Meeting the Requirements

Reporting Data Breaches

PECYN CYMORTH LLYWODRAETHU GWYBODAETH CYMRU

WELSH INFORMATION GOVERNANCE TOOLKIT

Introduction

A personal data breach (information incident) means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data. All incidents and near misses should be reported, recorded and appropriately managed so that where incidents do occur, the damage from them is minimised and lessons are learnt from them.

The organisation should be aware that the GDPR has introduced a duty on all organisations to report certain types of data breaches to the Information Commissioner's Office (ICO) and the individuals affected. Certain incidents must be reported within 72 hours of the organisation becoming aware of the breach. If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you must also inform those individuals without undue delay.

The ICO website has a number of useful resources for organisations including pages on 'Security' and 'Personal data breaches'.

How do we reach Attainment Level 1?

Information incidents are not always apparent, for example, a computer stolen during a burglary may be seen as merely a hardware issue. However, the information contained on the computer, especially sensitive information, can undermine the security and good reputation of the organisation if disclosed to those not authorised to see it. Other incidents should also be taken into account, for example, an attempt to access confidential information by an unauthorised person; a software malfunction; etc.

The organisation should ensure staff are made aware of their responsibility and are confident to spot an IG related incident and know how to report the incident to the appropriate level by ensuring supporting policies and procedures are in place and made available to staff.

Advice and guidance may be sought from the organisations' appointed Data Protection Officer (DPO). The DPO is responsible for liaising with the ICO regarding any breaches. See the 'ICO pages on reporting a breach'. Policies and procedures should set out who, when, how and what to include when reporting a breach to the ICO, the data subject and Welsh Government. Organisations need to inform individuals without undue delay should a breach occur that is likely to result in a high risk to the rights and freedoms of individuals.

GDPR requires organisations to document the facts relating to the breach, its effects and remedial actions taken. This is part of the organisation's overall obligation to comply with the accountability principle. As with any security incident, you should investigate whether the breach was a result of human error or a systematic issue and see how a recurrence can be prevented; whether this is through better processes, further training or corrective steps.

How do we reach Attainment Level 2?

All IG related incidents and near misses should be reported and documented internally through the incident management system. On becoming aware of a breach, organisations should try to contain it and assess the potential adverse consequences for individuals, based on how serious or substantial these are, and how likely they are to happen. Any trends should be identified and escalated to the DPO as necessary.

To enable organisations to effectively manage information incidents and near misses, a clear defined procedure, in compliance with the GDPR requirements, should be developed and be made available to all staff. This procedure should outline the steps to be taken when dealing with a possible incident including the investigation stages and guidelines provided to staff on how to identify an incident. They should form part of the organisation's Business Continuity Plan and where relevant they should be read in conjunction with one another. The organisation should ensure staff who implement measures to manage damage control are appropriately trained.

Procedures should have a clear a process to follow, including reviewing the breach, allowing discussion and reflection in the event of an incident. The review should involve all disciplines of staff and the process should be carried out avoiding the allocation of blame. A culture of blame is not conducive to improvements being made; lessons can usually be learnt from any identified shortcomings, allowing improved processes for the future. Where applicable, new countermeasures and procedures should be put into place to avoid a repetition of the event.

On reflection of an incident, an action plan should be developed having identified any areas of risk, the risks should be weighed against the likelihood of the threatened risk actually occurring. For example, the assessment may identify a risk of burglary, the question to be asked is whether this a high risk, a medium risk or a low risk.

How do we reach Attainment Level 3?

The organisation should ensure that lessons learnt, and the outcome of IG incidents are effectively communicated to the relevant Board/Committee to ensure appropriate oversight. Lessons learnt should also be shared with staff in order to improve change in future processes throughout the organisation.

Policies and procedures should be regularly reviewed with regular checks are made to ensure procedures are up to date, relevant and work in practice.

Supporting Resources

ICO Guidance on Security

ICO Guidance on Personal Data Breaches

ICO - Report a Data Breach

Summary Requirement

Attainment Level	Summary Requirement
1	There are supporting policies and procedures available to inform individuals of the reporting structure of any Information Governance related incidents. Such policies and procedures also detail the requirements around the reporting of data breaches to the ICO, data subjects and Welsh Government (when required). These are made easily available to staff so they are aware of their responsibilities
2	IG related incidents and near misses are appropriately documented and managed
3	Improvements are made to reduce the chance of re-occurrence and are reported to the Board. A review process is in place to ensure the notification procedure remains relevant and works in practice