Crois Dhearg na hÉireann
Irish Red Cross

DATA PROTECTION POLICY – AREAS & BRANCHES

Background

The Data Protection Acts 1988 and 2003 were introduced in order to regulate the collection, processing, storage and disclosure of personal data that is processed either electronically or manually.

The Irish Data Protection Act 1988 was passed on 13 July 1988 and came into full force on 19 April 1989. This Act established the Irish Data Protection Commission.

The Irish legislation was updated in 2003 by the Data Protection (Amendment) Act. This act incorporates EC Directive 95/46 into Irish law.

Definition of Personal Data

Personal Data is defined very broadly in the Acts. It covers data relating to a living individual who is or can be identified either from the data we have or from the data in conjunction with other information in the possession of Irish Red Cross. The definition is technology neutral. It does not matter how the personal data is stored – on paper, on an IT system or as an image.

The Eight provisions of the Act

The data protection commissioner notes 8 legal responsibilities and states that we must:

Obtain and process the information fairly

This is the fundamental principle of data protection. If your Area/Branch wishes to keep personal information about people, then you must collect the information fairly, and you must process (or use) the information fairly. This means that the person giving the information to an Area/Branch is clear about what use will be made of the information i.e. fundraising, membership, volunteering, and medical.

Keep data only for one or more specified and lawful purposes

You may not keep information about people unless it is held for a specific, lawful and clearly stated purpose. It is therefore unlawful to collect information about people routinely and indiscriminately, without having a sound, clear and legitimate purpose for so doing.

"The data shall have been obtained only for one or more specified explicit and legitimate purposes"
- Section 2(1) (c) (i) of the Act

Each Area/Branch should designate one member to be responsible for processing and storing data. They should include in each file containing information a data statement of their purpose for holding personal data.

Process data only in ways compatible with the purposes for which it was given to you initially

If you obtain personal information for a particular purpose, you may not use the data for any other purpose, and you may not divulge the personal data to a third party, except in ways that are "compatible" with the specified purpose. A key test of compatibility is whether you use and disclose the data in a way in which those who supplied the information would expect it to be used and disclosed.

Keep data safe and secure

The security of personal information is all-important. It will be more significant in some situations than in others, depending on such matters as confidentiality and sensitivity. High standards of security are, essential for all personal information. Both "data controllers" and "data processors" must meet the requirement to keep data secure. Access to this data must be limited to authorised persons only. If you keep written data keep it under lock and key. If the data is held electronically, access should be password protected and it should be encrypted.

Keep data accurate, complete and up-to-date

You must ensure that the personal information you keep is accurate, complete and up-to-date. Apart from ensuring compliance with the Acts, this requirement has an additional importance in that the organisation may be liable to an individual for damages if you fail to observe the duty of care provision in the Act applying to the handling of personal data.

Ensure that the data is adequate, relevant and not excessive

The personal data you keep should be enough to enable you to achieve your purpose, and no more. You do not collect or keep personal information that you do not need, "just in case" a use can be found for the data in the future. You should not ask intrusive or personal questions, if the information obtained in this way has no bearing on the specified purpose for which you hold personal data.

Retain data no longer than is necessary for the specified purpose or purposes

Nowadays information can be kept cheaply and effectively on computer. This requirement places a responsibility on the organisation to be clear about the length of time for which data will be kept and the reason why the information is being retained. In determining how long to retain personal information, regard should be given to both statutory and regulatory obligations. Some finance information must be retained securely for seven years and medical data will also have a retention period set down by the HSE.

If there is no legal reason for retaining personal information, then that information should be routinely deleted. Information should never be kept "just in case" a use can be found for it in the future.

Give a copy of his/her personal data to any individual, on request.

Section 4 of the Data Protection Acts gives an individual a right to obtain a copy of any personal data held by an organisation about him or her. The requester is entitled to

(a) a copy of their data,
(b) a description of the purposes for which it is held,
(c) a description of those to whom the data may be (have been) disclosed
(d) the source of the data unless this would be contrary to public interest

The information includes both data held manually and data held in electronic format.

The requester is only entitled to personal data about themselves. The requested information may make references to third parties i.e. to individuals other than the individual making the access request. When supplying the data the references to third parties should be blocked or deleted so that personal data of another individual is not released inappropriately.

Members who express **opinions** about other members in the course of their membership should be aware that their opinion may be disclosed in an access request (i.e. references, disciplinary procedures, management of performance etc.). Personal data that is classified as the opinion of another person must be provided unless the "opinion" was given on the understanding that it would be treated confidentially. You are also obliged to explain to the data subject the logic used in any automated decision making process where the decision significantly affects the individual and the decision is solely based on the automated process.

Duty of Care

Volunteers controlling or processing the data should take care that their activities do not cause damage or distress to third party individuals by maintaining inaccurate information on files or disclosing personal data to someone who is not entitled to this data. The Society holds data to administer its functions and volunteers are provided with access to that data in order to meet the responsibilities of their roles. Data should not be accessed unless there is a direct business requirement.

Confidential customer or member information must never be discussed with or disclosed to any unauthorised third party, either internally or externally.

Crois Dhearg na hÉireann
Irish Red Cross

Breaches of Data Protection

All allegations of suspected breaches of data protection should be investigated. All complaints in this area from whatever source (e.g. volunteers, staff, management, clients etc.) should be forwarded to the Branch or Area Chairperson for forwarding to the Secretary General. Any breach of trust with regard to confidentiality of personal data will be treated as serious misconduct and will lead to disciplinary steps being taken against the perpetrator.

Storage of Personal Data

Personal data must only be kept for the length of time necessary to perform the processing for which it was collected. This applies to both electronic and non-electronic personal data. Data, in general, can be stored in a wide range of formats and can be retained for various periods, depending on the type and content.

The data must be routinely reviewed to ensure that it is accurate and up to date and if data is amended, any older copies should be securely destroyed. This includes committee forms, membership contact lists, duty attendance lists and lists of clients availing of our community services.

Where data is being stored off IRC servers (e.g. on personal PCs and laptops), it is recommended that encrypted storage devices are used. Free encryption security software could include http://www.truecrypt.org/

Crois Dhearg na hÉireann
Irish Red Cross

Holding of Medical data

Medical data is highly privileged information. This data may only be held following a patient care scenario where Red Cross personnel having treated a person produce an ACR or PCR. The information is set down on paper and stored in the locked box in each ambulance. The information contained in the locked box will be retrieved only by the person who completed the information or given with the injured parties' permission to a medic in an emergency situation. Once back at base the information must be sent immediately by registered post to the National Office of the Irish Red Cross. The information will then be held in a secure fire proof safe to be reviewed annually by PHECC. The information is to be held for a period of five years. The information may not be passed electronically.

Medical incidents and real life incidents are sometimes used as part of training scenarios or competitions. Also as part of EMT registration, the EMT must maintain a log of patient contacts. It is important that in these scenarios, no information that could identify a patient is recorded or used.

Subject Access

All subject access requests under the Data Protection Act guidelines should be handled by the designated Data Protection Officer of the Irish Red Cross.

The access request must made be in writing, which can include email or text message. The individual may be asked to provide proof of identity and reasonable information to locate any personal data. The information must be supplied to the requester within 40 calendar days so if such a request is received, it should be forwarded immediately to the Secretary General.