Personal Data Security Breach Code of Practice

[Approved by the Data Protection Commissioner under Section 13 (2) (b) of the Data Protection Acts, 1988 and 2003]

1.The Data Protection Acts 1988 and 2003 impose obligations on data controllers [1] to process personal data entrusted to them in a manner that respects the rights of data subjects to have their data processed fairly (Section 2(1)).Data controllers are under a specific obligation to take appropriate measures to protect the security of such data (Section 2(1)(d)).

This Code of Practice does not apply to providers of publicly available electronic communications networks or services.[2]

2.This Code of Practice addresses situations where personal data has been put at risk of unauthorised disclosure, loss, destruction or alteration. The focus of the Office of the Data Protection Commissioner in such cases is on the rights of the affected data subjects in relation to the processing of their personal data.

3. Where an incident gives rise to a risk of unauthorised disclosure, loss, destruction or alteration of personal data, in manual or electronic form, the data controller must give immediate consideration to informing those affected.[3] Such information permits data subjects to consider the consequences for each of them individually and to take appropriate measures. In appropriate cases, data controllers should also notify organisations that may be in a position to assist in protecting data subjects including, where relevant, An Garda Síochána, financial institutions etc.

4. If the data concerned is protected by technological measures such as to make it unintelligible to any person who is not authorised to access it, the data controller may conclude that there is no risk to the data and therefore no need to inform data subjects. Such a conclusion would only be justified where the technological measures (such as encryption) were of a high standard.

5.All incidents of loss of control of personal data in manual or electronic form by a data processor must be reported to the relevant data controller as soon as the data processor becomes aware of the incident.

6.All incidents in which personal data has been put at risk should be reported to the Office of the Data Protection Commissioner as soon as the data controller becomes aware of the incident, except when the full extent and consequences of the incident has been reported without delay directly to the affected data subject(s) **and** it affects no more than 100 data subjects **and** it does not include sensitive personal data or personal data of a financial nature.[4]In case of doubt- in particular any doubt related to the adequacy of technological risk-mitigation measures - the data controller should report the incident to the Office of the Data Protection Commissioner.

7.Data controllers reporting to the Office of the Data Protection Commissioner in accordance with this Code should make initial contact with the Office within two working days of becoming aware of the incident, outlining the circumstances surrounding the incident. This initial contact may be by e-mail (preferably), telephone or fax and must not involve the communication of personal data. The Office of the Data Protection Commissioner will make a determination regarding the need for a detailed report and/or subsequent investigation based on the nature of the incident and the presence or otherwise of appropriate physical or technological security measures to protect the data.

8. Should the Office of the Data Protection Commissioner request a data controller to provide a detailed written report of the incident, the Office will specify a timeframe for the delivery of the report based on the nature of the incident and the information required. Such a report should reflect careful consideration of the following elements:

- the amount and nature of the personal data that has been compromised;
- the actionbeing taken to secure and / or recover the personal data that has been compromised;
- the action being taken to inform those affected by the incident or reasons for the decision not to do so;
- the action being taken to limit damage or distress to those affected by the incident;
- a chronology of the events leading up to the loss of control of the personal data; and the measures being taken to prevent repetition of the incident.

9. Depending on the nature of the incident, the Office of the Data Protection Commissioner may investigate the circumstances surrounding the personal data security breach. Investigations may include on-site examination of systems and procedures and could lead to a recommendation to inform data subjects about a security breach incident where a data controller has not already done so.If necessary, the Commissioner may use his enforcement powers to compel appropriate action to protect the interests of data subjects.

10. Even where there is no notification of the Office of the Data Protection Commissioner, the data controller should keep a summary record of each incident which has given rise to a risk of unauthorised disclosure, loss, destruction or alteration of personal data. The record 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 Office of the Data Protection Commissioner. Such records should be provided to the Office of the Data Protection Commissioner upon request.

11.This Code of Practice applies to all categories of data controllers and data processors to which the Data Protection Acts 1988 and 2003 apply.

How to Notify The Office of the DP Commissioner

E-Mail - dpcbreaches@dataprotection.ie

Phone - 1890 252231(lo-call); 00 353 (0) 57 8684800

Fax- 00 353 (0) 57 8684757

Footnotes:

[1] Unless otherwise indicated, terms used in this Code – such as "personal data", "sensitive personal data", "data controller", "data processor" – have the same meaning as in the Data Protection Acts 1988 and 2003.

[2]The European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011 (SI 336 of 2011) place specific obligations on providers of publicly available electronic communications networks or services to safeguard the security of their services.Further information is available in the Guidance Note that accompanies this Code of Practice.

[3] Except where law enforcement agencies haverequested a delay for investigative purposes.Even in such circumstances consideration should be given to informing affected data subjects as soon as the progress of the investigation allows.

[4] '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.