WelshBoxing
BocsioCymru

Data Breach Policy

This policy covers what to do when a Data Breach occurs and will be issued to all present staff and Board athletes and new staff and Board athletes at time of induction.

Contents

1. What is a Data Breach?

Organisations which process personal data must take appropriate measures against unauthorised or unlawful processing and against accidental loss, destruction of or damage to personal data. Sometimes, these steps may fail, leading to personal information being accessed by, or at risk of being accessed by people without authorisation.

When this happens, a Data Breach is said to have occurred. Data Breaches can occur in a number of ways:

Data Breach	Examples
Loss or theft of data or equipment on which data is stored	Losing a laptop with Time Credit member information on it Having a mobile phone with contacts saved on it stolen
Inappropriate access controls allowing unauthorised use	Someone obtaining your password to Welsh Boxing's online services, such as the Online Reporting Tool Someone accessing material on a laptop that has been left logged in.
Equipment failure	A laptop breaking when it has athlete's data saved on its local hard drive The loss of information by the failure of an online server's hard drive
Human error	Posting athletes information to the wrong person Uploading athletes to the wrong group on the Online Reporting Tool
Unforeseen circumstances such as a fire or flood	Destruction of personal information in a filing cabinet in an office fire.
Hacking attack	Hackers accessing the Online Reporting Tool The use of keyboard recorders within malware installed on a computer revealing passwords and account details.

'Blagging' offences where information is obtained by deceiving the organisation who holds it	Someone posing as Time Credit Lead telephoning an office to get personal information. Responding to a 'phishing' email and providing personal information

There's no assumption that one type of data breach is more 'damaging' than another. Each individual breach will be assessed against the degree of risk posed by the information at risk and processed as such.

Data Breaches where a Supplier or Third party are Involved

It is possible that personal information that Welsh Boxing is responsible for is breached by a service provider, who are obligated to contact us to tell us as soon as they discover it. Welsh Boxing still needs to consider this a data breach itself and undertake the steps here.

2. What do to when a Data Breach Occurs

Regardless of your role within Welsh Boxing, or how the Data Breach occurred, it's essential than anyone encountering a Data breach report it as soon as possible.

Data breaches may require us to notify the Information Commissioners Office within 72 hours, so it's essential to act fast.

If you encounter a Data breach, you need to do four things:

1. Email and telephone the Chief Executive on their mobile. He will start a Data Breach Incidence process.

2. Inform your line manager.

3. Start recording the process – your notes and records may help with the response and evaluation.

4. Consider are there any steps you can take reduce the risk? – for example, searching for a lost laptop, reporting its theft to the police. Discuss these with the Chief Executive.

3. Starting a Data Breach Incidence Process

In the first instance, the Chief Executive will assess the risk to those individuals to whom their information has gone missing. The Chief Executive will need to know:

- how and when the data breach has occurred
- what personal information has gone missing
- how many people does it affects
- what the risks and privacy issues are to those whose information has gone missing if it is accessed by someone
- if the personal information cover any of the 'special categories' of information under GDPR? (race, ethnicity, health, sexual orientation or political views

The initial priority is to assess the risk the data breach presents, and what steps are needed to contain or recover the information.

If there is minimal risk to individuals to whom the information relates to then the Chief Executive will notify the Board, take the necessary steps to manage the breach, and launch an evaluation and wrap up process to avoid the breach occurring again. At all stages, the Chief Executive will communicate directly with the Chair and the Board.

Data mobilizing strategy

If the risk presented to individuals is moderate to high, unknown, or the information includes that considered a special category by GDPR then the Chief Executive will convene a Data Breach Incident Group.

GDPR requires all Data Breaches to be recorded, regardless of size or impact. The Chief Executive will document the facts relating to the breach, its effects and the remedial action taken.

4. Convening a Data Breach Incidence Group

The Data Breach Incident Project Group will consist of:

- The Chief Executive
- Performance Director
- Any individuals requested by the Chief Executive or other athletes of the group

ICO requires data breaches to be reported within 72 hours of being reported, so it's vital that the data breach is reported and the Response Group convened as quickly as possible to ascertain the need to report the breach.

The group will meet initially meet over internet or phone conference call within 1 working day of the report of the breach, and then at a frequency required to manage the process effectively. This may mean convening the meeting outside of normal working hours.

The purpose of the group is to consider:

- Decide on who should take the lead on investigating the breach and ensure they have the appropriate resources.

- Establish who needs to be made aware of the breach and inform them of what they are expected to do to assist in the containment exercise.

Containment may include such things as isolating or closing a compromised online service, finding a lost piece of equipment or simply changing the access codes at the front door.

- Establish whether there is anything can be done to recover any losses and limit the damage the breach can cause.

This could mean physical recovery of lost equipment, changing password, taking online services down temporarily, the use of backups to restore lost or damaged data or ensuring that staff recognise if someone tries to use stolen data to access accounts.

- Where appropriate, decide to inform the Information Commissioner's Office, the police or external stakeholders.

- Follow up evaluation and responses to minimise the chance of reoccurrence

Depending on the seriousness of the breach, the Response Group may decide in the initial meeting to bring in specialists including other Welsh Boxing staff, IT providers, online service providers, HR, legal and external commissioners/funders.

Key Questions for the Response Group

The Response Group will want to answer the following key questions:

- What type of data is involved?
- How sensitive is it?

Remember that some data is sensitive because of its very personal nature (health information of our athletes for example) while other data types are

sensitive because of what might happen if it is misused (emails or telephone numbers).

- If data has been lost or stolen, are there any protections in place such as encryption?
- What has happened to the data?

If data has been stolen, it could be used for purposes which are harmful to the individuals to whom the data relate; if it has been damaged, this poses a different type and level of risk.

- Regardless of what has happened to the data, what could the data tell a third party about the individual?
- How many individuals' personal data are affected by the breach?

It is not necessarily the case that the bigger risks will accrue from the loss of large amounts of data but is certainly an important determining factor in the overall risk assessment.

- Who are the individuals whose data has been breached?

Whether they are staff, athletes, commissioners or suppliers, for example, will to some extent determine the level of risk posed by the breach and, therefore, Welsh Boxing's actions in attempting to mitigate those risks.

- What harm can come to those individuals affected?
- Are there risks to physical safety or reputation, of financial loss or a combination of these and other aspects of their life?
- Are there wider consequences to consider such as a risk to public health or loss of public confidence in the service Welsh Boxing provides?

5. Notification of Breaches

There may be the requirement for Welsh Boxing to notify others about the breach, including both those whose data has been breached, and regulatory bodies such as the Information Commissioners Officer. The Response Group should decide on who needs to be informed.

Notification should have a clear purpose, whether this is to enable individuals who may have been affected to take steps to protect themselves or to allow the appropriate regulatory bodies to perform their functions, provide advice and deal with complaints.

When Does Welsh Boxing need to notify the ICO?

When a personal data breach has occurred, the Response Group need to establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there may or will be a risk to people's rights and freedoms, then Welsh Boxing must notify the ICO.

If the Response Group decides not to report the breach, they need to be able to justify this decision document it.

Under Recital 85 of the GDPR, a data breach must be reported where it may:

"result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned"

Reporting to ICO

When reporting a data breach to the ICO, the Response Group will need to provide:

- a description of the nature of the personal data breach including, where possible:
- the categories and approximate number of individuals concerned; and
- the categories and approximate number of personal data records concerned;
- the name and contact details of the Chief Executive or other contact point where more information can be obtained;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

It may be possible that not all that information will be available at the time of the report, and the Response Group will need to pass it to ICO later.

When does Welsh Boxing need to tell individuals about a breach?

If a breach is likely to result in a high risk to the rights and freedoms of individuals, GDPR states Welsh Boxing must inform those concerned directly and without undue delay. A 'high risk' means the threshold for informing individuals is higher than for notifying the ICO, so Welsh

Boxing must always inform the ICO if it believes individuals should be notified.

The Response Group will need to assess both the severity of the potential or actual impact on individuals as a result of a breach and the likelihood of this occurring. If the impact of the breach is more severe, the risk is higher; if the likelihood of the consequences is greater, then again the risk is higher. In such cases, Welsh Boxing need to promptly inform those affected, particularly if there is a need to mitigate an immediate risk of damage to them. One of the main reasons for informing individuals is to help them take steps to protect themselves from the effects of a breach.

When does Welsh Boxing need to tell funders or external stakeholders?

The Response Group will need to assess whether informing funders at the start of the data breach will help reduce the risk for those individuals affected, for example, if the data breach affects athletes who also are part of another sporting body.

6. Evaluation and Response

The Chief Executive is charged with recording the breach process and the decisions of the Response Group and maintaining a record of all data breaches. All data breaches will be reported to the Board.

The Response Group will continue to manage the Breach process until they are satisfied that they have complied with the GDPR principles. The Group may charge Welsh Boxing teams or individuals with implementing processes and policies to remove or reduce the risk of reoccurrence.

At the evaluation stage, the Chief Executive will prepare an evaluation plan for the Board including:

- Updating breach records, and any Risk registers associated with the event
- Lessons learnt from the process
- Recommendations for process or policy changes to prevent similar occurrences
- Process of detecting any negative impact on the individuals affected by the breach where appropriate

At a time set by the Response Group, but no longer than six months, the Chief Executive will review the breach and evaluation plan and report back to the Board.

If the breach has been reported to the ICO, an action plan and review may be independently undertaken by the ICO, and penalty fines may be levied.