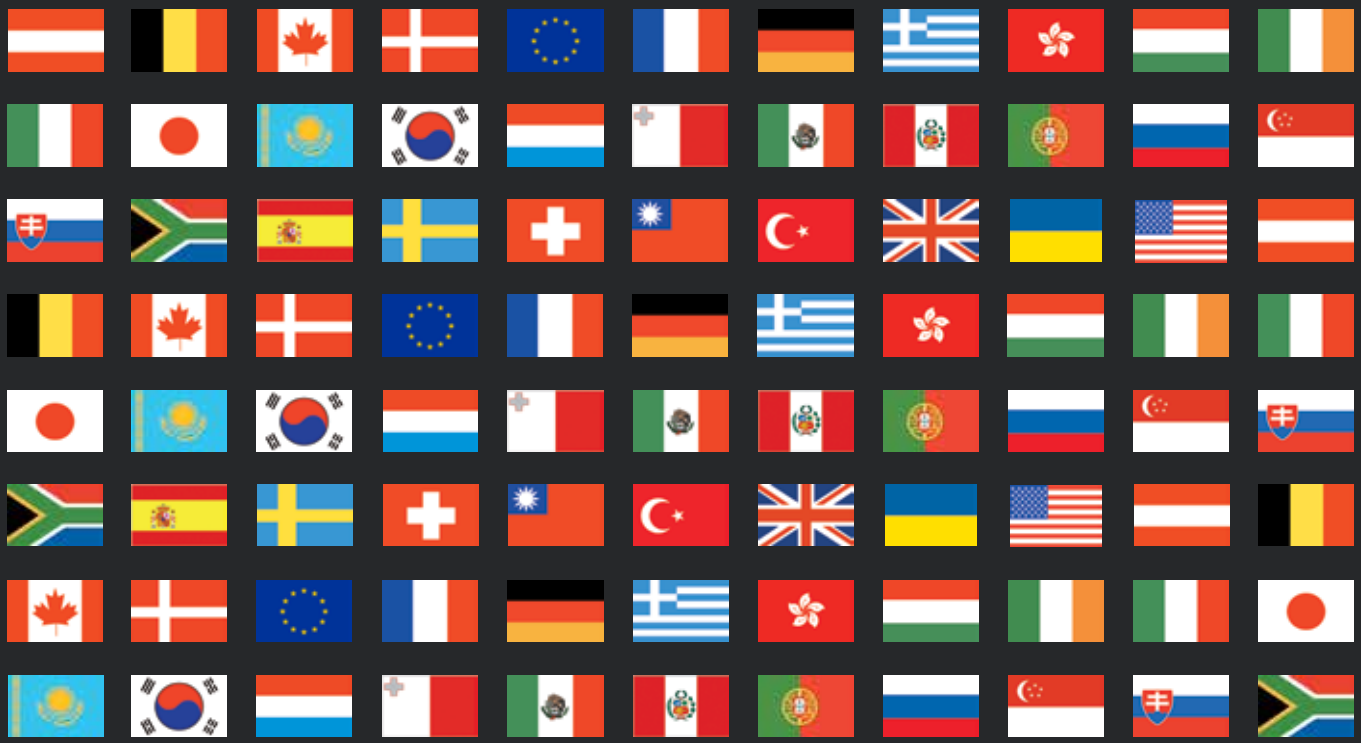
Data Protection & Privacy

In 31 jurisdictions worldwide

Contributing editor
Rosemary P Jay



2015

GETTING THE DEAL THROUGH

GETTING THE DEAL THROUGH

Data Protection & Privacy 2015

Contributing editor

Rosemary P Jay

Hunton & Williams

Publisher
Gideon Roberton
gideon.roberton@lbresearch.com

Subscriptions
Sophie Pallier
subscriptions@gettingthedealthrough.com

Business development managers
George Ingledew
george.ingledew@lbresearch.com

Alan Lee
alan.lee@lbresearch.com

Dan White
dan.white@lbresearch.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 7908 1188
Fax: +44 20 7229 6910

© Law Business Research Ltd 2014
No photocopying: copyright licences do not apply.
First published 2012
Third edition
ISSN 2051-1280

The information provided in this publication is general and may not apply in a specific situation. Legal advice should always be sought before taking any legal action based on the information provided. This information is not intended to create, nor does receipt of it constitute, a lawyer–client relationship. The publishers and authors accept no responsibility for any acts or omissions contained herein. Although the information provided is accurate as of September 2014, be advised that this is a developing area.

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

CONTENTS

Ireland

John O'Connor and 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? Have any international instruments on privacy or data protection been adopted in your jurisdiction?

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

As well as conferring rights on individuals, the DPA also place 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 which the data controller is in possession of or is likely to come into possession of).

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

The DPA place responsibilities on both 'data controllers' and 'data processors'. A data controller is one 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.

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.

2 Data protection authority

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

The DPA confer 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.

Powers of the ODPC

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. These usually take the form of scheduled privacy audits in practice although 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 in this jurisdiction 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 by 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 this jurisdiction to an area outside of this jurisdiction, however 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.

Such an 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.

The ODPC may bring summary legal proceedings for an offence under the DPA.

The ODPC does not have the power to impose fixed monetary penalties, unlike the information commissioner in the UK.

3 Breaches of data protection

Can breaches of data protection lead to 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.

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?

Some areas of activity are outside the scope of the DPA. The DPA applies to individuals or organisations established in Ireland that collect, store, or process personal data about living people on any type of computer (or structured filing system).

© Law Business Research Ltd 2014

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
- the personal data is kept by an individual for his or her personal, family or household affairs, or for solely recreational purposes.

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.

No. Interception of communications is covered by the Interception of Postal Packets and Telecommunications (Regulation) Act 1993 and surveillance is covered by the Criminal Justice (Surveillance) Act 2009.

6 Other laws

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

Any processing of personal data in the context of e-health records, social media, or credit information must comply with the principles as set out in the DPA.

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 which the data controller is in possession of or is likely to come into possession of).

8 Extraterritoriality

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

Yes. The DPA apply to data controllers in respect of the processing of personal data only if:
- the data controller is established in Ireland, and the data are 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.

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 services to owners?

Yes. The DPA applies to individuals or organisations established in Ireland that collect, store or process data about living people on any form of computer system.

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.

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 without the data subject's consent (except where sensitive personal data is concerned – see question 11 below) 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 the contract, which require the personal data to be processed);
- 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 grounds for which the restrictions in the DPA (including consent) do not apply (for example, 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).

11 Legitimate processing – types of data

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

Yes. Section 2B of the DPA imposes the following special obligations on the data controller for the processing of sensitive personal data:
- the personal data must be fairly obtained;
- the data subject, a parent or legal guardian (where required) must give explicit consent, having been informed of the purpose of the processing;
- if consent is not obtained, a data controller can still process the sensitive personal data if he or she is:
  - 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;

© Law Business Research Ltd 2014

- 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.

Data handling responsibilities of owners of PII

12 Notification

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

Not as such. However, data subjects need to be notified at the point of collection of personal data. Personal data is not considered to be processed fairly, under section 2D of the DPA, unless, in the case of personal data obtained 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 the information that is necessary 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.

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.

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 which 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.

Third, 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).

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 and 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.

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 process the personal data only in ways compatible with the purposes for which it was given to 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 or 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 are not used in such a way that damage or distress is caused to any data subject.

Security

19 Security obligations

What security obligations are imposed on data owners and entities that process PII on their behalf?

According to section 2 of the DPA data controllers must have 'appropriate security measures' in place. These measures 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.

© Law Business Research Ltd 2014

20 Notification of security breach

Does the law include obligations to notify the regulator or individuals of breaches of security?

Yes. The ODPC 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 as these are subject to a mandatory reporting obligation under the e-Privacy Regulations 2011.

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 is 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); and
- 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;
  - the breach does not involve sensitive personal data or personal data of a financial nature; or
  - if the data controller is unclear about whether to report the incident or not, 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.

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 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 which is collected.

22 Record keeping

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

No. No such specific rules relating to internal records are provided for in the DPA.

Registration and notification

23 Registration

Are owners and 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;
- data controllers whose business consists of processing personal data for the supply of others, other than for journalistic, literary or artistic purposes; 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 3 of SI No. 657 of 2007 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.

There is also a broad exemption applied to normal commercial activity, which by definition requires the processing of personal data.

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.

Additionally, 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 above categories):

- 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 Acts;
- 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.

© Law Business Research Ltd 2014

Subject to the above, all data controllers and data processors are required to register, except to the extent that:

- they carry out processing for the sole purpose of keeping in accordance with law of a register that is intended to provide information to the public and is open to consultation either by the public in general or by any person demonstrating a legitimate interest;
- they process manual data (other than such categories, if any, of such data as may be prescribed);
- they carry out any combination of the above; or
- the data controller is a body that is not established or conducted for profit and is carrying out processing for the purposes of establishing or maintaining membership of or support for the body or providing or administering activities for the members of the body or persons who have regular contact with the body.

The DPA also provide 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.

The ODPC is obliged not to 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 concerned are being, and will continue to be, provided by him or her.

Where the ODPC refuses an application for registration he or she shall notify the applicant in writing and specify the reasons for the refusal. An appeal against such decision can be made to the Circuit Court.

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. The information necessary for registration can be submitted online or 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 provide 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 or 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, e-mail, date of birth, etc) must also be listed or described. For each of these applications listed, a list of the persons or bodies to whom the personal data maybe 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, sexual life, criminal convictions etc).

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.

25 Penalties

What are the penalties for a data owner or processor 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 and 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)).

© Law Business Research Ltd 2014

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 the jurisdiction 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?

According to 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 contain the security conditions attaching to the processing of personal data, and must 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.

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 e-Privacy Regulations 2011 set out security measures for electronically stored data.

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.

As for the United States, transfers are permitted if the recipient has signed up for the US Department of Commerce's so-called 'Safe Harbor' privacy principles.

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

- where the ODPC authorises such;
- 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.

Other methods of enabling the transfer of personal data include using binding corporate rules (in practice these criteria are very narrowly construed), which are internal 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. Binding Corporate Rules are submitted to the ODPC for approval. The EU model clauses may also be used. These are incorporated into the actual transfer agreement and are clauses that the European Commission and the ODPC have declared as providing an adequate level of protection to transfers. Approval of a data transfer agreement (for example using the EU model clauses mentioned in question 32) does not require approval of the ODPC. The ODPC can approve contractual clauses that do not necessarily conform to the European model clauses.

32 Notification of transfer

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

This varies depending on the circumstance, for example whether the transfer of personal data involves a transfer to another jurisdiction or to another entity within this jurisdiction.

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 see a copy of their personal information held by PII owners? Describe 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 fee of €6.35 is required when a request is made under section 4 and the organisation or entity is given 40 days to reply to such a request.

© Law Business Research Ltd 2014

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 an organisation 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; or
- hinder the assessment or collection of any taxes or duties; or if
- disclosure of estimates of damages or compensation regarding a claim against the data controller is likely to cause damage to 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 such 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 the physical or mental health of that data subject.

35 Other rights

Do individuals have other substantive rights?

Yes. An individual may object to processing which 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 (for example 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 however delete personal data once it is no longer reasonably required.

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.

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 but certain actions by data processors or controllers can attract either civil or criminal liability.

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 data 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, if an individual receives an 'information notice' from the ODPC, this can also be appealed by the individual to the Circuit Court (see question 2).

40 Criminal sanctions

In what circumstances can owners of PII be subject to criminal sanctions?

Failure by a data controller or data processor to register with the ODPC, is a criminal offence. Examples of other actions that have the potential to attract criminal liability under the DPA are:

- failure to comply with enforcement, information and prohibition notices;
- unauthorised disclosure of personal data by a data processor; and
- failure by a registered data controller or data processor to notify the ODPC of a change in address.

41 Internet use

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

Cookies

Under the e-Privacy Regulations 2011 the storage of cookies or of equivalent devices without the express (and informed) consent from the data subject in question is prohibited. Obtaining 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.

42 Electronic communications marketing

Describe any rules on marketing by e-mail, fax or telephone.

Under the e-Privacy Regulations 2011, using publicly available communications services to make any unsolicited calls or send unsolicited e-mails

© Law Business Research Ltd 2014

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 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.

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 e-mail 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);
- 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;
- 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 simplistic); 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.

John O'Connor **john.oconnor@matheson.com**
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

© Law Business Research Ltd 2014

Getting the Deal Through

Acquisition Finance
Advertising & Marketing
Air Transport
Anti-Corruption Regulation
Anti-Money Laundering
Arbitration
Asset Recovery
Aviation Finance & Leasing
Banking Regulation
Cartel Regulation
Climate Regulation
Construction
Copyright
Corporate Governance
Corporate Immigration
Data Protection & Privacy
Debt Capital Markets
Dispute Resolution
Domains and Domain Names
Dominance
e-Commerce
Electricity Regulation
Enforcement of Foreign Judgments
Environment
Foreign Investment Review
Franchise
Gas Regulation
Government Investigations
Insurance & Reinsurance
Insurance Litigation
Intellectual Property & Antitrust
Investment Treaty Arbitration
Islamic Finance & Markets
Labour & Employment
Licensing
Life Sciences
Mediation
Merger Control
Mergers & Acquisitions
Mining
Oil Regulation
Outsourcing
Patents
Pensions & Retirement Plans
Pharmaceutical Antitrust
Private Antitrust Litigation
Private Client
Private Equity
Product Liability
Product Recall
Project Finance
Public-Private Partnerships
Public Procurement
Real Estate
Restructuring & Insolvency
Right of Publicity
Securities Finance
Ship Finance
Shipbuilding
Shipping
State Aid
Tax Controversy
Tax on Inbound Investment
Telecoms and Media
Trade & Customs
Trademarks
Transfer Pricing
Vertical Agreements

Also available digitally

Online

www.gettingthedealthrough.com

iPad app

Available on iTunes

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 Partner of the ABA Section of International Law