



Building Locally
Competing Globally

DATA PROTECTION ACT 1998

POLICY DOCUMENT

PUBLISHED [FEBRUARY 2003]
UPDATED [OCTOBER 2010]

Introduction

The Eight Principles of Data Protection

Principle 1 – Processing personal data fairly and lawfully

Principle 2 – Processing personal data for specified purposes

Principle 3 – Must be adequate, relevant & not excessive

Principle 4 – Personal data must be accurate & up to date

Principle 5 – Must not be kept for longer than is necessary

Principle 6 – Rights of Individuals

Principle 7 – Personal data must be kept secure

Principle 8 – Sending personal data outside the EEA

The Human Rights Act and the Right to Privacy

Individual's Rights

Subject Access

Prevention of processing likely to cause damage or distress

Prevention of processing for purposes of direct marketing

Automated decision making

Compensation

Inaccurate Data

Exemptions

Crime and taxation

Disclosures required by law

Legal advice and proceedings

Confidential References

Management Information

Negotiations

Further exemptions

Enforcement

Complying with the Act

Introduction

The Data Protection Act 1998 (the "Act") came into force on 1 March 2000. It gives effect in UK law to the 1995 EC Data Protection Directive. The Act establishes a framework of rights and duties which are designed to safeguard personal data. This framework balances the legitimate needs of organisations to collect and use personal data for business and other purposes against the right of individuals to respect for the privacy of their personal details.

This policy document is intended as a broad guide to the Act and the implications for Invest NI as a data controller. This policy should be read in conjunction with other guidance issued on Data Protection issues ([available on the intranet](#)). All specific queries regarding data protection matters should be referred to Danny Smyth, Information Governance Manager for guidance.

"Personal data" means data which relates to a living individual who can be identified from the information. This includes any expression of opinion about the individual and any indication of the intentions of Invest NI in respect of the individual. It includes photographs, email messages and images recorded on CCTV. It also covers information identified by reference numbers where a separate list can be used to match the reference numbers to named individuals.

Invest NI's information systems (such as Meridio, CCMS, Goldmine, OaCS) and various other computer databases held within the organisation contain personal data on Invest NI clients, staff, consultants and other information sources. These are also held in manual filing systems such as the off site storage list.

The 1998 Act applies to any processing of personal data held electronically and personal data held in structured manual files. The Freedom of Information Act 2000 amended the Act to include unstructured personal data held by Public Authorities. Processing means obtaining, recording or holding the data or carrying out any operation on the data. It includes collection, organising, adapting and amending the data, storage, retrieval, consultation and use of the data, disclosing and erasure or destruction of the data.

Under the Act Invest NI is deemed to be a Data Controller as an organisation that determines the purposes for which and the manner in which any personal data are, or are to be, processed. As a Data Controller Invest NI must comply with the Act and, in particular, must handle all personal data held in accordance with the data protection principles.

The Eight Principles of Data Protection

There are eight Data Protection Principles (the "Principles") in the Act. All of the principles apply to Invest NI who must comply with them in the processing of personal data. The main purpose of these principles is to protect the interests of the individuals whose personal data is being processed. They apply to everything Invest NI does with personal data, except where an exemption can be claimed.

The Data Protection Act lists the data protection principles in the following terms:

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –
 - (a) at least one of the conditions in Schedule 2 is met, and
 - (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

PRINCIPLE 1 – Processing personal data fairly and lawfully

Principle one prohibits the processing of personal data unless one of the conditions set out in the legislation can be established. In practice, it means that Invest NI must:

- have legitimate grounds for collecting and using the personal data;
- not use the data in ways that have unjustified adverse effects on the individuals concerned;
- be transparent about how we intend to use the data, and give individuals appropriate privacy notices when collecting their personal data;
- handle people's personal data only in ways they would reasonably expect; and
- make sure we do not do anything unlawful with the data.

Schedule 2 of the Act lists the conditions required to process personal data and Schedule 3 lists the conditions for processing sensitive personal data.

The conditions of Schedule 2 are as follows:

- The individual has given his or her consent to the processing;
- The processing is necessary for the performance of or entering into a contract by the data subject;
- The processing is necessary for Invest NI to comply with a legal obligation;
- The processing is necessary to protect the vital interests of the individual;
- The processing is necessary for the exercise of functions of a public nature exercised in the public interest;
- The processing is necessary in order to pursue the legitimate interests of Invest NI or third parties (unless it could prejudice the interests of the individual).

"Sensitive personal data" includes data about a person's ethnic or racial origin, political opinions, religious beliefs, trade union membership, health, sexual life and criminal history whether actual or alleged. Such data can only be processed when one of the ordinary processing conditions listed above and one of the conditions for processing sensitive data listed below are met:

- Having the explicit consent of the individual;
- Being required by law to process the data for employment purposes;
- Needing to process the information in order to protect the vital interests of the data subjects or another;
- Dealing only with individuals who are members of a non profit body such as a political or religious association, TU etc;
- The personal data has already been put in the public domain by the individual;
- Dealing with the administration of justice or legal proceedings.

Consent is not defined in the Data Protection Act. However, the European Data Protection Directive (to which the Act gives effect) defines an individual's consent as "any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed".

The fact that an individual must "signify" their agreement means that there must be some active communication between the parties. An individual may "signify" agreement other than in writing, but organisations should not infer consent if an individual does not respond to a communication – for example, from a customer's failure to return a form or respond to a leaflet.

The Data Protection Act distinguishes between:

- the nature of the consent required to satisfy the first condition for processing; and
- the nature of the consent required to satisfy the condition for processing sensitive personal data, which must be "explicit".

This suggests that the individual's consent should be absolutely clear. It should cover the specific processing details; the type of information (or even the specific information); the purposes of the processing; and any special aspects that may affect the individual, such as any disclosures that may be made.

This type of sensitive information would typically be processed by Invest NI to comply with the Fair Employment legislation in relation to the monitoring of employees. Other examples of the processing of this type of data in Invest NI would be for the purposes of monitoring participants on certain programmes.

PRINCIPLE 2 - Processing personal data for specified purposes

The principle two aims to ensure that organisations are open about their reasons for obtaining personal data, and that what they do with the information is in line with the reasonable expectations of the individuals concerned.

In practice, principle two means that Invest NI must:

- be clear from the outset about why we are collecting personal data and what we intend to do with it;
- comply with the Act's fair processing requirements – including the duty to give privacy notices to individuals when collecting their personal data;
- comply with what the Act says about notifying the Information Commissioner; and
- ensure that if we wish to use or disclose the personal data for any purpose that is additional to or different from the originally specified purpose, the new use or disclosure is fair.

The Act provides two ways in which Data Controllers can specify the relevant purposes:

- in a “privacy notice” given to individuals at the time their personal data is collected; or
- in a notification given to the Information Commissioners Office (ICO).

Invest NI has employed the latter means of notification i.e. given notification to the Commissioner. In reality, of course, members of the public do not check ICO notification entries very often, and as such, in line with best practice recommendations by the ICO, Invest NI has adopted a [privacy notice](#) which complies with the ICO Privacy Notice Code of Practice. This notice is found on the Invest NI website and should be referred to when collecting personal data (either in person or on forms etc).

Principle two says, in effect, that personal data must not be processed for any purpose that is incompatible with the original purpose or purposes for which it was collected.

The interpretation of the Principle two further provides that, in deciding whether any disclosure of personal data is compatible with the purpose or purposes for which the data were obtained, consideration should be given to the purpose or purposes for which the personal data are to be processed by any person to whom they are disclosed. **In other words, would the data subject regard disclosure of their information to someone else as being compatible with the original reason for which they provided the information to Invest NI?**

If you wish to use or disclose personal data for a purpose that was not contemplated at the time of collection (and therefore not specified in a privacy notice), you have to consider whether this will be fair. If using or disclosing the information would be unfair because it would be outside what the individual concerned would reasonably expect, or would have an unjustified adverse effect on them, then you should regard the use or disclosure as incompatible with the purpose you obtained the information for. In practice, you often need to get prior consent to use or disclose personal data for a purpose that is additional to, or different from, the purpose you originally obtained it for.

PRINCIPLE 3 - Personal data must be adequate, relevant and not excessive

Personal data shall be adequate, relevant and not excessive in relation to the purposes for which it is processed. This involves identifying the minimum amount of information required in order to fulfill the purpose(s) and this will be a question of fact in each case. If it is necessary to hold additional information about certain individuals, such information should only be collected and recorded in those cases. That is, if a particular item of information is held on all the individuals which will be used or useful only in relation to some of them, the information is likely to be excessive and irrelevant in relation to those individuals in respect of

whom it will not be used or useful and should not be held in these cases. **It is not acceptable to hold information on the basis that it might possibly be useful in the future without a view of how it will be used.**

Changes in circumstances or failure to keep information up to date may mean that information which was originally adequate becomes inadequate. If data are kept for longer than necessary then they may well be irrelevant and excessive.

PRINCIPLE 4 - Personal data must be accurate and up to date

Personal data shall be accurate and, where necessary, kept up to date. Data are inaccurate if they are incorrect or misleading as to any matter of fact.

The Act provides guidance in interpreting this Principle - basically the principle will not be contravened because of any inaccuracy in personal data if:

- (a) Invest NI has taken reasonable steps to ensure the accuracy of the data, and
- (b) the individuals have notified Invest NI of their view that the data are inaccurate, the data indicate that fact.

It is important to note that by virtue of (a) above it is not enough for Invest NI to say that, because the information was obtained from either the individual or a third party, they had done all that they could reasonably have done to ensure the accuracy of the data at the time. Invest NI may have to go further and take reasonable steps to ensure the accuracy of the data themselves and mark the data with any objections. The extent to which such steps are necessary will be a matter of fact in each individual case and will depend upon the nature of the data and the consequences of the inaccuracy for the data subject.

The second part of the Principle, which refers to keeping personal data up to date, is qualified. Updating is only required "where necessary". The purpose for which the data are held or used will be relevant in deciding whether updating is necessary. For example, if the data were intended to be used merely as an historical record of a transaction between Invest NI and the individual, updating would be inappropriate. To change the data so as to bring them up to date would defeat the purpose of maintaining the historical record. However, sometimes it is important for the purpose that the data reflect the data subjects current circumstances, for example, if the data are used to decide whether to grant credit or confer or withhold some other benefit. In those cases either steps should be taken to ensure that the data are kept up to date, or when the data are used, account should be taken of the fact that circumstances may have changed.

PRINCIPLE 5 - Personal data must not be kept for longer than is necessary

Personal data shall be kept for no longer than is necessary for the purposes for which it is processed. To comply with this principle, Invest NI will need to review their personal data regularly and to delete the information that is no longer required for their purposes. You will need to take account of any professional rules or regulatory requirements that apply. There are various legal requirements and professional guidelines about keeping certain kinds of records – such as information needed for income tax and audit purposes, or information on aspects of health and safety. If Invest NI keeps personal data to comply with a requirement like this, it will not be considered to have kept the information for longer than necessary. There are retention periods set out in the Records Management Policy and these should be strictly adhered to in practice.

If personal data have been recorded because of a relationship between Invest NI and an individual, the need to keep the information should be considered when the relationship ceases to exist. For example, an individual may be an employee who has left the employment of Invest NI however this will not necessarily cause Invest NI to delete all the personal data held on that person. It may well be necessary to keep some of the information so that we will be able to confirm details of their employment for, say, the provision of references in the future or to enable the employer to provide the relevant information in respect of their pension arrangements. It may well be necessary in some cases to retain certain information to enable Invest NI to defend legal claims, which may be made in the future. Unless there is some other reason for keeping them, the personal data should be deleted when the possibility of a claim arising no longer exists, that is, when the relevant statutory time limit has expired.

At the end of the retention period, or the life of a particular record, it should be reviewed and deleted, unless there is some special reason for keeping it. You should only retain a record (rather than delete it) if you still need to hold it. You must be prepared to give subject access to it, and to comply with the data protection principles. If it is appropriate to delete a record from a live system, it should also be deleted from any back-up of the information on that system.

The Act provides that personal data processed only for historical, statistical or research purposes, in compliance with the conditions set out in section 33, may be kept indefinitely.

PRINCIPLE 6 - Rights of Individuals

The rights of individuals are central to this principle. These rights include the following:

- the right of subject access lets individuals find out what information is held about them;
- individuals have a right to prevent processing that is likely to cause damage or distress to themselves or anyone else. They also have the right to claim compensation for damage or distress caused by someone breaking the conditions of the Act;
- rights in relation to automated decision-making mean that significant decisions should not be made about individuals using automatic processing alone. Examples of automated decision making would be job selection procedures such as psychometric testing and CV scanning;
- individuals have the right to prevent processing for direct marketing. Data controllers must not use personal data for direct marketing purposes if the data subject asks them not to;
- individuals have the right to take action to correct, block, erase or destroy data that is inaccurate or contains opinions that are based on inaccurate data.

There may be situations where these rights do not apply, e.g. individuals do not have the right of subject access if it affects the way crimes are detected or taxes are assessed. These are known as exemptions.

PRINCIPLE 7 - Personal data must be kept secure

This principle demonstrates what the Act requires in terms of security for personal data held. In practice, it means that Invest NI must have appropriate security to prevent the personal data it holds being accidentally or deliberately compromised. In particular, the Act requires Invest NI to:

- design and organise security to fit the nature of the personal data held and the harm that may result from a security breach;
- be clear about who in the organisation is responsible for ensuring information security;
- make sure it has the right physical and technical security, backed up by robust policies and procedures and reliable, well-trained staff; and
- be ready to respond to any breach of security swiftly and effectively.

The principle relates to the security of every aspect of processing of personal data. The security measures put in place should seek to ensure that:

- only authorised people can access, alter, disclose or destroy personal data;
- those people only act within the scope of their authority; and
- if personal data is accidentally lost, altered or destroyed, it can be recovered to prevent any damage or distress to the individuals concerned.

The Act does not define the security measures required for compliance. However, Physical and technological security is likely to be essential, but is unlikely to be sufficient of itself. Management and organisational security measures are likely to be equally important in protecting personal data.

It is vital that Invest NI staff understand the importance of protecting personal data; that they are familiar with the organisation's security policy; and that they put its security procedures into practice.

At times Invest NI will use third party "data processors" to process personal data on its behalf. Particular care regarding security is needed because the organisation (and not the data processor) will be held responsible under the Data Protection Act for what the data processor does with the personal data. The Act contains special provisions that apply in these circumstances. It says that, where a data processor is used Invest NI must:

- choose a data processor that provides sufficient guarantees about its security measures to protect the processing it will do on its behalf;
- take reasonable steps to check that those security measures are being put into practice; and
- have in place a written contract setting out what the data processor is allowed to do with the personal data. The contract must also require the data processor to take the same security measures you would have to take if you were processing the data yourself. The standard terms and conditions for CPD procurement cover this requirement. In all circumstances where CPD have not been used for the tender the Invest NI [Third Party Data Processing contract](#) should therefore be used.

PRINCIPLE 8 - Sending personal data outside the European Economic Area

You may transfer personal data to countries within the European Economic Area on the same basis as you may transfer it within the UK. However, you may only send it to a country or territory outside the European Economic Area if that country or territory ensures an adequate level of protection for the rights and freedoms of individuals in relation to processing personal data.

The interpretation to Principle eight provides that an adequate level of protection is one that is adequate in all the circumstances of the case, having regard in particular to:

- (a) the nature of the personal data;
- (b) the country or territory of origin of the information contained in the data
- (c) the country or territory of final destination of that information,
- (d) the purposes for which and period during which the data are intended to be processed,
- (e) the law in force in the country or territory in question,
- (f) the international obligations of that country or territory,
- (g) any relevant codes of conduct or other rules which are enforceable in that country or territory (whether generally or by arrangement in particular cases); and
- (h) any security measures taken in respect of the data in that country or territory.

This is not an exhaustive list.

Schedule 4 of the Act provides for circumstances in which Principle eight does not apply to a transfer. These are where:

- (a) The individual has given their consent to the transfer
- (b) The transfer is necessary:
 - for the performance of a contract between the individual and Invest NI, or
 - for the taking of steps at the request of the individual with a view to them entering into a contract with Invest NI.
- (c) The transfer is necessary:
 - for the conclusion of a contract between Invest NI and a person other than the individual which: is entered into at the request of the individual or is in their interests, or
 - for the performance of such a contract.
- (d) The transfer is necessary for reasons of substantial public interest. The Secretary of State may specify by order the circumstances in which a transfer is to be taken to be necessary for reasons of substantial public interest. No order to this effect has been made to date.
- (e) The transfer:
 - is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),
 - is necessary for the purpose of obtaining legal advice, or
 - is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

- (f) The transfer is necessary in order to protect the vital interests of the data subject.
- (g) The transfer is part of the personal data on a public register and any conditions subject to which the register is open to inspection are complied with by any person to whom the data are or may be disclosed after the transfer.
- (h) The transfer is made on terms that are of a kind approved by the Commissioner as ensuring adequate safeguards for the rights and freedoms of data subjects. It is not the practice of the Commissioner to consider or approve individual draft contracts submitted to him.
- (i) The transfer has been authorised by the Commissioner as being made in such a manner as to ensure adequate safeguards for the rights and freedoms of individual.

A transfer is not the same as the transit of information through a country. Principle 8 will only apply if the information moves to a country, rather than simply passing through it on route to its destination.

The Human Rights Act and the right to privacy

The Human Rights Act 1998 incorporates the European Convention on Human Rights into UK law. It is unlawful for a public body to act in a way that is incompatible with a Convention right. One of these rights is the right to respect for private and family life of living persons (Article 8).

Article 8 of the Convention underpins the European Data Protection Directive, and therefore the Data Protection Act 1998. Article 8 goes further than the Directive however - it does not just cover personal data but also provides a more general right to respect for private and family life. It is broad in scope and covers, for example, the collection, use and exchange of personal data as well as issues such as telephone tapping and the right to be free from pollution.

Article 8 is a 'qualified right' in that it allows a public authority to interfere where that interference is in accordance with law; in pursuit of a legitimate aim; and necessary in a democratic society. It is very important to be alert to the potential effect of Article 8 when considering personal data issues.

Individual's Rights

The Data Protection Act, against the backdrop provided by the Human Rights Act 1998, gives individuals certain rights in respect of personal information held about them by others.

- (a) **Right to subject access** - upon making a request in writing and upon paying the appropriate fee to Invest NI, an individual is entitled to be told

by Invest NI whether they or someone else on their behalf is processing that individuals' personal data, and if so, to be given a description of:

- the personal data;
- the purposes for which they are being processed; and
- those to whom they are or may be disclosed.

The individual is also entitled to have communicated to him in an intelligible form, all the information that forms any such personal data.

This information must be supplied in permanent form by way of a copy, except where the supply of a copy in permanent form is not possible or would involve disproportionate effort, or the data subject agrees otherwise. "Disproportionate effort" is not defined in the Act.

If any of the information in the copy is not intelligible without explanation, the data subject should be given an explanation of that information, e.g. where Invest NI holds the information in coded form which cannot be understood without the key to the code and, subject to third party information referred to below, any information as to the source of those data.

Where a decision significantly affecting a data subject is, or is likely to be, made about that data subject by fully automated means, for the purpose of evaluating matters about that data subject such as his creditworthiness or his reliability he is entitled to be told of the logic involved in the process. In order to obtain this information the individual must specifically request it when making the subject access request by virtue of the Data Protection (Subject Access)(Fees and Miscellaneous Provisions) Regulations 2000 (S.1. No.191).

A data controller may charge a fee for dealing with subject access. Currently, the maximum fee chargeable is £10, or £2 if it is a request for limited information from a credit reference agency. There are special rules that apply to fees for access to manual health records. Invest NI waives the ten pound fee that we can charge for subject access requests.

Invest NI must comply with a subject access request promptly, in other words as quickly as possible, and in any event within forty calendar days of receipt of the request or, if later, within forty days of receipt of:

- the information required to satisfy himself as to the identity of the person making the request to enable him to locate the information which that person seeks; and
- the fee.

If the information requested consists of information as to the physical or mental health of the data subject and Invest NI is not a health professional (as defined in The Data Protection (Subject Access Modification)(Health)

Order 2000 (S.1. No. 413») the information should not be provided unless the appropriate health professional (also defined) has been consulted.

If accidental disclosure of the information held by Invest NI to an individual other than the data subject would not be likely to cause damage or distress to the data subject, Invest NI may rely upon the usual signature of the individual as proof of identity and the information may be sent to an address known to Invest NI as being the address of the person making the request.

If the information is such that its accidental disclosure to an Individual impersonating the data subject would be likely to cause damage or distress to the real data subject, the data controller might reasonably require better proof by, for example, asking the individual to give information which has been recorded as personal data by the data controller and which the individual might be expected to know.

- (b) **Right to prevent processing likely to cause damage or distress** -If an individual believes that a data controller is processing personal data in a way that causes, or is likely to cause, substantial unwarranted damage or substantial, unwarranted distress to them or to another, section 10 of the Act provides that the individual has the right to send a notice to the data controller requiring him, within a reasonable time, to stop the processing (the "data subject notice").

This right to serve a data subject notice applies whether the individual objects to the processing taking place at all, or whether the objection relates specifically to processing for a particular purpose or in a particular way.

When a data controller receives a data subject notice he must, within 21 days, give the individual a written notice stating either:

- that he has complied with the data subject notice, or intends to comply with it; or
- the extent to which he intends to comply with the data subject notice (if at all) and explaining the parts of the data subject notice he considers to be unjustified in any way.

An individual can only serve a data subject notice that relates to personal data in respect of which he is the data subject. However, an individual is not entitled to serve a notice if any of the following conditions of processing apply:

- he has given a valid consent to the processing (although consent may be withdrawn);
- the processing is necessary for the taking of steps, at the data subject's request, with a view to entering into a contract, or the

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

- the processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract;
- the processing is necessary to protect the individual's vital interests (i.e. it is a life or death situation).

The Secretary of State may prescribe additional circumstances where this right is not exercisable. No order has been made to date to this effect.

- (c) **Right to prevent processing for the purposes of direct marketing** – An individual is entitled by written notice, to require a data controller to cease, or not to begin, processing his personal data for the purpose of direct marketing. When a data controller receives such a notice, he must comply as soon as he can. There are no exceptions to this and the data subject may apply to Court for an order if, fails to comply with the notice.

"Direct marketing" is defined in the Act for the purposes of this provision as meaning the communication (by whatever means) of any advertising or marketing material that is directed to particular individuals. The Commissioner regards the term "direct marketing" as covering a wide range of activities, which will apply not just to the offer for sale of goods or services, but also the promotion of an organisation's aims and ideals.

- (d) **Rights in relation to automated decision taking** - An individual is entitled, by written notice, to require a data controller to ensure that no decision which significantly affects that individual is based solely on the processing by automatic means of personal data of which that individual is the data subject. The Act includes specific examples of the purposes for which such automated decision taking might be employed, i.e. evaluating matters relating to the data subject such as his performance, his creditworthiness, his reliability or his conduct. This is not an exhaustive list.

Where no notice has effect and where a decision which significantly affects an individual is based solely on such automatic processing, the data controller must notify the individual that the decision was taken on that basis as soon as reasonably practicable. In addition, within 21 days of receiving such notification, an individual is entitled by written notice (the "data subject notice") to require the data controller to reconsider the decision or to take a new decision on a different basis. Within 21 days of receiving the data subject notice the data controller must give the data subject a written notice specifying the steps the data controller intends to take to comply with the data subject notice.

The Act provides for the exemption from such provisions of certain decisions reached in this way. These are called "exempt decisions". To qualify as an exempt decision certain conditions must be met.

- (e) **Right to take action for compensation** if the individual suffers damage by any contravention of the Act by the data controller - An individual who suffers damage, or damage and distress, as the result of any contravention of the requirements of the Act by a data controller, is entitled to compensation where the data controller is unable to prove that he had taken such care as was reasonable in all the circumstances to comply with the relevant requirement.

"Damage" includes financial loss or physical injury. Unless processing is for the "special purposes", compensation is not payable for distress alone. If the individual can prove that damage has been suffered, the Court may award compensation for any distress that has also been suffered by reason of the breach of the Act.

Damages for distress alone can be claimed where the contravention relates to the processing of personal data for the "special purposes", and which comprise journalistic, artistic or literary purposes. Again, it is a defence for the data controller to prove that he had taken such care as in all the circumstances was reasonably required to comply with the requirement concerned. There are, however, reduced circumstances in which a contravention may occur as processing only for "special purposes" is, in certain circumstances, exempt from all but one of the Data Protection Principles and some sections of the Act.

- (f) **Right to take action to rectify, block, erase or destroy inaccurate data** – A data subject may apply to the Court for an order requiring the data controller to rectify, block, erase or destroy such data relating to that data subject as are inaccurate together with any other personal data relating to the data subject which contain an expression of opinion which the Court finds is based on the inaccurate data.

Data are inaccurate if they are incorrect or misleading as to any matter of fact. A Court may also make such an order if it is satisfied that the data subject has suffered damage by reason of any contravention by a data controller of any of the requirements of the Act in respect of personal data, entitling the data subject to compensation under section 13, and that there is a substantial risk of further contravention in respect of those data in such circumstances.

In either case, the Court may, where it considers it reasonably practicable, order the data controller to notify third parties to whom the data have been disclosed of the rectification, blocking, erasure or destruction. In deciding

whether it is reasonably practicable to require such notification the Court shall have regard, in particular, to the number of persons who would have to be notified.

If the data are incorrect but accurately record the information given to the data controller by the data subject or a third party, the Court may consider the requirements set out in the interpretation of the Fourth Data Protection Principle namely:

- whether the data controller took reasonable steps to ensure that the data were correct, having regard to the purpose or purposes the data were obtained and further processed; and
- if the data subject has already notified the data controller of his view that the data are inaccurate, and whether the data indicate that fact.

If the Court considers that these requirements have been complied with, the Court may, as an alternative, order that the data be supplemented by a Court approved statement of the true facts. If the Court considers that any or all of the above requirements have not been complied with, the Court may make such order as it sees fit.

If the data subject has suffered damage or damage and distress as a result of the data controllers processing of inaccurate data, compensation may be awarded.

Exemptions

The rights and duties set out in the Data Protection Act are designed to apply generally, but there are some exemptions from the Act to accommodate special circumstances. If an exemption applies, then (depending on the circumstances) Invest NI will be exempt from the requirement:

- to grant subject access to personal data; and/or
- to give privacy notices; and/or
- not to disclose personal data to third parties.

Each exemption must be considered on a case-by-case basis because the exemptions only permit departure from the Act's general requirements to the minimum extent necessary to protect the particular functions or activities the exemptions concern.

Different exemptions work in different ways. An exemption may:

- restrict certain rights of individuals in relation to the processing of their personal data; and/or
- limit the duties of organisations when processing that data.

The Act bundles several rights and duties into two groups, and the exemptions tend to work by “disapplying” (blocking) one or both of these groups. The two groups are called the “subject information provisions” and the “non-disclosure provisions”.

The subject information provisions are:

- an organisation’s duty to provide individuals with a privacy notice when their personal data is collected; and
- an individual’s right to make a subject access request.

The non-disclosure provisions are:

- an organisation’s duty to comply with the first data protection principle, but not including the duty to satisfy one or more of the conditions for processing – you must still do this.
- an organisation’s duty to comply with the second, third, fourth and fifth data protection principles;
- an individual’s right to object to processing that is likely to cause or is causing damage or distress; and
- an individual’s right in certain circumstances to have inaccurate personal information rectified, blocked, erased or destroyed.

An exemption from “the non-disclosure provisions” – which would, for example, allow you to disclose personal data that would otherwise be protected from disclosure – is not an automatic exemption from all (or any) of those provisions. This is because an exemption only applies to the extent that the provisions are inconsistent with the disclosure in question. So if you think you may be exempted from any of the non-disclosure provisions, you should consider each of those provisions in turn and decide:

- which, if any, would be inconsistent with the disclosure in question; and
- the extent of the inconsistency.

Crime and taxation

The Act recognises that it is sometimes appropriate to disclose personal data for certain purposes to do with criminal justice or the taxation system. In these cases, individuals’ rights may occasionally need to be restricted.

Personal data is exempt from the non-disclosure provisions if:

- the disclosure is for any of the crime and taxation purposes; and
- applying those provisions in relation to the disclosure would be likely to prejudice any of the crime and taxation purposes.

However, the exemption applies, in any particular case, only to the extent that applying those provisions would be likely to prejudice the crime and taxation purposes. You need to judge whether or not this effect is likely in each case –

you should not use the exemption to justify withholding subject access to whole categories of personal data if for some individuals the crime and taxation purposes are unlikely to be prejudiced.

The Act does not explain “likely to prejudice”. However, the ICO view is that for these exemptions to apply, there would have to be a substantial chance (rather than a mere risk) that complying with the provision would noticeably damage one or more of the crime and taxation purposes. If challenged, Invest NI must be prepared to defend its decision to apply an exemption, to the ICO or the court. Therefore any such decisions should be taken at an appropriately senior level and the reasons for the decision should be documented.

These exemptions do not require disclosure of personal data to the police or to other law enforcement agencies – they merely keep Invest NI within the Data Protection Act if it decides to disclose information in the circumstances in which the exemptions apply.

Disclosures required by law

Personal data is exempt from the non-disclosure provisions if you are required to disclose it:

- by or under any UK enactment;
- by any rule of common law; or
- by an order of a court or tribunal in any jurisdiction.

In these circumstances, the legal obligation overrides any objection the individuals may have. If you know that you are likely to be legally required to disclose certain kinds of personal data, it is good practice to tell individuals about this when you collect the information from them. This is because telling individuals about the legal requirement is compatible with the disclosure of personal data to comply with the requirement.

Legal advice and proceedings

Personal data is exempt from the non-disclosure provisions where the disclosure of the data is necessary:

- for or in connection with any legal proceedings (including prospective legal proceedings);
- for obtaining legal advice; or
- for establishing, exercising or defending legal rights.

You do not have to disclose personal data in response to a request from a third party simply because this exemption applies. You can choose whether or not to apply the exemption to make a disclosure, and you should do so only if you are satisfied that the disclosure falls within the scope of the exemption.

When faced with a request for disclosure, it can be difficult to decide whether the necessity test can be satisfied. You may also be reluctant to make a disclosure of

personal data because of your relationship with the individual. In such circumstances you may decide not to comply with the request, unless obliged to do so under a court order.

Personal data is also exempt from the subject information provisions if it consists of information for which legal professional privilege could be claimed in legal proceedings.

Confidential references

Personal data is exempt from an individual's right of subject access if it comprises a confidential reference that an organisation gives (or is to give) in connection with education, training or employment, appointing office holders, or providing services. The exemption only applies to references given by Invest NI, and not to references received.

Management information

A further exemption applies to personal data that is processed for management forecasting or management planning. Such data is exempt from the subject information provisions to the extent that applying those provisions would be likely to prejudice the business or other activity of the organisation.

Negotiations

Personal data that consists of a record of your intentions in negotiations with an individual is exempt from the subject information provisions to the extent that applying those provisions would be likely to prejudice the negotiations.

Further Exemptions

The exemptions noted in this policy are those which may apply to Invest NI during the course of its business activities. There are other exemptions such as personal data processed for the purposes of making judicial, Crown, or Ministerial appointments or for conferring honours which may also be relevant. It is recommended that you discuss any possibility of applying exemptions with Danny Smyth, Information Governance Manager.

Enforcement

The Information Commissioner's Office is the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The ICO enforces and oversees the Data Protection Act through educating and influencing (promoting good practice and providing information and advice), resolving problems (resolving eligible complaints from people who think their rights have been breached) and enforcing (using legal sanctions against those who ignore or refuse to accept their obligations).

There are a number of tools available to the ICO for taking action to change the behaviour of organisations and individuals within those organisations that collect, use and keep personal information. They include criminal prosecution, non-criminal enforcement and audit. The Information Commissioner also has the power to serve a monetary penalty notice on a data controller.

The tools are not mutually exclusive and the ICO can use them in combination where justified by the circumstances.

The main options are:

- serve information notices requiring organisations to provide the Information Commissioner's Office with specified information within a certain time period;
- issue undertakings committing an organisation to a particular course of action in order to improve its compliance;
- serve enforcement notices and 'stop now' orders where there has been a breach, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law;
- conduct consensual assessments (audits) to check organisations are complying;
- serve assessment notices to conduct compulsory audits to assess whether organisations processing of personal data follows good practice;
- issue monetary penalty notices, requiring organisations to pay up to £500,000 for serious breaches;
- prosecute those who commit criminal offences under the Act; and
- report to Parliament on data protection issues of concern.

COMPLYING WITH THE ACT

The Data Protection Act affects everyone in Invest NI. **All staff should know their responsibilities and help protect the privacy of information about other people.**

Keeping personal information secure

You must adhere to the [10 Key Rules on securing sensitive data](#) which applies equally to electronic and paper based information.

Meeting reasonable expectations of customers and employees

You must:

- only collect the personal information you need for a particular business purpose.
- explain new or changed business purposes to customers and staff and obtain consent or provide an opt-out where appropriate.
- update records promptly, for example, changes of address.
- delete personal information the organisation no longer needs (in line with records management requirements).
- ensure only staff who need access to personal information are authorised to do so.

You must not:

- release customer or employee records without ensuring it meets the requirements of the Data Protection Act – if you do you are committing an offence.

Disclosing personal information over the phone

- Be aware that there are people who will try to trick you to give out personal information.
- To prevent this, always carry out identity checks before giving out personal information.

- Limit the amount of personal information given out over the telephone and ask for written confirmation if necessary.

Notifying under the Data Protection Act

Are you aware that:

- Invest NI has a [notification entry](#) with the ICO about the personal information that it holds?
- you need to monitor changes in business use of personal information and notify the Information Governance Team if appropriate?

Handling requests from individuals for their personal information (subject access requests)

Do you know:

- that people have a right to have a copy of the information that Invest NI holds about them?
- that Invest NI has 40 days to respond?
- what to do if you receive a subject access request?
- what to do if other people's (third party) information is contained in the proposed response?

Always refer to guidance when dealing with subject access requests or for advice on all aspects of handling personal information.

Updated guidance can be found on the Invest NI intranet:

[homepage – resources – access to information – data protection](#)