

Quality Control & Compliance Initiative

DATA PROTECTION POLICY

Author:	Phonovation Quality Control Group Gavin Carpenter
Effective Date:	19 th Nov 2013
Revised:	20 th Jan 2015
Revised by:	Pedro Quintas
To:	All Phonovation Staff

This document is publicly available to any staff member on the following network path:

<File:\\srvadmdc00\dev & it\Quality Control\QC - Phonovation Data Protection Policy.docx>

Data Protection Policy

Introduction

At Phonovation privacy and data protection rights are very important to us.

Phonovation is registered under the **Data Protection Acts 1988 - 2003** with the registration number **1736/A** as an authorized Electronic Communications Network provider and all personal data will be maintained in accordance with the obligations of that Act.

Data Protection is the safeguarding of the privacy rights of individuals in relation to the processing of personal data, in both paper and electronic format. The Data Protection Acts 1988 and 2003 (the “Data Protection Acts”) lay down strict rules about the way in which personal data and sensitive personal data are collected, accessed, used and disclosed. The Data Protection Acts also permit individuals to access their personal data on request, and confer on individuals the right to have their personal data amended if found to be incorrect.

This document outlines Phonovation’s policy to help ensure that we comply with the Data Protection Acts.

Inquiries about this Data Protection Policy should be made to: **Privacy Officer, Quality Control & Compliance, Phonovation, 8 Clarinda Park North, Dun Laoghaire, Co, Dublin.**

Data Protection Policy

Purpose of this policy

This policy is a statement of Phonovation's commitment to protect the rights and privacy of individuals in accordance with the Data Protection Acts.

Individuals' Responsibilities

Any staff member of Phonovation who is involved in the collection, storage or processing of personal data has responsibilities under the legislation:

Any staff member involved in the processing/storing of personal data should make sure;

- to obtain and process personal data fairly.
- to keep such data only for explicit and lawful purposes.
- to disclose such data only in ways compatible with these purposes
- to keep such data safe and secure.
- to keep such data accurate, complete and up-to-date.
- to ensure that such data is adequate, relevant and not excessive.
- to retain such data for no longer than is necessary for the explicit purpose.
- to give, on request, a copy of the data to the individual to whom they relate, such a request is known as an ACCESS REQUEST (sample access request letter is attached in Appendix II)

Any data access requests received should be forwarded immediately to the Quality Control & Compliance Department.

Individual Rights

The individuals for whom Phonovation stores personal data have the following rights:

- to have their personal data obtained and processed fairly
- to have personal data kept securely and not illegitimately disclosed to others.
- to be informed of the identity of the Data Controller and of the purpose for which the information is held.
- to get a copy of their personal data.
- to have their personal data corrected or deleted if inaccurate.
- to prevent their personal data from being used for certain purposes: for example, one might want to have the data blocked for research purposes where it is held for other purposes.
- under Employment Rights, not to be forced to disclose information to a prospective employer. No one can force another person to make an access request, or reveal the results of an access request, as a condition of recruitment, employment or provision of a service. Where vetting for employment purposes is necessary, this can be facilitated where the individual gives consent to the data controller to release personal data to a third party.
- It should be noted that under the Freedom of Information Acts (1997 and 2003) records containing personal information may be released to a third party, where the public interest so requires.

Principles of the Acts

Phonovation will administer its responsibilities under the legislation in accordance with the eight stated data protection principles outlined in the Act as follows:

1. Obtain and process information fairly.

Phonovation will obtain and process personal data fairly and in accordance with the fulfilment of its functions.

2. Keep data only for one or more specified, explicit and lawful purposes.

Phonovation will keep data for purposes that are specific, lawful and clearly stated and the data will only be processed in a manner compatible with these purposes.

3. Use and disclose data only in ways compatible with these purposes.

Phonovation will only disclose personal data that is necessary for the purpose/s or compatible with the purpose/s for which it collects and keeps the data.

4. Keep data safe and secure.

Phonovation will take appropriate security measures against unauthorised access to, or alteration, disclosure or destruction of, the data and against their accidental loss or destruction. Phonovation is aware that high standards of security are essential for all personal data.

5. Keep data accurate, complete and up-to-date.

Phonovation will have procedures that are adequate to ensure high levels of data accuracy. Phonovation will examine the general requirement to keep personal data up-to-date. Phonovation will put in place appropriate procedures to assist staff in keeping data up-to-date.

6. Ensure that data are adequate, relevant and not excessive.

Personal data held by Phonovation will be adequate, relevant and not excessive in relation to the purpose/s for which it is kept.

7. Retain data for no longer than is necessary for the purpose or purposes for which they are kept.

Phonovation has a policy on retention periods for personal data. Please see Data Retention Policy.

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

Phonovation will have procedures in place to ensure that data subjects can exercise their rights under the Data Protection legislation.

Roles/Responsibilities of Phonovation

Phonovation has overall responsibility for ensuring compliance with the Data Protection legislation. However, all employees of Phonovation who collect and/or control the contents and use of personal data are also responsible for compliance with the Data Protection legislation. Phonovation will provide support, assistance, advice and training to all relevant Departments, Offices and staff to ensure it is in a position to comply with the legislation.

Phonovation is registered as a Data Controller in compliance the Act and the following roles are included in the registration,

Contact Person: Ann Vines, Privacy Officer, Quality Control & Compliance

Compliance Person: Ann Vines, Privacy Officer, Quality Control & Compliance

Procedures and Guidelines

This policy supports the provision of a structure to assist in Phonovation's compliance with the Data Protection legislation, including the provision of best practice guidelines and procedures in relation to all aspects of Data Protection.

Review

This Policy will be reviewed regularly in light of any legislative or other relevant indicators.

Appendix I

Definitions

The following definitions are taken from the Data Protection Acts 1998 and 2003

Full copies of the act are available at the Data Protection Commissioner web site www.dataprotection.ie.

Personal data means data relating to a living individual who is or can be identified either from the data or from 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 means personal data as to:

- (a) The racial or ethnic origin, the political opinions or the religious or philosophical beliefs of the data subject.
- (b) whether the data subject is a member of a trade-union.
- (c) the physical or mental health or condition or sexual life of the data subject.
- (d) the commission or alleged commission of any offence by the data subject, or
- (e) any proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings.