ANGLING COUNCIL IRELAND
DATA PROTECTION BREACH
CODE OF PRACTICE

At ACI privacy and data protection rights are very important to us. We have adopted the Data Protection Breach Code of Practice

This Code of Practice will be used by ACI and member federations. It is a statement of ACI commitment to protect the rights and privacy of individuals in accordance with the Data Protection Acts.

Angling Council Ireland

DATA PROTECTION SECURITY BREACH CODE OF PRACTICE

The Angling Council of Ireland has adopted the Personal Data Security Breach Code of Practice.

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:

· a chronology of the events leading up to the loss of control of the personal data;
· the amount and nature of the personal data that has been compromised;
· the action being 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; 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.

29 July 2011

---

[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 have requested 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.

Breach Notification Guidance

The Data Protection Commissioner has approved a personal data security breach Code of Practice to help organisations to react appropriately when they become aware of breaches of security involving customer or employee personal information. In the public sector, guidance from the Department of Finance on data security also advises departments and agencies to report data breaches immediately to this Office. **The Code of Practice does not apply to providers of publicly available electronic communications networks or services.** This is because 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. These obligations are dealt with separately below.

Notification of data security breaches to the Office of the Data Protection Commissioner allows us to advise organisations, at an early stage, how best to deal with the aftermath of a disclosure and how to ensure that there is no repetition. It also allows us to reassure members of the public that we are aware of the problem and that the organisation in question is taking the issue seriously.

Applying the Personal Data Security Breach Code of Practice

Organisations confronted with a breach of security affecting personal data should study the Code of Practice carefully. Some key considerations in relation to the application of the terms of the Code are set out below. The Office of the Data Protection Commissioner will be happy to offer further advice to organisations about how best to apply the terms of the Code. Contact details for the Office are set out at the end of this guidance note.

Paragraph one of the Code of Practice sets out the legal obligation to process personal data fairly and to take appropriate security measures to protect it.

Paragraph two refers to the need to focus on the rights of data subjects where their personal data has been put at risk.

Paragraph three states that data controllers who have experienced an incident giving rise to a risk of unauthorised disclosure, loss, destruction or alteration of personal data must give immediate consideration to notifying the affected data subjects. As the Code states, "this permits data subjects to consider the consequences for each of them individually and to take appropriate measures." The consequences may include the potential for fraud / identity theft, but it may also involve the potential for damage to reputation, public humiliation or even threats to physical safety. The Data Protection Acts give individuals the right to exercise control over how their data is used. A breach of personal data security may compromise that right. Notifying data subjects is a remedial measure intended to redress the balance and restore some measure of knowledge and control.

The information communicated to data subjects should include information on the nature of the personal data breach and a contact point where more information can be obtained. It should recommend measures to mitigate the possible adverse effects of the personal data breach. If the affected data subjects are not immediately identifiable, public notification may be the most appropriate means of communication, for example through the media or through a website. Data controllers should consider whether the method of notification adopted might increase the risk of harm to the data subjects.

Paragraph three of the Code also advises that data controllers should notify organisations that may be in a position to assist in protecting data subjects and mentions An Garda Síochána and financial institutions. Depending on the circumstances, other

examples could include IT experts that can offer containment advice or internet companies that may assist in removing relevant cached links from their search engines. As with all other aspects of the Code, the Office of the Data Protection Commissioner is happy to offer advice in this regard.

Paragraph four notes that there may be circumstances where the data controller may reasonably conclude that there is no risk to personal data due to the adoption of high-quality technological measures that effectively make the data inaccessible. For example, personal data stored on an encrypted laptop with secure access controls may be considered inaccessible in practice and the Office of the Data Protection Commissioner considers that the loss of such a device would not normally involve a risk to the personal data stored on it. However the strongest encryption software [1] is useless if the access password is stored with the device or if the password is weak [2]. Other access controls (such as biometric identifiers, swipe cards, tokens etc) may further strengthen security, particularly when used in combination with a complex password.

Paragraph five of the Code of Practice states that a data processor must report breaches of personal data security to the relevant data controller as soon as they become aware of the incident. This duty should be reflected in appropriate contracts signed between data controllers and data processors. The data controller should then follow the steps set out in the Code.

Paragraph six of the Code of Practice states that all incidents in which personal data has been put at risk should be reported to the Office of the Data Protection Commissioner. The only exceptions are when the data subjects have already been informed **and** the loss affects no more than 100 data subjects **and** the loss involves only non-sensitive, non-financial personal data. It should be noted that the fact that a data controller has notified the Office of the Data Protection Commissioner of a loss of control of personal data does not necessarily imply that a breach of the Data Protection Acts 1988 and 2003 has taken place. The Code also makes clear that if a doubt exists - especially whether the technological measures protecting the data are such as to permit a reasonable conclusion that the personal data has not been put at risk - the matter should be reported to the Office of the Data Protection Commissioner.

Paragraph seven of the Code of Practice sets a timeframe of two days for a data controller to inform the Office of the Data Protection Commissioner once the data controller has become aware that personal data has been put at risk. Complex personal data security breach incidents may take a considerable period of time to fully investigate and resolve. All that is required is initial contact with the Office describing the facts as they are known and the steps being taken to address those facts. Personal data should not be included in such reports to the Office of the Data Protection Commissioner and it is a matter for the data controller to decide the most secure method of contact, based on the nature of the information to be imparted.

Paragraph eight of the Code of Practice sets out the elements to be included in any formal report that may be sought by the Office of the Data Protection Commissioner. The elements set out in paragraph eight should also be considered when preparing to notify data subjects directly of a personal data security breach incident. The Office may seek other documents in addition based on the circumstances surrounding the incident. The Office will also set a timeframe for the delivery of a detailed report based on the nature of the incident and extent of the information required.

Paragraph nine of the Code of Practice states that the Data Protection Commissioner may launch a detailed investigation depending on the nature of the personal data security breach incident. Such investigations may produce a list of recommendations for the

attention of the relevant data controller. Responsible data controllers cooperate willingly with the Commissioner's investigations and are happy to comply with any recommendations he may issue. However, in rare cases in which such compliance is not forthcoming, the Commissioner may use his legal powers to compel appropriate actions.

Even if the Office of the Data Protection Commissioner is not notified, **paragraph ten** of the Code of Practice states that data controllers should keep centrally a brief summary record of each personal data security breach incident with an explanation of the basis for not informing the Office of the Data Protection Commissioner. The purpose of this record is to allow the Office of the Data Protection Commissioner to check compliance with the Code of Practice during audits. It also allows the Office to search for patterns indicating problems within particular organisations or sectors.

Paragraph eleven of the Code of Practice is self-explanatory, stating simply that the Code applies to all categories of data controllers and data processors to which the Data Protection Acts apply.

Obligations on providers of publicly available electronic communications networks or services

As mentioned above, 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. At a general level, such undertakings are required to have in place appropriate **technical** and **organisational** measures to keep personal data safe and secure. More specifically, providers of publicly available electronic communications networks or services are required to:

- have a security policy in place (and be in a position to demonstrate that the security policy has been implemented and kept relevant);
- ensure that personal data can only be used by **authorised** personnel for **authorised** purposes; and
- protect personal data against unlawful use or access.

In case of any particular risk to the security of the network, providers of publicly available electronic communications networks or services must provide information to subscribers **without delay** about the risks and any possible remedies (including the likely costs involved) even where the proposed measures are outside the direct control of the undertaking.

In case of a personal data security breach affecting even one individual, providers of publicly available electronic communications networks or services must **without undue delay:**

- notify the Office of the Data Protection Commissioner of the breach (even in circumstances where it considers the data would be unintelligible to third parties) including a description of the measures to be taken to address the breach; and
- notify any individual that may be adversely affected by the breach.

It is not necessary to notify individuals if the Office of the Data Protection Commissioner is satisfied that the data would be unintelligible to third parties. The Commissioner can require an undertaking to notify individuals if the undertaking does not consider it necessary. Any notification to individuals affected by a personal data security breach must contain:

- an outline of the breach;
- a contact point for obtaining more information; and
- recommended measures to mitigate any possible adverse effects from the breach.

Additionally providers of publicly available electronic communications networks or services must maintain an inventory of personal data breaches which can be checked by the Office of the Data Protection Commissioner.

Failure to comply with these obligations can result in a criminal prosecution with fines of up to €5,000 and on indictment €250,000 per offence.

"Prevention is better than Cure"

Following the steps outlined in the Code of Practice following a data security breach is no substitute for the proper design of systems to secure personal data from accidental or deliberate disclosure. Our general advice on data security is here. But we accept that, even with the best-designed systems, mistakes can happen. As part of a data security policy, an organisation should anticipate what it would do if there were a data breach. Some questions you might ask yourself:

· What would your organisation do if it had a data breach incident?

· Have you a policy in place that specifies what a data breach is? (It is not just lost USB keys/disks/laptops. It may include any loss of control over personal data entrusted to organisations, including inappropriate access to personal data on your systems or the sending of personal data to the wrong individuals).

· How would you know that your organisation had suffered a data breach? Does staff at all levels understand the implications of losing personal data?

· Has your organisation specified whom staff tell if they have lost control of personal data?

· Does your policy make clear who is responsible for dealing with an incident?

· Does your policy meet the requirements of the Data Protection Commissioner's approved Personal Data Security Breach Code of Practice?

How to Notify Us

E-Mail - dpcbreaches@dataprotection.ie

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

Fax- 00 353 (0) 57 8684757

[1] the standard of encryption required to adequately secure data changes with advances in technology. Whole-disk encryption of 256-bit strength should meet the requirement at present.

[2] a strong password would typically be 14 characters long, contain a random selection of letters, numbers and symbols and be impossible to guess