, W11 1QQ, UK
Tel: +44 20 3708 4199
Fax: +44 20 7229 6910

First published 2012
Sixth edition
ISSN 2051-1280

Printed and distributed by
Encompass Print Solutions
Tel: 0844 2480 112

CONTENTS

Introduction 5
Wim Nauwelaerts
Hunton & Williams

EU overview 9
Wim Nauwelaerts and Claire François
Hunton & Williams

Safe Harbor and the Privacy Shield 12
Aaron P Simpson
Hunton & Williams

Australia 14
Alex Hutchens, Jeremy Perier and Eliza Humble
McCullough Robertson

Austria 20
Rainer Knyrim
Knyrim Trieb Attorneys at Law

Belgium 28
Wim Nauwelaerts and David Dumont
Hunton & Williams

Brazil 36
Ricardo Barretto Ferreira and Paulo Brancher
Azevedo Sette Advogados

Chile 42
Claudio Magliona, Nicolás Yuraszeck and Carlos Araya
García Magliona & Cía Abogados

China 47
Vincent Zhang and John Bolin
Jincheng Tongda & Neal

France 55
Benjamin May and Clémentine Richard
Aramis

Germany 63
Peter Huppertz
Hoffmann Liebs Fritsch & Partner

India 69
Stephen Mathias and Naqeeb Ahmed Kazia
Kochhar & Co

Ireland 75
Anne-Marie Bohan
Matheson

Italy 84
Rocco Panetta and Federico Sartore
Panetta & Associati

Japan 93
Akemi Suzuki and Tomohiro Sekiguchi
Nagashima Ohno & Tsunematsu

Lithuania 99
Laimonas Marcinkevičius
Juridicon Law Firm

Luxembourg 106
Marielle Stevenot and Audrey Rustichelli
MNKS

Mexico 113
Gustavo A Alcocer and Abraham Díaz Arceo
Olivares

Poland 119
Arwid Mednis and Gerard Karp
Wierzbowski Eversheds Sutherland

Portugal 126
Helena Tapp Barroso, João Alfredo Afonso and Tiago Félix da Costa
Morais Leitão, Galvão Teles, Soares da Silva & Associados

Russia 133
Ksenia Andreeva, Anastasia Dergacheva, Vasilisa Strizh and Brian Zimbler
Morgan, Lewis & Bockius LLP

Serbia 140
Bogdan Ivanišević and Milica Basta
BDK Advokati

Singapore 145
Lim Chong Kin and Charmian Aw
Drew & Napier LLC

South Africa 159
Danie Strachan and André Visser
Adams & Adams

Spain 168
Alejandro Padín, Daniel Caccamo, Katiana Otero, Francisco Marín and Álvaro Blanco
J&A Garrigues

Sweden 174
Henrik Nilsson
Wesslau Söderqvist Advokatbyrå

Switzerland 181
Lukas Morscher and Leo Rusterholz
Lenz & Staehelin

Turkey 189
Ozan Karaduman and Bentley James Yaffe
Gün + Partners

United Kingdom 195
Aaron P Simpson
Hunton & Williams

United States 202
Lisa J Sotto and Aaron P Simpson
Hunton & Williams

Ireland

Anne-Marie Bohan
Matheson

Law and the regulatory authority

1 Legislative framework

Summarise the legislative framework for the protection of personally identifiable information (PII). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments on privacy or data protection?

The data protection regime in Ireland is currently governed by the Data Protection Acts 1988 and 2003 (collectively, the DPA). The DPA transposes European Directive 95/46/EC on data protection into Irish law.

As well as conferring rights on individuals, the DPA also places obligations on those who collect and process personal data. 'Personal data' is defined as any information relating to a living individual identifiable from that data (or from a combination of that data and other information of which the data controller is in possession or is likely to come into possession).

The DPA seeks to regulate the collection, processing, keeping, use and disclosure of personal data that is processed automatically or, in certain circumstances, manually.

The DPA places responsibilities on both 'data controllers' and 'data processors'. A data controller is a person who controls the use and contents of personal data, while a data processor refers to a person who processes personal data on behalf of a data controller.

The European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011 (e-Privacy Regulations) deal with specific data protection issues relating to use of electronic communication devices, and particularly with direct marketing restrictions.

The General Data Protection Regulation (Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data) (GDPR) will have direct effect in Ireland from 25 May 2018, and will largely replace the DPA. The GDPR is intended to harmonise further the data protection regimes within the EU, and will introduce a number of changes into the data protection regime, including:

- increased scope to include focus on the residence of the data subject;
- lead authority supervision;
- privacy by design and by default;
- additional focus on processers and processing arrangements;
- improved individual rights;
- mandatory breach reporting; and
- significantly increased sanctions for breach.

A preliminary draft of the proposed national legislation dealing with member state derogations and options under the GDPR was published in May 2017.

Ireland is a signatory to both the 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data and the European Convention on Human Rights and Fundamental Freedoms. The Charter of Fundamental Rights of the European Union also has application in Ireland.

In addition, the Irish Constitution, Bunreacht na hEireann, has been held by the Irish courts to encapsulate an unenumerated right to privacy.

2 Data protection authority

Which authority is responsible for overseeing the data protection law? Describe the investigative powers of the authority.

The DPA confers specific rights on the Office of the Data Protection Commissioner (ODPC) and explicitly states 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. The powers of the ODPC are as follows.

Investigations
Under section 10 of the DPA, 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 (as to which, see note on the powers of 'authorised officers' under section 24 of the DPA, below).

Power to obtain information
Under section 12 of the DPA, 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 under section 26 of the DPA.

Power to enforce compliance with the Act
Under section 10 of 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.

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 European Economic Area (EEA). In exercising this power, the ODPC must have regard to the need to facilitate international transfers of information.

The powers of authorised officers
Under section 24 of the DPA, 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 or the e-Privacy Regulations. The ODPC does not have the power to impose fixed monetary penalties, unlike the Information Commissioner in the UK.

The enforcement regime is likely to change significantly following the coming into force of the GDPR, not least in that it is anticipated that the ODPC will be replaced by the Data Protection Commission (Commission), which will assume the ongoing work of the ODPC. It is currently proposed that there may be up to three Data Protection Commissioners appointed to the Commission, which is likely to qualify as the lead authority for a significant number of large social media companies and other controllers of large volumes of personal data with headquarters in Ireland. In addition, for the first time the Commission will have the authority to impose administrative fines directly on controllers and processors (subject to a right of appeal to the courts).

3 Breaches of data protection

Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?

Yes. 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 to maximum fines ranging from €50,000 for a natural person to €250,000 for a body corporate.

Under the GDPR, sanctions for breach will increase substantially, and will range from up to €10 million or 2 per cent of worldwide turnover to up to €20 million or 4 per cent of worldwide turnover, depending on the breach.

Scope

4 Exempt sectors and institutions

Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?

The DPA applies to all sectors and all types of organisation. Some areas of activity are, however, outside the scope of the DPA. Under section 1(4) the DPA does not apply if the personal data:

- is or at any time was kept for the purposes of safeguarding Ireland's security;
- consists of information that the person keeping the personal data is required by law to make available to the public; or
- is kept by an individual for his or her personal, family or household affairs, or for solely recreational purposes.

Processing may also be exempt in certain circumstances. Processing will fall outside the scope of the GDPR if it is:

- in the course of an activity outside the scope of EU law;
- for purely personal or household activities;
- by competent authorities in connection with crime or public security; or
- by member states in connection with justice and social security (Chapter 2 Title 5 TFEU).

5 Communications, marketing and surveillance laws

Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals? If not, list other relevant laws in this regard.

Electronic marketing is addressed in the e-Privacy Regulations. The e-Privacy Regulations also prohibit the listening, tapping, storage or other interception or surveillance of communications and related traffic data without consent. Further restrictions are found in the Postal and Telecommunications Services Act 1983, the Interception of Postal Packets and Telecommunications (Regulation) Act 1993 and the Criminal Justice (Surveillance) Act 2009.

The Criminal Justice (Offences Relating to Information Systems) Bill 2016 (the Bill) is currently working its way through the legislative process in Ireland, and is designed to implement certain provisions of Directive 2013/40/EU (the Cyber-Crime Directive). The Bill will introduce a specific offence addressing intercepting and transmission of data without lawful authority, will introduce more stringent penalties and will make misuse of personal data an aggravating factor in relation to sentencing.

6 Other laws

Identify any further laws or regulations that provide specific data protection rules for related areas.

Any processing of personal data, including in the context of e-health records, social media and financial or credit information, must comply with the principles as set out in the DPA, as well as any requirements of sectoral regulators. The Central Bank of Ireland, which authorises and regulates financial institutions and service providers in Ireland, requires high standards of data security generally, including compliance with the DPA. The Central Bank has had an increasing focus on cybersecurity risks in recent years, and published cross-industry guidance in respect of information technology and cybersecurity risks, which includes data security guidance, in September 2016. Processing of genetic data is subject to additional restrictions in the Disability Act 2005 and the Data Protection (Processing of Genetic Data) Regulations 2007. Collection and use of personal public service numbers is also subject to restrictions.

Further data protection requirements, including in relation to phone, email, internet and SMS use in connection with unsolicited communications, are set out in the e-Privacy Regulations, which implement Directive 2002/58/EC (the e-Privacy Directive), and are of particular importance to providers of publicly available electronic communications networks and services, as well as businesses engaged in direct marketing. The European Commission has published a proposal for an e-Privacy Regulation, which if enacted would replace the Irish e-Privacy Regulations with potentially more restrictive requirements.

7 PII formats

What forms of PII are covered by the law?

Personal data includes any automated and manual data (ie, data that is recorded as part of a structured filing system) relating to a living individual who can be identified from the personal data in question (or from a combination of that data and other information of which the data controller is in possession or is likely to come into possession).

Under the GDPR, the definition of personal data will be clarified and will cover any information relating to an identified or identifiable person, with an identifiable person being one who can be identified directly or indirectly, in particular by reference to an identifier such as, for example, a name, ID number, location data, online identifier, etc.

8 Extraterritoriality

Is the reach of the law limited to PII owners and processors of PII established or operating in the jurisdiction?

Unitl 25 May 2018, yes. The DPA applies to data controllers in respect of the processing of personal data only if:

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

- the data controller is established neither in Ireland nor in any other state that is a contracting party to the European Economic Area (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:
- an individual who is normally resident in Ireland;
- a body incorporated under the laws of Ireland;
- a partnership or other unincorporated association formed under the laws of Ireland; and
- 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.

The GDPR will extend the scope of application of EU data protection rules, focusing as it does on the location of the data subject in the EU, rather than simply the place of establishment of the data controller. The GDPR will have application to non-EU controllers who offer goods and services to individuals in the EU or who monitor the behaviour of individuals as far as the behaviour takes place in the EU.

9 Covered uses of PII

Is all processing or use of PII covered? Is a distinction made between those who control or own PII and those who provide PII processing services to owners?

The DPA applies to individuals or organisations established in Ireland that collect, store or process personal data on any form of computer system and in certain forms of structured manual filing systems. There are no exclusions from scope, save as described in response to question 4.

Under the DPA, a distinction is made between those who control personal data and those who process it. A 'data controller' is one who (either alone or with others), controls the use and contents of personal data, while a 'data processor' refers to a person who processes data on behalf of a data controller. Generally, those who provide services to owners will be data processors. Employees who process personal data in the course of their employment are not included in these definitions.

Data controllers are subject to the full scope of the DPA. Data processors have fewer direct statutory obligations, but importantly are subject to the data security principle, and owe a statutory duty of care to data subjects.

The GDPR retains the distinction between data controllers and data processors, but significantly increases the focus on processing activities. Data processors will have additional obligations once the GDPR comes into force.

Legitimate processing of PII

10 Legitimate processing – grounds

Does the law require that the holding of PII be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?

Yes. Under section 2A(1)(a) of the DPA, consent of the individual is a legitimate ground for processing personal data. Data controllers can also process personal data (excluding sensitive personal data – see question 11) without the data subject's consent if it is necessary for one of the following reasons:
- for the performance of a contract to which the data subject is a party (including steps taken at the request of the data subject before entering into the contract);
- for compliance with a legal obligation, including:
  - the administration of justice;
  - the performance of a function conferred on a person by law;
  - the performance of a function of the government or a minister of the government; and
  - the performance of any other function of a public nature, which is performed in the public interest;
- to prevent injury or other damage to the health, or serious loss or damage to the property, of the data subject;
- to protect the vital interests of the data subject where the seeking of the consent of the data subject is likely to result in those interests being damaged; and
- for the purpose of the legitimate interests pursued by a data controller, except if processing is unwarranted in any particular case by reason of prejudice to the fundamental rights and freedoms or legitimate interests of the data subject.

Section 8 of the DPA details circumstances in which the restrictions in the DPA (including consent) do not apply (eg, if the processing of personal data is required for the investigation of an offence, or by order of a court or under an enactment or rule of law).

The legitimate processing grounds in the DPA apply in addition to the data protection (or data quality) principles (see questions 12 and 15 to 19).

The legitimate processing grounds in the DPA are narrowly interpreted.

The GDPR contains broadly similar provisions, but expands on the concept of consent, imposing on the data controller a requirement to demonstrate consent has been obtained by a statement or clear affirmative action. It is expected that the legitimate processing grounds under the GDPR will also be narrowly construed.

11 Legitimate processing – types of PII

Does the law impose more stringent rules for specific types of PII?

Yes. In addition to the requirements outlined in question 10, section 2B of the DPA imposes the following additional obligations on the data controller for the processing of sensitive personal data:
- the data subject, or a parent or legal guardian (where applicable), must give explicit consent, having been informed of the purpose of the processing; and
- if consent is not obtained, a data controller can still process the sensitive personal data if the processing is necessary for:
  - exercising or performing any right or obligation that is conferred or imposed by law on the data controller in connection with employment;
  - preventing injury or other damage to the health of the data subject or another person, or serious loss in respect of, or damage to, property or otherwise to protect the vital interests of the data subject or of another person in a case where consent cannot be given or the data controller cannot reasonably be expected to obtain such consent;
  - preventing injury to, or damage to the health of, another person, or serious loss in respect of, or damage to, the property of another person, in a case where such consent has been unreasonably withheld;
  - carrying out the processing for a not-for-profit organisation in respect of its members or other persons in regular contact with the organisation;
  - processing information that has already been made public as a result of steps deliberately taken by the data subject;
  - obtaining legal advice, obtaining information in connection with legal proceedings, or where processing is necessary for the purposes of establishing, exercising or defending legal rights;
  - obtaining personal data for medical purposes;
  - processing by a political party or candidate for election in the context of an election;
  - assessing or paying a tax liability; or
  - administering a social welfare scheme.

For the purposes of the DPA, sensitive personal data includes information in relation to physical or mental health, racial or ethnic origin, political opinions, religious or philosophical beliefs, the commission or alleged commission of any offence, proceedings for an offence committed or alleged to have been committed, the disposal of such proceedings, or the sentence of any court in such proceedings.

Under the GDPR, a broadly similar approach is taken to the processing of sensitive (recharacterised as 'special') categories of personal data. However, data relating to criminal convictions and offences will

be treated slightly differently, and may only be processed by official authorities or if authorised by law providing for appropriate safeguards for individual rights and freedoms.

Data handling responsibilities of owners of PII

12 Notification

Does the law require owners of PII to notify individuals whose PII they hold? What must the notice contain and when must it be provided?

Data subjects need to be notified of certain matters at the point of collection of personal data. Personal data is not considered to be processed fairly, under the data protection principles, unless, in the case of personal data obtained directly from the data subject, the data controller ensures that the data subject has been provided with at least the following information at the point of collection:

- the name of the data controller;
- the purpose for collecting the personal data;
- the identity of any representative nominated for the purposes of the DPA;
- the persons or categories of persons to whom the personal data may be disclosed;
- whether replies to questions asked are obligatory and if so, the consequences of not providing replies to those questions;
- the data subject's right of access to their personal data;
- the data subject's right to rectify their data if inaccurate or processed unfairly; and
- any other information which is necessary so that processing may be fair, and to ensure the data subject has all necessary information to be aware as to how their personal data will be processed.

Many of these points are typically dealt with in a data controller's terms and conditions or privacy policy.

Where information is indirectly obtained, the data subject must also be informed of the categories of data and the name of the original data controller.

The GDPR places greater emphasis on transparency, and will require more specific disclosures to data subjects, in intelligible and clearly accessible form, using clear and plain language.

13 Exemption from notification

When is notice not required?

There is an exemption from notification where, in particular for processing for statistical purposes or for the purposes of historical or scientific research, the provision of the information specified therein proves impossible or would involve a disproportionate effort, or in any case where the processing of the information contained or to be contained in the personal data by the data controller is necessary for compliance with a legal obligation to which the data controller is subject other than an obligation imposed by contract.

Under the GDPR, the notice requirements will apply unless the data subject already has the information, or in the case of indirectly obtained personal data, the provision of the information would be impossible or involve disproportionate effort, the obtaining and disclosure of the personal data is expressly set out in law, or the personal data is subject to an obligation of professional secrecy.

14 Control of use

Must owners of PII offer individuals any degree of choice or control over the use of their information? In which circumstances?

Yes. An individual can have his or her personal data rectified, blocked or deleted if he or she requests this in writing. The relevant information must be provided as soon as possible following a data subject access request, and no later than 40 days following compliance with section 4 of the DPA by the individual requesting the information.

In addition, an individual has the right to object to processing that is likely to cause damage or distress. This right applies to processing that is necessary for either:

- the performance of a task carried out in the public interest or in the exercise of official authority; or
- the purposes of the legitimate interests pursued by the data controller to whom the personal data is, or will be, disclosed, unless those interests are overridden by the interests of the data subject in relation to fundamental rights and freedoms and, in particular, his or her right to privacy.

Objections to current or future processing can be submitted in writing to the data controller.

Furthermore, unless a data subject consents, a decision that has a legal or other significant effect on him or her cannot be based solely on the processing by automatic means of his or her personal data, which is intended to evaluate certain personal matters relating to him or her (for example, his or her performance at work, creditworthiness, reliability and conduct).

Individuals also have the right to control the extent to which they receive marketing (including, in particular, by electronic means), and to be removed from marketing databases.

Under the GDPR, in addition to the rights of access, rectification, erasure (ie the right to be forgotten) and restriction of processing, data subjects will in certain circumstances have the right to object to processing and to data portability. None of the rights under the GDPR is an absolute right, and each may be made subject to certain restrictions.

15 Data accuracy

Does the law impose standards in relation to the quality, currency and accuracy of PII?

Yes. Data controllers must keep the personal data safe and secure, accurate, complete and, where necessary, up to date.

16 Amount and duration of data holding

Does the law restrict the amount of PII that may be held or the length of time it may be held?

Yes. Data controllers must ensure that personal data is adequate, relevant and not excessive and retain it for no longer than is necessary for the specified purpose or purposes for which it was obtained.

17 Finality principle

Are the purposes for which PII can be used by owners restricted? Has the 'finality principle' been adopted?

Yes. The DPA specifies that data controllers must obtain personal data only for specified, explicit and legitimate purposes, and process the personal data only in ways compatible with the purposes for which it was obtained by the data controller initially.

18 Use for new purposes

If the finality principle has been adopted, how far does the law allow for PII to be used for new purposes? Are there exceptions or exclusions from the finality principle?

The finality principle does not apply to personal data kept for statistical, research or other scientific purposes, and the keeping of which complies with such requirements as may be prescribed for the purpose of safeguarding the fundamental rights and freedoms of data subjects if the personal data is not used in such a way that damage or distress is caused to any data subject.

Section 8 of the DPA details circumstances in which the restrictions in the DPA (including the finality principle) do not apply. This includes where the data subject has requested or consented to the new purpose.

Under the GDPR, processing for purposes other than those for which the personal data was originally collected should only be allowed where the further processing is compatible with the original purposes.

Security

19 Security obligations

What security obligations are imposed on PII owners and service providers that process PII on their behalf?

According to section 2 of the DPA, data controllers must have 'appropriate security measures' in place. Data processors are subject to the same data security principle, which must also be included in processing

contracts. These measures adopted must be appropriate to the nature of the data concerned and must provide a level of security that is appropriate to the potential level of harm that could result from any unauthorised or unlawful processing or from any loss or destruction of personal data. Data controllers and data processors must also ensure that their employees comply with any and all security measures in place.

The GDPR adopts a 'privacy by design and by default' approach to data protection, putting security at the core of data protection obligations, and will impose on the data controller the need to demonstrate compliance with the GDPR. Both data controllers and data processors will be subject under the GDPR to obligations relating to the security of personal data.

20 Notification of data breach

Does the law include (general and/or sector-specific) obligations to notify the supervisory authority and individuals of data breaches? If breach notification is not required by law, is it recommended by the supervisory authority?

The ODPC has published the 'Personal Data Security Breach Code of Practice' (the 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:

- 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;
- 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;
- 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 necessary);
- any incident which 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
- if the data controller is unclear about whether or not 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 becoming aware of the incident.

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.

Breach notification will become mandatory once the GDPR comes into effect. Controllers will be obliged to notify the Commission where there has been a breach unless the breach is unlikely to result in a risk to data subjects. Data subjects must be informed of a breach without undue delay where the breach is likely to result in a high risk to them.

Internal controls

21 Data protection officer

Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities?

No. While the DPA does 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 is collected.

Under the GDPR, it will be compulsory to appoint a data protection officer in certain circumstances (for example, public authorities and bodies must appoint them, as well as organisations whose core activities consist of the systematic monitoring of data subjects on a large scale or the large-scale processing of special categories of personal data).

22 Record keeping

Are owners of PII required to maintain any internal records or establish internal processes or documentation?

No specific rules relating to internal records are provided for in the DPA. This will change once the GDPR comes into effect. The GDPR will increase focus on processors and processing, and will mandate records of processing activities.

Registration and notification

23 Registration

Are PII owners and/or processors of PII required to register with the supervisory authority? Are there any exemptions?

Yes. The specific requirements relating to registration are dealt with under sections 16 to 20 of the DPA and secondary legislation.

It is mandatory for certain types of data processors and data controllers to register with the ODPC if they hold personal data in automated form and have a legal presence in Ireland, or use equipment located here.

It is obligatory for the following parties to register with the ODPC and no exemption may be claimed on their behalf:

- government bodies or public authorities;
- banks, financial or credit institutions and insurance undertakings;
- data controllers whose business consists wholly or mainly of direct marketing;
- data controllers whose business consists wholly or mainly in providing credit references;
- data controllers whose business consists wholly or mainly in collecting debts;
- internet access providers, telecommunications networks or service providers;
- data controllers that process genetic data (as specifically defined in section 41 of the Disability Act 2005);
- health professionals processing personal data related to mental or physical health; and
- data processors that process personal data on behalf of a data controller in any of the categories listed above.

Exemptions

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

- organisations that only carry out processing to keep, in accordance with law, a register that is intended to provide information to the public;
- organisations that only process manual data (unless the personal data had been prescribed by the ODPC as requiring registration); and
- 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 in respect of which no exemption may be claimed):

- data controllers who only process employee data in the ordinary course of personnel administration and where the personal data is not processed other than where it is necessary to carry out such processing;
- solicitors and barristers;
- candidates for political office and elected representatives;
- schools, colleges, universities and similar educational institutions;
- data controllers (other than health professionals who process data relating to the physical or mental health of a data subject

for medical purposes) who process personal data relating to past, existing or prospective customers or suppliers for the purposes of:
  - advertising or marketing the data controller's business, activity, goods or services;
  - keeping accounts relating to any business or other activity carried on by the data controller;
  - deciding whether to accept any person as a customer or supplier;
  - keeping records of purchases, sales or other transactions for the purpose of ensuring that requisite payments and deliveries are made or services provided by or to the data controller in respect of those transactions;
  - making financial or management forecasts to assist in the conduct of business or other activity carried on by the data controller; or
  - performing a contract with the data subject where the personal data is not processed other than where it is necessary to carry out such processing for any of the purposes set out above;
- companies who process personal data relating to past or existing shareholders, directors or other officers of a company for the purpose of compliance with the Companies Act 2014;
- data controllers who process personal data with a view to the publication of journalistic, literary or artistic material; and
- data controllers or data processors who operate under a data protection code of practice.

If an exemption does apply, however, it is limited only to the extent to which personal data is 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.

The registration process will no longer apply once the GDPR comes into effect.

24 Formalities

What are the formalities for registration?

Under section 17 of the DPA, an application for registration as a data processor or data controller must be filed with the ODPC. An application to register as a data controller or data processor with the ODPC can be made using an online system through the ODPC's website. Alternatively, an application form can be downloaded from the website and sent via postal service.

Fees

A fee is also required and can be paid online or by cheque. The fee for registration varies significantly depending on the number of employees (there is also some variance between postal application fees and online application fees).

For applicants with 26 employees or more (inclusive), the online application fee is €430, while the postal application fee is €480.

For applicants with between six and 25 employees (inclusive), the online application fee is €90 and the postal application fee is €100.

Finally, for applicants with between zero and five employees (inclusive), the online application fee is €35, while the postal application fee is €40.

According to section 17(1)(a) it is for the ODPC to prescribe the information he or she requires for registration.

The DPA also provides that, where a data controller intends to keep personal data for two or more related purposes, he or she is only required to make one application in respect of those purposes. If, on the other hand, he or she intends to keep personal data for two or more unrelated purposes, then he or she will be required to make separate applications in respect of each of those purposes and entries will be made in the register in accordance with each such application.

Information to be included

There are separate registration forms available on the ODPC's website for the registration of either a data processor or a data controller. A data controller must provide a general statement of the nature of their business, trade or profession and of any additional purposes for which they keep personal data. Each application of personal data relating to the purposes that the controller lists along with the types of personal data (such as name, email, date of birth) must also be listed or described. For each of these applications listed, a list of the persons or bodies to whom the personal data may be disclosed must also be given.

If any transfers are made (or intended to be made) to a country outside of the EU member states, a list of these countries along with a description of the data to be transferred and the purpose of the transfer must be provided.

Information on any sensitive personal data that is kept by the controller must also be given (such as data relating to race, religion, sex life, criminal convictions).

For data processors, a name, address and details on the nature of the data being processed must also be provided.

Finally, for both processors and controllers details of a 'compliance person' who will supervise the application of the DPA within the organisation in relation to personal data that are collected must be given.

Validity and renewal

The registration is valid for one year (from the date the ODPC receives a correctly completed application form and fee). Unless renewed after a period of one year, the entry on the register will expire. A letter is sent as a reminder approximately three weeks prior to the renewal date. Amendments may be made upon renewal free of charge. However, there is a fee for amendments made during the year-long period.

The registration process will no longer apply once the GDPR comes into effect.

25 Penalties

What are the penalties for a PII owner or processor of PII for failure to make or maintain an entry on the register?

Once registered, the applicant must keep their registry entry up to date. In addition, the ODPC must be informed if any part of the entry becomes incomplete or inaccurate as processing personal data without an accurate and complete entry on the register can incur a criminal penalty. It is an offence for a data controller or data processor who is required to be registered but is not registered, to process personal data.

Under section 19(1) of the DPA, a data controller to whom section 16 applies is not permitted to keep personal data unless there is an entry on the register in respect of him or her.

26 Refusal of registration

On what grounds may the supervisory authority refuse to allow an entry on the register?

Under section 17(2) of the DPA, the ODPC may refuse an application for registration by means of a Registration Refusal Notice if he or she is of the opinion that the particulars proposed for inclusion in an entry in the Register are insufficient or any other information required by him or her either has not been furnished or is insufficient, or the person applying for registration is likely to contravene any of the provisions of the DPA.

Under section 17(3) the ODPC may not accept an application for registration from a data controller who keeps sensitive personal data unless he or she is of the opinion that appropriate safeguards for the protection of the privacy of the data subjects are being, and will continue to be, provided by him or her.

27 Public access

Is the register publicly available? How can it be accessed?

Yes, under section 16 of the DPA the register is available to the public for inspection and can be accessed via a link on the ODPC's website. According to section 16 of the DPA, a member of the public may inspect the register free of charge at all reasonable times and may take copies of or extracts from entries in the register. Upon payment of a fee, a

member of the public may also obtain from the ODPC a certified copy or extract from an entry in the register (section 16(3)).

28 Effect of registration

Does an entry on the register have any specific legal effect?

Yes. Section 19 of the DPA covers the 'effect of registration' and may be summarised as follows.

A data controller to whom section 16 of the DPA applies shall not keep personal data unless there is for the time being an entry in the register in respect of him or her. A data controller in respect of whom there is an entry in the register shall not:

- keep personal data of any description other than that specified in the entry;
- keep or use personal data for a purpose other than the purpose or purposes described in the entry;
- if the source from which such personal data (and any information intended for inclusion in such personal data) are obtained is required to be described in the entry, obtain such personal data or information from a source that is not so described;
- disclose such personal data to a person who is not described in the entry (other than a person to whom a disclosure of such data may be made in the circumstances specified in section 8 of the DPA); or
- directly or indirectly transfer such personal data to a place outside Ireland other than one named or described in the entry.

Transfer and disclosure of PII

29 Transfer of PII

How does the law regulate the transfer of PII to entities that provide outsourced processing services?

Under the DPA, where a third party processes personal data on behalf of the data controller, the data controller must ensure that any and all of the processing that is carried out by the processor is subject to a contract between the controller and the processor. The contract must, among other things, contain the security conditions attached to the processing of personal data, and should also specify whether the personal data is to be deleted or returned upon termination of the contract. The data processor must make sure that no unauthorised person has access to the personal data and that it is secure from loss, damage or theft.

The requirements applicable to data processors and the mandatory contractual provisions to be included in processing contracts will increase under the GDPR.

30 Restrictions on disclosure

Describe any specific restrictions on the disclosure of PII to other recipients.

Under the DPA, data controllers must prevent unauthorised access to or disclosure of the personal data. Security measures should be in place to ensure the above requirements are met. The approach under the GDPR is substantially the same.

The e-Privacy Regulations set out security measures for electronically stored data applicable to providers of publicly available electronic communications networks and services.

31 Cross-border transfer

Is the transfer of PII outside the jurisdiction restricted?

Yes. The general rule in Ireland is that personal data cannot be transferred to third countries unless the country ensures an adequate level of data protection.

Generally transfers of personal data from Ireland to other EEA member states are permitted without the need for further approval. The transfer of personal data to a country outside the EEA, however, is prohibited, unless that country ensures an adequate level of protection for the privacy and rights of data subjects.

The ODPC can prevent transfers of personal data to other countries where it considers that the data protection rules are likely to be contravened. The ODPC does this by issuing a 'prohibition notice' to the data controller or data processor in question, which prevents any transfer outside of Ireland.

Certain countries are subject to the European Commission's findings of adequacy in relation to their data protection laws (for certain types of personal data and subject to the fulfilment of some preconditions). These countries are: Canada, Israel, Switzerland, Uruguay, the Isle of Man, Argentina, Guernsey, the Faroe Islands, Andorra and New Zealand.

If the country to which a data controller or data processor wishes to transfer is not on the approved lists above then transfer may nonetheless be possible in the following circumstances:

- where the ODPC authorises such (see following question);
- where the data subject has given clear consent to such;
- where the transfer is required or authorised by law;
- if the transfer is necessary for performing contractual obligations between the data controller and the data subject;
- if the transfer is necessary for the purpose of obtaining legal advice;
- to prevent injury or damage to a data subject's health;
- for reasons of substantial public interest; and
- to prevent serious loss to the property of the data subject.

In practice these criteria are very narrowly construed.

Other methods of enabling the transfer of personal data include using binding corporate rules (BCR), which are intra-group rules designed to allow multinational companies to transfer personal data from the EEA to affiliates located outside the EEA in compliance with Directive 95/46/EC. The BCRs are submitted to the ODPC for approval. The EU standard contractual clauses (SCCs) may also be used. These are clauses that the European Commission has approved as providing an adequate level of protection for transferred data. Approval of a data transfer agreement using the SCCs does not require approval of the ODPC. The ODPC also has the power to approve contractual clauses that do not necessarily conform to the SCCs, but in practice is only likely do so where there is a strong justification for not using the SCCs.

From 1 August 2016, US companies have been able to self-certify under the new EU-US Privacy Shield, which replaces the previous Safe Harbor regime.

Equivalent transfer restrictions and exemptions will apply under the GDPR, which helpfully anticipates processor-to-processor SCCs, and also expressly recognises BCRs.

32 Notification of cross-border transfer

Does cross-border transfer of PII require notification to or authorisation from a supervisory authority?

Transfer of personal data involving a transfer to another jurisdiction, and the basis upon which the transfer is being justified, must be notified if a controller is required to register with the ODPC.

The ODPC can prohibit transfers of personal data to places outside Ireland where it considers that the data protection rules are likely to be contravened and that individuals are likely to suffer damage or distress.

33 Further transfer

If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?

Yes. The same restrictions apply equally to transfers to service providers and onwards transfers, whether by service providers or data owners.

Rights of individuals

34 Access

Do individuals have the right to access their personal information held by PII owners? Describe how this right can be exercised as well as any limitations to this right.

Yes. Under section 3 of the DPA, individuals have the right to find out free of charge whether an organisation or an individual holds information about them. This right includes the right to be given a description of the information and to be told the purposes for which that information is held. A request for this information must be made in writing by the individual and the individual must receive a reply within 21 days according to the DPA.

Section 4 of the DPA provides that individuals have the right to obtain a copy of any information that relates to them that is held

either on a computer or in a structured manual filing system, or that is intended for such a system. A maximum fee of €6.35 is permitted when a request is made under section 4 and the organisation or entity is given 40 days to reply to such a request.

Exceptions to the right of access

The DPA set out specific circumstances when an individual's right of access to their personal information held by a controller may be restricted.

Disclosure is not mandatory if the information would be likely to:

- hinder the purposes of anti-fraud functions;
- damage international relations;
- impair the security or order in a prison or detention facility;
- hinder the assessment or collection of any taxes or duties; or
- to cause prejudice to the interests of the data controller where the data relates to estimates of damages or compensation regarding a claim against the data controller.

Certain information is also exempt from disclosure if the information is:

- protected by legal privilege;
- used for historical, statistical or research purposes, where the information is not disclosed to anyone else, and where the results of such work are not made available in a form that identifies any of the individuals involved;
- an opinion given in confidence; or
- used to prevent, detect or investigate offences, or will be used in the apprehension or prosecution of offenders.

If a request would be either disproportionately difficult or impossible to process the data controller or processer does not have to fulfil the request.

Exemptions also apply in respect of access to social work data, disclosure of which may be refused if it is likely to cause serious damage to the physical, mental or emotional condition of the data subject.

A request for health data may also be refused if disclosure of the information is likely to seriously damage to the physical or mental health of the data subject.

The GDPR will reduce the timeline for compliance with data access requests to one month in most cases. Such requests will also have to be complied with free of charge unless the request is manifestly unfounded or excessive.

35 Other rights

Do individuals have other substantive rights?

Yes. An individual may 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 is, 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.

An individual has the right to have his or her data either deleted or rectified provided a request for such is made in writing (eg, a data subject can require the rectification of incorrectly held information about him or her). The person to whom the request is made must respond within a reasonable amount of time and no later than 40 days after the request. It should be noted, however, that there is no express right of an individual to request the deletion of their information if it is being processed fairly within the terms of the DPA.

Data controllers must delete personal data once it is no longer reasonably required.

As a result of the *Google Spain* case in 2014, data subjects may have a 'right to be forgotten' in certain circumstances.

The GDPR expands and strengthens data subject rights, introducing additional rights, such as the right to be forgotten and data portability, on a legislative basis.

The GDPR also recasts the data protection principles, reframes security obligations in a structure of data protection by design and by default, and introduces the principle of data controller accountability for compliance. Obligations as to accuracy, retention, finality and security (see questions 12 and 15 to 19) will all be impacted by these changes.

36 Compensation

Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

Where the ODPC upholds or partially upholds a complaint against an organisation for the mishandling of personal data, this does not give the complainant a right to compensation. If, however, an individual suffers damage through the mishandling of his or her personal information, then he or she may be entitled to claim compensation separately through the courts. Section 7 of the DPA makes it clear that organisations that hold personal data owe a duty of care to those individuals. Actual damage is required.

Under the GDPR, the rights of individuals to compensation for breach of their rights is clarified, and will apply whether the damage is material or non-material.

37 Enforcement

Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

In the first instance, these rights are enforced by the ODPC through the courts. However, certain actions by data processors or controllers can attract either civil or criminal liability. This will continue to be the case under the GDPR, although under the GDPR, the Commission will have the power to impose administrative fines directly.

Exemptions, derogations and restrictions

38 Further exemptions and restrictions

Does the law include any derogations, exclusions or limitations other than those already described? Describe the relevant provisions.

No. All exemptions and restrictions are dealt with in the answers to other questions.

Supervision

39 Judicial review

Can PII owners appeal against orders of the supervisory authority to the courts?

Yes. Decisions and orders of the ODPC are appealable though the courts system. For example, if a data controller or data processor objects to a prohibition notice issued by the ODPC (such a notice prohibits transfers of personal data outside of the jurisdiction), then they have the right to appeal it to the Irish Circuit Court.

Also, an 'information notice' from the ODPC can be appealed to the Circuit Court (see question 2).

Under the GDPR, data controllers, data processors and data subjects will continue to have the right to appeal decisions of the Commission.

Specific data processing

40 Internet use

Describe any rules on the use of 'cookies' or equivalent technology.

Under the e-Privacy Regulations the storage of cookies or of equivalent devices without the express (and informed) consent from the data subject is prohibited. Obtaining unauthorised access to any personal data through an electronic communications network is also prohibited.

There are situations, however, where the use of cookies without the express and informed consent of the data subject is allowed. This is permitted when the use of cookies is strictly necessary to facilitate a transaction, (and that transaction has been specifically requested by the data subject). In this situation, the use of cookies is only permitted while the session is live.

41 Electronic communications marketing

Describe any rules on marketing by email, fax or telephone.

Under the e-Privacy Regulations, using publicly available communications services to make any unsolicited calls or send unsolicited emails for the purpose of direct marketing, is restricted. The rules relating to such are summarised below.

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 order 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); and
- be a current customer of the company.

Direct marketing by email or text message

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

An exception is where the person is firstly an existing customer and secondly the service or product that is being marketed is either the same or very similar to the product previously sold to that person.

In general, the details obtained during the sale of a product or a service can only be used for direct marketing by email if:

- the product or service being marketed is similar to that which was initially sold to the customer (ie, at the time when their details were first obtained);
- at the point when the personal data was initially collected, the customer was given the opportunity to object to the use of his or her personal data for marketing purposes (note that the manner of doing so must be free of charge and simple);
- each time the customer is sent a marketing message, he or she is given the option to opt out of such messages in the future; or
- the related sale occurred in the past 12 months, or where applicable, the contact details were used for sending an electronic marketing communication during that 12-month period.

The European Commission has published a proposal for an e-Privacy Regulation, which if enacted would replace the Irish e-Privacy Regulations with potentially more restrictive requirements.

42 Cloud services

Describe any rules or regulator guidance on the use of cloud computing services.

The ODPC has published guidance on its website relating to cloud computing services. That guidance focuses on security, data location and the requirement for a written contract that meets the requirements of the DPA. The ODPC guidance also cross refers to the 'Adopting the Cloud – Decision Support for Cloud Computing' (April 2012) published by the National Standards Authority of Ireland in conjunction with the Irish Internet Association, which provides information on the different models of cloud computing and the issues (including data protection and security) that need to be addressed by any organisation considering using a cloud provider. The ODPC guidance also references extensive guidance provided by the European Network and Information Security Agency.

Anne-Marie Bohan **anne-marie.bohan@matheson.com**

70 Sir John Rogerson's Quay
Dublin 2
Ireland

Tel: +353 1 232 2000
Fax: +353 1 232 3333
www.matheson.com

Getting the Deal Through

Acquisition Finance
Advertising & Marketing
Agribusiness
Air Transport
Anti-Corruption Regulation
Anti-Money Laundering
Arbitration
Asset Recovery
Automotive
Aviation Finance & Leasing
Banking Regulation
Cartel Regulation
Class Actions
Commercial Contracts
Construction
Copyright
Corporate Governance
Corporate Immigration
Cybersecurity
Data Protection & Privacy
Debt Capital Markets
Dispute Resolution
Distribution & Agency
Domains & Domain Names
Dominance
e-Commerce
Electricity Regulation
Energy Disputes
Enforcement of Foreign Judgments
Environment & Climate Regulation
Equity Derivatives
Executive Compensation & Employee Benefits
Financial Services Litigation
Fintech
Foreign Investment Review
Franchise
Fund Management
Gas Regulation
Government Investigations
Healthcare Enforcement & Litigation
High-Yield Debt
Initial Public Offerings
Insurance & Reinsurance
Insurance Litigation
Intellectual Property & Antitrust
Investment Treaty Arbitration
Islamic Finance & Markets
Labour & Employment
Legal Privilege & Professional Secrecy
Licensing
Life Sciences
Loans & Secured Financing
Mediation
Merger Control
Mergers & Acquisitions
Mining
Oil Regulation
Outsourcing
Patents
Pensions & Retirement Plans
Pharmaceutical Antitrust
Ports & Terminals
Private Antitrust Litigation
Private Banking & Wealth Management
Private Client
Private Equity
Product Liability
Product Recall
Project Finance
Public-Private Partnerships
Public Procurement
Real Estate
Restructuring & Insolvency
Right of Publicity
Securities Finance
Securities Litigation
Shareholder Activism & Engagement
Ship Finance
Shipbuilding
Shipping
State Aid
Structured Finance & Securitisation
Tax Controversy
Tax on Inbound Investment
Telecoms & Media
Trade & Customs
Trademarks
Transfer Pricing
Vertical Agreements

Also available digitally

Online

www.gettingthedealthrough.com

Law Business Research

Data Protection & Privacy
ISSN 2051-1280

THE QUEEN'S AWARDS FOR ENTERPRISE: 2012

LACCA
LATIN AMERICAN CORPORATE COUNSEL ASSOCIATION

Official Partner of the Latin American Corporate Counsel Association

ABA Section of International Law
Your Gateway to International Practice

Strategic Research Sponsor of the ABA Section of International Law