Ireland

Rob Corbet, Colin Rooney, Caroline O’Gorman and Olivia Mullooly
Arthur Cox

REGULATION

Legislation

1. What national laws regulate the collection and use of personal data?

General laws
This area is governed by the Data Protection Act 1988 as amended, among others, by the Data Protection (Amendment) Act 2003 (DPA), which transpose Directive 95/46/EC on data protection into Irish law.

Secondary legislation
The following statutory instruments have been introduced:

- S.I. No. 336 of 2011 – European Communities (Electronic Communications Networks and Services) Regulations 2011 (Privacy and Electronic Communications) (e-Privacy Regulations).

Scope of legislation

2. To whom do the laws apply?

The laws apply to individuals or organisations established in Ireland that collect, store or process data about living people on any type of computer or in a structured filing system.

The DPA applies to processing by both data controllers and data processors. A “data controller” is a person who, either alone or with others, controls the contents and use of personal data. A “data processor” means a person who processes data on behalf of a data controller. This does not include employees who process data in the course of their employment. A “person” can be a natural person or a body corporate. (See Question 4 for a definition of “processing”.)

3. What data is regulated?

The DPA regulates the processing of personal data of a living person, which is in the possession or under the control of a data controller.

The definition of “data” includes both manual and automated data:

- Manual data means the information that is recorded either:
  - as part of a relevant filing system; or
  - with the intention that it should form part of a relevant filing system.

- Automated data is information that is either:
  - being processed by means of equipment operating automatically in response to instructions given for that purpose; or
  - recorded with the intention that it should be processed by means of equipment operating automatically.

Personal data is defined as information from which the individual concerned can be identified, either directly or through use of the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller.
"Sensitive personal data" is any data that relates to a data subject’s:
- Racial or ethnic origin, political opinions, religious or philosophical beliefs.
- Trade union membership.
- Physical or mental health or condition, or sexual life.
- The commission or alleged commission of any offence, or related proceedings, disposal of proceedings or sentence.

4. What acts are regulated?

The DPA regulates the processing of data. “Processing” is very broadly defined and encompasses the performance of any operation in relation to information or records, either automatically or otherwise, including:
- Obtaining, recording or keeping the information or data.
- Collecting, organising, storing, altering or adapting the information or data.
- Retrieving, consulting or using the information or data.
- Disclosing the information or data by transmitting, disseminating or otherwise making it available.
- Aligning, combining, blocking, erasing or destroying the information or data.

5. What is the jurisdictional scope of the rules?

The DPA applies to:
- Data controllers established in Ireland.
- Persons who ordinarily reside in Ireland.
- An organisation incorporated under the laws of Ireland.
- A partnership or other unincorporated body established under the laws of Ireland.
- An individual who maintains an office, branch, or agency in Ireland, where the person carries on any activity, or a regular practice that processes personal data.

A wide exemption is available for normal commercial activity, which by definition requires the processing of personal data, for example:
- Keeping details of customers and suppliers. However, this exemption does not include health professionals who process personal data relating to physical or mental health.
- Data controllers who only process data relating to personnel administration.
- Candidates for and holders of elective political office who only process personal data for electoral activities or for the purpose of providing advice or assistance.
- Educational establishments in relation to functions related to the provision of education.
- Solicitors and barristers who only process personal data for legal professional purposes.
- Companies that only process personal data relating to shareholders, directors or other officers of the company with a view to compliance with the Companies Acts 1963 to 2012.
- Data controllers who only process personal data with a view to the publication of journalistic, literary or artistic material.
- Data processors who process personal data on behalf of data controllers where the processing of the data would fall under one or more of the above categories.

6. What are the main exemptions (if any)?

The DPA does not apply if one of the following applies (section 1(4), DPA):
- The data is, or at any time was, kept for the purpose of safeguarding Ireland’s security.
- The data consists of information that the person keeping the data is required by law to make available to the public.
- The data is kept by an individual for his personal, family or household affairs, or for recreational purposes only.

7. Is notification or registration required before processing data?

Certain types of data controllers and data processors must register with the Office of the Data Protection Commissioner (ODPC) if they both:
- Have a legal presence in, or use equipment located in Ireland.
- Hold personal data in an automated form.

The registration requirements are governed by sections 16 to 20 of the DPA, S.I. No. 657 of 2007 and S.I. No. 658 of 2007. Generally, all data controllers and data processors must register, unless they are exempt under either:
- Section 16(1)(a) or (b) of the DPA.
- Section 3 of S.I. No. 657 of 2007, which excludes from the registration requirements:
  - 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 data has been prescribed by the Commissioner as requiring registration); and
  - organisations that are not established or conducted for profit and that are processing data related to their members and supporters and their activities.

A wide exemption is available for normal commercial activity, which by definition requires the processing of personal data, for example:
If any of the exemptions do apply, the exemption from registration is limited only to the extent to which data is processed within the scope of that exemption.

The costs of registration depend on how many employees a data controller or data processor has, and whether registration is made online or by post (the former is cheaper). The fees applicable are available on the ODPC website at [http://dataprotection.ie/viewdoc.asp?m=g&fn=/documents/register/RegGuidanceFebruary2010.htm](http://dataprotection.ie/viewdoc.asp?m=g&fn=/documents/register/RegGuidanceFebruary2010.htm).

Mandatory registration requirements apply to the following parties who cannot claim an exemption:
- Government bodies/public authorities.
- Insurance undertakings.
- Financial institutions.
- Credit institutions.
- 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 network or service providers.
- Data controllers that process genetic data within the meaning of 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.
- Data processors that process personal data on behalf of a data controller, in any of the categories listed above.

**MAIN DATA PROTECTION RULES AND PRINCIPLES**

**Main obligations and processing requirements**

8. What are the main obligations imposed on data controllers to ensure data is processed properly?

Data controllers must:
- Obtain and process the personal data fairly.
- Keep the personal data only for one or more specified and lawful purpose.
- Process the personal data only in ways compatible with the purposes for which it was given to the data controller initially.
- Keep the personal data safe and secure.
- Keep the personal data accurate and up to date.
- Ensure that the personal data is adequate, relevant and not excessive.
- Retain the personal data for no longer than is necessary for the specified purpose or purposes.
- Give a copy of the personal data of an individual held to that individual, should he request it.
- Ensure that there are adequate security measures in place to:
  - prevent unauthorised access to, or unauthorised alteration, disclosure or destruction of the data (especially where the processing involves transmission over a network); and
  - ensure protection of the data against all unlawful forms of processing.

9. Is the consent of data subjects required before processing personal data?

While consent is not the only way to legitimise the processing of personal data, it is commonly used to legitimise data processing.

**Form and content of consent**

Express consent is required for the processing of sensitive personal data (section 2B, DPA). However, beyond this, the DPA does not outline the required form or content of consent. Consent does not need to be in writing. However, it is necessary to be able to prove consent is given.

Consent for receipt of direct marketing can be implied in the context of an ongoing business relationship subject to certain conditions (see Question 19) ([e-Privacy Regulations](http://www.practicallaw.com/e-privacy-regulations)). However, consumers may only be targeted in this manner with products that are similar to those they have already purchased. The ODPC interprets “similar” narrowly where consumers are involved. If the consumer is not an existing customer, they must expressly consent to the processing of their personal data for the purposes of direct marketing. Consumers and businesses must always be afforded a free of charge “opt out” in every subsequent communication.

**Minors**

The DPA does not provide any specific minimum age for giving consent to data processing. However, data controllers must decide if a minor (anyone under the age of 18) is capable of appreciating the implications of giving consent (section 2A(1), DPA). If a person is not able to appreciate the nature and effect of consent (due to physical or mental disability or age), consent should be given on his behalf by a parent, guardian or relative (section 2A(1), DPA).

10. If consent is not given, on what other grounds (if any) can processing be justified?

Data controllers can process data 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 the contract, which require the 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.

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 sets out 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).

**Special rules**

11. Do special rules apply for certain types of personal data, such as sensitive data?

Section 2B of the DPA imposes the following special obligations on the data controller for the processing of sensitive personal data (see Question 3 for a definition of sensitive personal data):
- The data must be fairly obtained (see Question 12);
- 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 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;
  - 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 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.

**RIGHTS OF INDIVIDUALS**

12. What information should be provided to data subjects at the point of collection of the personal data?

Personal data is not considered to be processed fairly, under section 2D of the DPA, unless, in the case of data obtained from the data subject, the data controller ensures that the data subject has been provided with at least the following information:
- The name of the data controller.
- The purpose for collecting the data.
- The identity of any representative nominated for the purposes of the DPA.
- The persons or categories of persons to whom the 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.
- 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 data will be processed.

13. What other specific rights are granted to data subjects?

An individual can write to an organisation to determine whether it holds their personal data. If so, they should receive a response within 21 days, which provides a description of the data and the purposes for which it is kept (section 3, DPA).

**Right of access**

A data subject can, on written application to a data controller and on payment of EUR6.35, ask for a copy of his personal data (section 4, DPA). Data access requests must be processed within 40 days of receipt.
Information is exempt from disclosure under the DPA if any of the following apply:

- The information is:
  - an opinion on the data subject given in confidence. In practice this exemption is narrowly applied by the ODPC;
  - protected by legal professional privilege;
  - used to prevent, detect or investigate offences, or will be used in the apprehension or prosecution of offenders;
  - used for historical, statistical or research purposes, where the information is not disclosed to anyone else, and where the results of the statistical work or research are not made available in a form that identifies any of the individuals involved; or
  - back-up material.
- Disclosing the information would be likely to:
  - hinder the purposes of anti-fraud functions;
  - hinder the assessment or collection of any taxes or duties;
  - impair the security, maintenance or order in a prison or detention facility, or
  - damage Irish international relations.
- Disclosure of estimates of damages or compensation regarding a claim against the data controller is likely to cause damage to the data controller.

An individual's request for health data may be refused if disclosure of the information is likely to seriously damage the physical or mental health of the data subject (Data Protection (Access Modification) (Health) Regulations, 1989 (S.I. No. 82 of 1989)) (Health Data Access Regulations).

Data controllers or data processors (if they are not health professionals) must consult with the individual’s doctor before disclosing health data (Health Data Access Regulations).

Similar exemptions are available in respect of access to social work data (under the Data Protection (Access Modification) (Social Work) Regulations, 1989 (S.I. No. 83 of 1989)). Disclosure of this data can be refused if it is likely to cause serious damage to the physical or mental health or emotional condition of the data subject.

A data controller is not obliged to disclose the personal information of third parties under data access request (section 4(4), DPA). Redactions can take place to exclude the third party's information.

If a request would be impossible or disproportionately difficult to process, a data controller or processor is not obligated to process the request (section 4(9), DPA).

Rectification or deletion

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

Processing likely to cause damage or distress

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.
- Purposes of the legitimate interests pursued by the data controller to whom the 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 right to privacy.

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

Automated decision-making

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

14. Do data subjects have a right to request the deletion of their data?

There is no express right for a data subject to request the deletion of his information if it is being processed fairly within the terms of the DPA. A data controller must delete personal data once it is no longer reasonably required. A data subject can require rectification of any incorrect data held about them (see Question 13, Rectification or deletion).

15. What security requirements are imposed in relation to personal data?

Data controllers must have “appropriate security measures” in place (section 2(c), DPA). In determining what an appropriate security measure is, the data controller must:

- Take into account technological development and the cost of implementing the measures.
- Ensure that the measures:
  - provide a level of security appropriate to the harm that might result from any unauthorised or unlawful processing, accidental or unlawful destruction or loss of data; and
  - are appropriate to the nature of the data concerned.

Data controllers and data processors must ensure all of their employees comply with the security measures in place.

No specific provisions relating to data security are set out in the DPA. However, the e-Privacy Regulations set out security measures for electronically stored data, which only apply to providers of publicly available electronic communications services in public communications networks in the state and, where relevant, in the EU.
16. Is there a requirement to notify personal data security breaches to data subjects or the national regulator?

The ODPC has published a non-binding code of practice entitled the Personal Data Security Breach Code of Practice (Code), which provides the following guidelines for when a data breach occurs:

- The data controller should immediately consider whether to inform those impacted by the data breach. Informing the data subjects allows them to consider the consequences for each of them individually and to take appropriate measures to mitigate the impact of the breach. In certain cases, data controllers should also notify organisations that might be able to assist in protecting the data subjects (such as An Garda Síochána and financial institutions).

- If the data concerned was encrypted or otherwise protected by technological measures to the 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 data. Consequently, it may be unnecessary to inform the data subjects. In the view of the ODPC, it is only possible to reach this conclusion where the technological measures are of an extremely high standard.

- If the breach is caused by a data processor, he should report it to the relevant data controller as soon as he becomes aware of the breach.

- All incidents in which personal data has been put at risk should be reported to the ODPC as soon as the data controller is aware of the incident. The only exception is where:
  - the full extent and consequences of the incident have been reported without delay directly to the affected data subjects;
  - it affects fewer than one hundred data subjects; and
  - the breach does not involve sensitive personal data or personal data of a financial nature. (“Personal data of a financial nature” means an individual’s last name or any other information from which an individual’s last name can reasonably be identified in combination with that individual’s account number, credit or debit card number.)

- Where the data controller is unclear as to whether it should report the incident or not, he should report the incident to the ODPC.

- If the data controller decides to advise the ODPC of the data breach, the Code suggests the data controller should make initial contact with the ODPC within two working days of becoming aware of the incident, outlining the circumstances surrounding the data breach. Contact can be made by e-mail, telephone or fax. At this point, the ODPC will decide whether a detailed report or subsequent investigation, or both are needed. In reaching his view, the ODPC will take into account the nature of the incident and whether or not security measures exist to protect the data.

- The ODPC may require a detailed written report of the data breach from the data controller. The ODPC will specify a timeframe for the delivery of the report and it should furnish full details of the incident to the ODPC.

- In addition to this report (or alternatively), the ODPC may decide to investigate the security breach. This could include examining the systems in place at the data controller’s premises and may lead to recommendations made by the ODPC to the data controller. The ODPC could use enforcement powers to force the data controller to take action to protect the data subjects’ interests. It is good practice for data controllers to keep records of each incident which has given rise to a concern relating to data security, destruction, loss or alteration. The records should include a brief description of the nature of the incident and an explanation of why the data controller did not consider it necessary to inform the ODPC, if no notification was made. From time to time, the ODPC may request that these reports are given to his office.

- The Code does not apply to providers of publicly available electronic communications services in public communications networks in Ireland (and where relevant in the EU), as these are subject to a mandatory reporting obligation in accordance with Regulation 4 of the e-Privacy Regulations.

### PROCESSING BY THIRD PARTIES

17. What additional requirements (if any) apply where a third party processes the data on behalf of the data controller?

The data controller must at least ensure that any processing of personal data that takes place is subject to a contract between the data controller and the data processor. This contract must specify:

- The conditions under which the data may be processed.
- The security conditions attaching to the processing of the data.
- That the data must be deleted or returned on completion or termination of the contract.

The data controller must take reasonable steps to ensure that the data processor complies with these requirements. The data processor must ensure that the personal data is secure from damage, theft, accidental loss and that no unauthorised person has access to the data.

### ELECTRONIC COMMUNICATIONS

18. Under what conditions can data controllers store cookies or equivalent devices on the data subject’s terminal equipment?

The storage of cookies or equivalent devices or obtaining access to any data through an electronic communications network without express consent from the data subject is prohibited (e-Privacy Regulations). Consent must be informed and the data controller or data processor must provide information about the device in a clear and comprehensive way. The obligation to give prior consent is not required where data obtained is strictly necessary to facilitate a transaction requested by the data subject (such as for shopping online). In these instances, the use of necessary cookies or similar devices is only permissible while the session is live.
19. What requirements are imposed on the sending of unsolicited electronic commercial communications (spam)?

The use of publicly available electronic communications services to send unsolicited communications or to make unsolicited calls for the purpose of direct marketing is restricted (Regulation 13, e-Privacy Regulations). Specifically:

- The use of automatic dialling machines, fax, e-mail or text messaging for direct marketing to individuals is prohibited. However, such is allowed where the user has provided consent in advance of this processing.
- The use of automatic dialling machines, fax, e-mail or text messaging for direct marketing to a non-natural person (that is, a body corporate) is prohibited where the non-natural person has recorded its objection in the National Directory Database or has advised the sender that it does not consent to receiving those messages.
- The making of telephone calls for direct marketing to a user is prohibited if the user has recorded his objection in the National Directory Database or has informed the sender that he does not consent to receiving such messages.
- The use of automatic dialling machines or telephone calls to the mobile telephone of a subscriber or user is prohibited, unless the subscriber or user has consented to such calls (that is, opted in).
- The placing of direct marketing information in a text message sent for non-marketing purposes is not allowed, unless the subscriber or user has consented to such direct marketing.

In summary, to direct market an individual by phone, the individual must be a current customer of the company who has given his consent to the receipt of the marketing calls and, where relevant, to the receipt of communications to his mobile phone.

A fax cannot be used for direct marketing purposes with a non-customer, unless the individual receiving the fax has previously consented to the receipt of marketing communications by fax.

To use e-mail and text messages to direct market an individual, it is necessary to ensure that the individual has consented to the receipt of the direct marketing communications.

An exception is where the party is an existing customer and the product or service being marketed is similar to or the same as the previous product sold. The details obtained during the sale of a product or service can only be used for direct marketing by e-mail if all of the following apply:

- The product or service being marketed is similar to that which was sold to the customer when their details were obtained.
- When the data was collected, the customer was given the opportunity to object, in an easy manner and without charge, to the use of data for marketing purposes.
- Every time the customer is sent a marketing message, he is given the right to opt out of receiving further messages.
- The sale of the product or service occurred not more than 12 months before the sending of the electronic marketing communication or, where applicable, the contact details were used for the sending of an electronic marketing communication during that 12-month period.

INTERNATIONAL TRANSFER OF DATA

Transfer of data outside the jurisdiction

20. What rules regulate the transfer of data outside your jurisdiction?

The transfer of personal data to a country outside the European Economic Area (EEA) is prohibited, unless that country ensures an adequate level of protection for the privacy and fundamental rights and freedoms of the data subjects (section 11, DPA) (see below, Transfer to approved countries outside the EEA).

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.

The ODPC can issue a written notice, called a “prohibition notice”, to the data controller or data processor, which will prohibit the transfer of personal data out of Ireland (section 11, DPA). A prohibition notice may prevent any transfer outside Ireland, or restrict the transfer of personal data until the person concerned takes certain steps to protect the interests of the data subject.

If the data controller or data processor objects to the prohibition notice, they have the right to appeal it to the Circuit Court. Non-compliance with the prohibition notice without reasonable excuse is an offence. Prohibition notices are very rarely used in practice.

Transfer to approved countries outside the EEA

The EU has approved a list of countries outside the EEA that afford an adequate standard of data protection. Transfers of personal data to the following countries can take place without too much concern:

- Switzerland.
- Guernsey.
- Argentina.
- Isle of Man.
- Faroe Islands.
- Jersey.
- Andorra.
- Israel.
- Canada (for certain types of personal data pursuant to the Canadian Personal Information Protection and Electronic Documents Act 2000).
- A number of US organisations which have signed up to the “Safe Harbor” arrangement and adhere to an enforceable code of good data protection practice.

The data controller must take account of all of the following, in advance of a transfer to approved countries:

- The nature of the data.
- The purposes for which and the period during which the data is intended to be processed.
The country of origin of the information contained in the data.

The country of final destination of the information.

The law in force in the country of final destination.

Any relevant codes of conduct or other rules which are enforceable in that country.

Any security measures taken in respect of the data in that country.

The international obligations of that country.

Transfer to non-approved countries

Where the country to which the personal data will be transferred does not appear on an approved list of countries, the transfer of personal data can still take place if one of the following applies:

- The transfer is required or authorised by law.
- The transfer is necessary for:
  - performing contractual obligations either between the data controller and the data subject or at the request of the data subject;
  - for reasons of substantial public interest;
  - for the purpose of obtaining legal advice;
  - to prevent injury or other damage to the data subject’s health;
  - to prevent serious loss to the property of the data subject.
- The transfer is of an extract from a statutory public register.
- The transfer is authorised by the ODPC.
- The data subject has given his unambiguous consent to the transfer.

Two alternative methods of legitimising a transfer of data are:

- Incorporating the EU model clauses into the data transfer agreement. These clauses contain EU-approved data protection provisions, which incorporate the EU standards into the contract. They can be used where there is no arrangement (such as the US Safe Harbor agreement) in place.
- Using the binding corporate rules. Multinational companies draft and submit these guidelines to the ODPC for approval. They are internal rules that apply to international transfers of data. When they are adhered to, they ensure that the company complies with the relevant data protection law.

Data transfer agreements

21. Are data transfer agreements contemplated or in use? Have any standard forms or precedents been approved by national authorities?

There are certain standard contractual clauses that the EU Commission (and the ODPC) has declared as providing an adequate level of protection to transfers. These can be used in the transfer of personal data outside the EEA whether from data controller to data controller or data controller to data processor.

22. Is a data transfer agreement sufficient to legitimise transfer, or must additional requirements (such as the need to obtain consent) be satisfied?

A data transfer agreement incorporating EU Model Clauses is sufficient to legitimise a transfer of data. However, transfers can also be legitimised where one or more of the following apply:

- The transfer is required by law.
- The data subject has given his consent to the transfer.
- The transfer is necessary for the performance of a contract to which the data subject is party.
- The transfer is necessary for the taking of steps at the request of the data subject with a view to entering a contract with the data controller.
- The transfer is necessary to conclude or perform a contract between the data controller and someone other than the data subject in cases where the contract is entered into at the request of the data subject or where the contract is in the interests of the data subject.
- There are reasons of substantial public interest. (This is only likely to be relevant to public sector data controllers and only in circumstances where they can show that there is a substantial Irish public interest in the transfer of personal data.)
- The transfer is necessary for obtaining legal advice or for legal proceedings.
- The transfer is necessary to:
  - prevent injury or other damage to the data subject’s health;
  - prevent serious damage to his property; or
  - protect his vital interests in some other way.
- The personal data to be transferred is an extract from a statutory public register.
- The transfer is authorised by the ODPC.

23. Does the relevant national regulator need to approve the data transfer agreement?

Approval of the data transfer agreement by the ODPC is not required. The ODPC can approve contractual clauses which do not necessarily conform to the EU model clauses. Only agreements that provide adequate data protection safeguards will be approved. In practice, it is rare for the ODPC to approve variations or bespoke data transfer agreements. Furthermore, the ODPC is only likely to approve contractual clauses where they can be relied on by a number of different data controllers within one sector or category.

ENFORCEMENT AND SANCTIONS

24. What are the enforcement powers of the national regulator?

Powers of investigation

The ODPC has powers of investigation where an individual complains that there has been a contravention of the provisions
of the DPA (section 10, DPA). The ODPC must investigate and arrange for an amicable resolution within a reasonable time. The ODPC can launch an investigation when either:

- He is of the opinion that there may be a breach of the DPA.
- He considers it appropriate to ensure compliance with the DPA.

Investigations take the form of a privacy audit. They aim to improve data protection practices. If a serious breach is discovered, the ODPC can consider imposing further required steps.

**Powers of entry and examination**

The ODPC can appoint an “authorised officer” to enter and examine the premises of the data controller or data processor to enable the ODPC to pursue or carry out its functions (section 24, DPA). He may, at reasonable times, enter premises where he reasonably believes that they are occupied by a data controller or data processor to inspect the premises and any data therein. He may also inspect and examine any data equipment on the premises. The authorised officer can require any person on the premises to disclose to him any such data and produce any data material that is in that person’s power. Any person who obstructs or impedes the work of the authorised officer commits an offence.

**Information notice**

The ODPC usually seeks to resolve complaints without recourse to litigation. Following an investigation into a complaint (see above, Powers of investigation), for contraventions which are not criminal offences, the ODPC has the power to:

- Issue information and enforcement notices requiring the data controller or data processor to:
  - provide certain information to the ODPC; and
  - take steps (such as ceasing data capture or processing) until its data activities comply with the law.
- “Name and shame” non-compliant individuals and organisations in the ODPC’s annual report. (This is the most frequent result of a finding of non-compliance.)

**Enforcement notice**

Where the ODPC has formed the opinion that a party is contravening the DPA, it may oblige the data controller to take steps to correct its use of the personal data by issuing an enforcement notice. This may include:

- Correcting the data held.
- Refraining from using or allowing the data to be used for certain purposes.
- Deleting the data or adding supplementary material to the data.

Non-compliance with the enforcement notice is an offence, but the enforcement notice can be appealed to the Circuit Court.

**Prohibition notice**

See Question 19.

**Criminal liability**

Examples of criminal offences include:

- Failure by a data controller or processor to register with the ODPC (which is required in section 16 of the DPA).
Furthermore, the ODPC can investigate complaints made by data subjects (see above, Powers of investigation).

25. What are the sanctions and remedies for non-compliance with data protection laws?

Penalties for offences under the DPA

Criminal offences. Breaches of the DPA are prosecuted by the ODPC and attract the following penalties (section 31, DPA):
- A maximum fine of EUR3,000 for summary offences.
- A maximum fine of EUR100,000 for indictable offence.

Where a party is convicted under the DPA, the court may additionally order:
- Any data material which appears to be connected with the commission of the offence to be forfeited or destroyed.
- The deletion of any relevant data.

A court would use these powers to prevent any further damage being done by the use of the material or data. When exercising this power, the court must give the owner of the data concerned or anyone who is otherwise interested in the data an opportunity to show cause as to why a forfeiture order should not be made.

Civil sanctions. Under section 7 of the DPA a duty of care is imposed on the data controller or data processor who processes or holds personal data (see Question 24, Civil liability).

Penalties for offences under the e-Privacy Regulations

Offences under the e-Privacy Regulations may be brought and prosecuted by the ODPC as follows:
- On summary conviction each call or message can attract a maximum fine of EUR5,000.
- If convicted on indictment the fines can be:
  - a maximum of EUR50,000 for natural persons;
  - a maximum of EUR250,000 for body corporates.
- The court may also order the destruction of data that is connected with the commission of an offence.

CONTRIBUTOR DETAILS

ROB CORBET
Arthur Cox
T +353 1 618 0566
F +353 1 616 3823
E rob.corbet@arthurcox.com
W www.arthurcox.com

Qualified. Ireland, 1999; Irish and European Trade Mark Agent, 1999
Areas of practice. Privacy and data protection; technology; intellectual property; betting and gaming.

COLIN ROONEY
Arthur Cox
T +353 1 618 0543
F +353 1 616 3883
E colin.rooney@arthurcox.com
W www.arthurcox.com

Qualified. Ireland, 2005
Areas of practice. Privacy and data protection; technology; e-Business; intellectual property; freedom of information.

CAROLINE O’GORMAN
Arthur Cox
T +353 1 618 1190
F +353 1 616 3986
E caroline.ogorman@arthurcox.com
W www.arthurcox.com

Qualified. Ireland, 2012
Areas of practice. Privacy and data protection; freedom of information; technology, intellectual property; commercial contracts.

OLIVIA MULLOLLY
Arthur Cox
T +353 1 618 1160
E olivia.mullooly@arthurcox.com
W www.arthurcox.com

Qualified. Ireland, 2011
Areas of practice. Intellectual property; information technology; data protection; commercial agreements.