Data Protection Commissioner

DATA PROTECTION GUIDELINES

GUIDELINES FOR THE PROMOTION OF GOOD PRACTICE

INSURANCE BUSINESS SECTOR

February 2006

These guidelines have been jointly developed by a working group composed of representatives of the Malta Insurance Association, the Association of Insurance Brokers, the Malta Financial Services Authority and the Office of the Data Protection Commissioner.

This consultation process is in line with the obligations of the Data Protection Commissioner who, in terms of article 40(g) of the Data Protection Act, has the function "*to encourage the drawing up of suitable codes of conduct by the various sectors affected by the provisions of this Act*."

There are certain issues which have not been dealt with in these guidelines as they are still grey and require further definition; these and other issues that will arise over time will be addressed and guidelines developed in due course.

However these guidelines provide a good platform for the promotion of good practice within the insurance business sector and assist controllers factor in data protection principles in the operation of their business.

Contents

1 Terminology

The definition of the following terms will assist in the better understanding of these guidelines.

- "data controller" or "controller" refers to the person who alone or jointly determines the means and purposes of the processing of personal data; in the insurance sector this is usually the insurance company, the insurance agent, the insurance sub-agent, the insurance manager or the insurance broker.

- "data subject" refers to a natural person to whom the personal data relates; in the insurance context this includes the policyholder and the insured as defined in the Insurance Business Act (Cap 403) and the proposer.

- "the Act" refers to the Data Protection Act (Cap 440).

2 Processing Operations for Insurance Purposes

These guidelines refer to the processing of personal data which, by its own nature, is inherent to the insurance business sector. These guidelines are therefore intended to cover those processing operations which are related to the sector and not processing of a general nature which applies to all sectors such as, processing of personnel data for employment purposes, processing of data for direct-marketing purposes etc.

The processing operations which are relevant to the insurance business sector are mainly the following:

- preparing and issuing insurance policies
- collecting premiums and submitting other bills
- settling claims and paying other benefits
- reinsurance
- co-insurance
- preventing, detecting and/or prosecuting insurance fraud
- establishing, exercising or defending a legal claim
- meeting another specific legal or contractual obligation
- prospecting new insurance markets
- internal management
- actuarial activities[1].

3 Notification of Processing Operations

Data controllers have an obligation to notify the Data Protection Commissioner with any processing operations as aforesaid[2]. The Commissioner is also to be informed of any new, discontinued or amended processing operations. Notification is to be made on the appropriate form and it is not an annual requirement. However any addition, discontinuation or amendment from the original notification form has to be notified as soon as it occurs, also on the appropriate form.

An annual fee of Lm10 is due by controllers who are obliged to notify their processing operations[3].

4 Consent

In the insurance business sector processing of personal data is normally undertaken on the basis of the consent criterion.

A distinction exists between personal data, processing of which requires the unambiguous consent of the data subject[4], and sensitive personal data, which requires explicit consent[5]. In either case consent must be freely given, specific and informed[6].

Generally consent is sought at each of the following stages:

- Proposal
- Underwriting
- Claims

4.1 Collection of data relating to third party beneficiaries

Where a proposer applies for insurance on behalf of others, personal data is not collected directly from the data subject himself; for example, for motor insurance in relation to named drivers, or family and group travel insurance, the data controller asks questions about individuals who may live or be travelling with the policy holder. The proposer is, in this case, deemed to be acting on behalf of the third party beneficiary and is therefore deemed to have obtained the consent of the data subject for the insurance purpose. Data about third party beneficiaries may not be processed where the third party expressly opposes to such processing.

In cases involving the processing of sensitive personal data, the proposer should be in a position to obtain the explicit consent of the beneficiaries. In such contracts it is the responsibility of the proposer to ensure that such explicit consent has been given by every individual who acts as beneficiary under the said contract. A standard question for the policyholder would be whether to his knowledge any of the named drivers suffers from a medical condition. If, by way of example, a potential insured suffers from poor eye sight it would be the proposer's duty to disclose such matter to the data controller.

The information requirements towards the beneficiaries, imposed by the Act, can be directed to the proposer.

4.2 Claims Stage

A claim form is completed by the collection of personal data required for the claim to be processed. At claims stage the claimant is consenting to the processing of additional personal data that is relevant to his claim.
It may be the case that in relation to a claim a data controller needs to process personal data relating to a person with whom the data controller has no contractual relationship. Where such data relating to the third party is not sensitive personal data and the controller needs to process this data in order to handle the claim of a policyholder, the controller is deemed to have a legitimate interest to process such third party data in order that he may comply with his legal and contractual obligation to handle and settle the claim of the data subject[7].

Where it is necessary for the controller to establish, exercise or defend legal claims in relation to a claim which requires the processing of sensitive personal data, the explicit consent is not required[8].

4.3 Appointing a broker

Insurance brokers are appointed by the proposer seeking insurance to act on his behalf and do everything necessary in his best interest so as to comply with his request for such insurance.

The requirement of consent will apply regardless of whether or not an insurance broker is appointed. Since the broker is appointed by the proposer to act as an intermediary between such proposer and the insurance companies providing the insurance, on appointing a broker the proposer thus signifies his consent to the broker to process personal data for the purpose of providing the proposer with the insurance service that the latter requires; and if the personal data so required is sensitive personal data, such consent shall be explicit. In the above-mentioned cases, the requirement of consent in terms of the Act is deemed to be satisfied and the broker may process the personal data to the extent that this is necessary to provide the proposer with the service requested by him.

4.4 Consent Form

Although there is no obligation at law for consent to be in writing, it is good practice, where consent is required, for such consent to be obtained on a form signed by the data subject. Such form should be drafted in a way so as to enable the controller obtain the informed, freely given and specific consent of the data subject.

4.4.1 Informed Consent

For consent to be valid, the data subject is to be informed in a concise and clear manner on the purpose for processing. Such information will distinguish between essential information and possible “further” information. Essential information needs to be provided at all data collection stages. In determining what is essential information, the controller should provide the data subject with sufficient information

for the latter to be able to give his informed consent at that point in time. "Further" information must be provided where it is necessary to guarantee fair processing having regard to the specific circumstances in which the data are collected.

4.4.2 Freely Given Consent

Where the controller wishes to seek consent for processing of data which is not strictly necessary for the performance of the contract, the consent form must be drawn up in a manner which will distinguish between the consent given for 'mandatory processing' and the consent given for other processing. The data subject will in this way consent for the 'mandatory processing' without prejudicing his right not to consent to other processing.

4.4.3 Specific Consent

As consent should be obtained for specific purposes, the terminology used in the consent form should not be in general terms but has to be specific having regard to the processing purpose.

4.5 Right to Revoke Consent

The data subject may, on compelling legitimate grounds, revoke his consent previously given in regard to the processing of his personal data[9].

Revocation of consent should only be permissible in relation to consent given for processing that is not inherent to the operation of providing the insurance service. Therefore, the term 'compelling legitimate grounds' should not be interpreted in a way so as to legitimise any action which is not acceptable in terms of the insurance contract or in any case of a fraudulent intention of the insured. Therefore an insured may not revoke his consent in any of the following cases where:

- consent is still necessary for the performance of the insurance contract;
- data is being processed for the purpose of preventing insurance fraud;
- the personal data in question is necessary to satisfy the object of the contract; this applies even when the contract has expired but liability thereunder continues to exist;
- the policy covers liability claims arising after the expiry of the policy but referring to an event within the period of the policy *e.g.* contracting an illness after the termination of an employment and of the insurance contract, which illness arises from a work condition present during the period of insurance; and
- the processing of personal data is necessary for the controller to defend himself pending a dispute between the controller and the data subject.

5 Right to Information

Where information needs to be provided to a data subject, such information shall be clear and understandable[10]. Controllers are encouraged to make this information available on-line, in a hard copy and via phone.

It is good practice to provide information in a multi-layered structure.

5.1 Multi-Layered Notices

5.1.1 The Short Notice

As a minimum data subjects are to be provided with the core information namely, the identity of the controller, the purposes of processing and any additional information which, in the particular circumstances of the case, must be provided to ensure fair processing.

This notice should then indicate access to additional information.

5.1.2 The Condensed Notice

Data subjects must at all times be able to access the following information:

- the identity and habitual residence or principal place of business of the controller;
- the purpose of processing;
- the recipients or categories of recipients;
- whether replies to any questions are obligatory or voluntary, as well the possible consequences of failure to reply;
- the possibility of transfer to third parties; and
- the right to access, to rectify and to oppose.

Additionally a point of contact must be given for questions and information on redress mechanisms.

5.1.3 The Full Notice

This layer must provide all information possible on the processing operations by the controller. This is usually captured in a privacy policy.

6 Right of Access

In the absence of exceptional circumstances, the data subject has the right to access his own personal data[11].

Upon receipt of a signed request in writing by the data subject, the data controller is obliged to confirm whether any personal data is processed about that individual. The reply must be given:

- in writing;
- without excessive delay;
- without expense; and
- in an intelligible form.

Where data is so processed, the controller must provide the data subject with the following information:

- the actual personal data which is processed;
- the source of the information;
- the purpose of the processing;
- any recipients or categories of recipients of the data; and
- logic involved in any automatic processing of data relating to the data subject.

This means that, as long as the above information is provided, the right of access does not require the controller to give physical access to the personal data or to provide him with a copy of the data. However the data controller may opt to give physical access or to provide a copy.

In providing the right of access the controller may not reveal personal data of third parties, and the rights of the data subject for access have to be balanced with the fundamental rights and freedoms of others.

6.1 Cases where the right of access does not apply

The right of access shall not be allowed in circumstances where such right, if exercised, would be prejudicial to the rights and freedoms of the controller, for example in view of legal proceedings, whether impending or commenced, between the controller and the data subject[12].

However this exemption from the right of access shall not apply in relation to all personal data, but only to such data, the provision of which, would result to be prejudicial to the controller; in this case the controller has to be able to prove such prejudice. Actual prejudice has to be determined on a case-by-case basis.

Upon cessation of the ground for prejudice the right of access must be re-instated by the data controller immediately.

7 Transfer of Personal Data within a Group

Companies within a group have a separate juridical personality and are separately responsible for the processing of personal data. Therefore a transfer of personal data between members of the same group is equivalent to a transfer of data between different controllers. There may also be a transfer of personal data between insurers and intermediaries.

In cases where the transfer does not involve sensitive personal data, the said transfer is legitimate when the data subject has given his unambiguous consent[13] or when the processing is necessary for the performance of the contract between the data subject and the controller[14] or when the processing is necessary for a purpose that concerns a legitimate interest of the controller or of such third party to whom personal data is provided[15].

Where sensitive personal data is involved and the controller relies on the data subject's explicit consent[16], then such consent obtained for this purpose at underwriting stage would extend to the transfer of such data where such transfer is necessary for insurance purposes.

8 Sharing of Information for the Purpose of Preventing, Detecting or Suppressing Fraud

The processing of personal data for the purpose of preventing, detecting or suppressing insurance fraud may involve the sharing of information between different data controllers in the insurance sector. Such sharing of information is allowed under the Insurance Business Act and thus deemed to be in conformity with the Act where such information sharing is undertaken:

(a) amongst companies authorised to carry on the business of insurance;
(b) amongst companies or persons registered or enrolled under the Insurance Brokers and Other Intermediaries Act;
(c) between insurers and intermediaries; and
(d) between insurers, or intermediaries, or insurers and intermediaries, and the Commissioner of Police,

provided that such exchange is compatible with or reasonably required for the purpose of preventing, detecting or suppressing insurance fraud[17].

Such sharing of information in relation to sensitive personal data is allowed under the Act, on condition that on signing of the contract the data subject is made aware that he is giving his explicit consent to the disclosure of sensitive personal data for the prevention of fraud[18]. Therefore, a proposal form for an insurance contract has to state clearly that the applicant is giving the consent for his data to be disclosed for the prevention of fraud.

9 Criminal Records

Controllers may request a proposer to disclose any data relating to his criminal convictions or to submit a conduct certificate by the Police together with the proposal form. If the proposer has a criminal record and in the opinion of the controller such record constitutes a reasonable ground for refusal of an insurance cover, the controller may opt not to issue such cover[19].

10 Hereditary Diseases and Illnesses Relating to Relatives of a Data Subject

In certain cases, controllers may require information relating to hereditary diseases or illnesses of relatives of the policyholder to assess the risk. This requires the explicit consent of the relatives which is not always possible. On the other hand the right to privacy of the relatives involved should be protected.

This topic is still under discussion between the insurance sector and Data Protection Commissioner with the aim of finding the correct balance.

---

[1] *vide* principle 4.4 of the Council of Europe Recommendation (2002)9 on the protection of personal data collected and processed for insurance purposes.
[2] Article 29 of the Act
[3] LN154 of 2003 Notification and Fees (Data Protection Act) Regulations, 2003, as amended by LN162 of 2004
[4] Article 9(a) of the Act
[5] Article 12(2)(a) of the Act
[6] *vide* definition of consent in article 2 of the Act
[7] Article 9(f) of the Act
[8] Article 13 (c) of the Act
[9] Article 11 of the Act
[10] Article 19 & 20 of the Act
[11] Article 21 of the Act
[12] Article 23(1)(g) of the Act
[13] Article9(a) of the Act
[14] Article 9(b) of the Act
[15] Article 9(f) of the Act
[16] Article 12(2)(a) of the Act
[17] Article 60 of the Insurance Business Act
[18] Article 12(2)(a) of the Act
[19] Article 17 of the Act