WelshBoxing
BocsioCymru

Data Protection Policy

Introduction

We hold personal data about our employees, athletes, suppliers and other individuals for a variety of business purposes.

This policy sets out how we seek to protect personal data and ensure that staff understand the rules governing their use of personal data to which they have access in the course of their work. In particular, this policy requires staff to ensure that the Chief Executive is consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

Scope

This policy applies to all staff, board athletes and volunteers. You must be familiar with this policy and comply with its terms.

This policy supplements our other policies relating to internet and email use. We may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff before being adopted.

Who is responsible for this policy?

- Welsh Boxing's Board are responsible for this policy and accountability for the compliance to the GDPR legislation and guidance.

- Welsh Boxing's Chief Executive has overall responsibility for the day-to-day implementation of this policy.

- All staff have a responsibility to understand and adhere to this policy.

What responsibilities do Welsh Boxing staff and Board athletes have under this policy?

The Board

- Accountable for GDPR and data protection compliance
- Reviewing this policy annually
- That they are satisfied policy is being implemented
- Tasking officers with reporting on the implementation, risks, and requirements to deliver this policy

The Chief Executive's responsibilities:

- Keeping the board updated about data protection responsibilities, risks and issues
- Reviewing all data protection procedures and policies on a regular basis
- Arranging data protection training and advice for all staff athletes and those included in this policy
- Answering questions on data protection from staff, board athletes and other stakeholders
- Responding to individuals such as clients and employees who wish to know which data is being held on them by Welsh Boxing
- Checking and approving with third parties that handle the company's data any contracts or agreement regarding data processing
- Approving data protection statements attached to emails and other marketing copy

Responsibilities of the Operations Team

- Ensure all systems, services, software and equipment meet acceptable security standards

- Checking and scanning security hardware and software regularly to ensure it is functioning properly

- Researching third-party services, such as cloud services the company is considering using to store or process data

Responsibilities of Coaches, Partnership and Business Development Team

- Following policy and procedures to protect sensitive data belonging to our athletes, their families and supporters.

- Ensuring personally identifiable data is safely stored and processed.

- Coordinating with the Chief Executive to ensure all programme and marketing initiatives adhere to data protection laws and the company's Data Protection Policy

Our procedures

Fair and lawful processing

Welsh Boxing must process personal data fairly and lawfully in accordance with individuals' rights. This generally means that we should not process personal data unless the individual whose details we are processing has consented to this happening.

The processing of all data must be:

- Necessary to deliver our services and kept to a minimum

- In our legitimate interests and not unduly prejudice the individual's privacy

Our website contains our Privacy Policy on data protection.

The notice:

- Sets out the purposes for which we hold personal data on athletes and employees.

- Highlights that our work may require us to give information to third parties such as evaluators and funders where it meets the conditions to do so under GDPR.

- Provides that athletes and staff have a right of access to the personal data that we hold about them

Sensitive personal data

In most cases where we process sensitive personal data we will require the data subject's *explicit* consent to do this unless exceptional circumstances apply or we are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work).

Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

Accuracy and relevance

We will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Individuals may ask that we correct inaccurate personal data relating to them. If you believe that information is inaccurate you should record the fact that the accuracy of the information is disputed and inform the Chief Executive.

Data security

All staff and Board members have a duty to keep personal data secure against loss or misuse. Where other organisations process personal data as a service on our behalf, the Chief Executive will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third-party organisations.

Storing data securely

- In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it

- Printed data should be shredded when it is no longer needed

- Data stored on a computer should be protected by strong passwords that are changed regularly. We encourage all staff to use a password manager to create and store their passwords.

- Data stored on CDs or memory sticks must be locked away securely when they are not being used.

- All notebooks, laptops, desktop computers and physical servers owned by Welsh Boxing should be encrypted to industry standard

- The Chief Executive must approve any apps, programmes or cloud-based services used to store data

- Servers containing personal data must be kept in a secure location, away from general office space

- Data should be regularly backed up in line with the company's backup procedures

- Data should never be saved directly to mobile devices such as laptops, tablets or smartphones

- All servers containing sensitive data must be approved and protected by security software and strong firewall.

Data retention

We must retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but should be determined in a manner consistent with our data retention guidelines.

Transferring data internationally

There are restrictions on international transfers of personal data. You must not transfer personal data anywhere outside the UK without first consulting the Chief Executive.

Processing data in accordance with the individual's rights

You should abide by any request from an individual not to use their personal data for direct marketing purposes and notify the Chief Executive about any such request.

Training

All staff will receive training on this policy. New joiners will receive training as part of the induction process. Further training will be provided at least every two years or whenever there is a substantial change in the law or our policy and procedure.

Training is provided on a regular basis.

It will cover:

- The law relating to data protection
- Our data protection and related policies and procedures.
- The impact on our day to day work, both operationally and within programmes.

Completion of training is compulsory.

Privacy Notice - transparency of data protection

Being transparent and providing accessible information to individuals about how we will use their personal data is important for our organisation.

Our policy is to ensure that links to Privacy Notices will be prominent on all our online materials.

Conditions for processing

We will ensure any use of personal data is justified using at least one of the conditions for processing and this will be specifically documented. All staff responsible for processing personal data will be aware of the conditions for processing. The conditions for processing will be available to data subjects in the form of a privacy notice.

Summary of Key Lawful Conditions:

Welsh Boxing will keep a clear and up to date list of all the personal information it keeps along with the lawful condition in place to allow it to do so. Broadly (notwithstanding exceptions and specifics) Welsh Boxing will:

- collect, store and process our Athlete's personal information based on Consent, and will always obtain explicit written consent.
- collect, store and process the information of our employees and volunteers based on entering into a Contract
- collect, store and process the information of our partners, funders, Board and based on legitimate business interest.

Justification for personal data

We will process personal data in compliance with all six data protection principles.

We will document the additional justification for the processing of sensitive data and will ensure any biometric and genetic data is considered sensitive.

Consent

The data that we collect is subject to active consent by the data subject. This consent can be revoked at any time.

Criminal record checks

Any criminal record checks are justified by law. Criminal record checks cannot be undertaken based solely on the consent of the subject.

Data portability

Upon request, a data subject should have the right to receive a copy of their data in a structured format. These requests should be processed within one month, provided there is no undue burden and it does not compromise the privacy of other individuals. A data subject may also request that their data is transferred directly to another system. This must be done for free.

Right to be forgotten

A data subject may request that any information held on them is deleted or removed, and any third parties who process or use that data must also comply with the request. An erasure request can only be refused if an exemption applies.

Privacy by design and default

Privacy by design is an approach to projects that promote privacy and data protection compliance from the start. The Chief Executive will be responsible for conducting Privacy Impact Assessments and ensuring that all programme, operational or IT projects commence with a privacy plan.

Data audit and register

Regular data audits to manage and mitigate risks will inform the data register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.

Reporting breaches

All athletes of staff have an obligation to report actual or potential data protection compliance failures. This allows us to:

- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures
- Notify the ICO of any compliance failures that are material either in their own right or as part of a pattern of failures

Please refer to our Data Breach Policy for our reporting procedure

Monitoring this policy

Everyone must observe this policy. The Chief Executive has overall responsibility for this policy. They will monitor it regularly to make sure it is being adhered to.

Consequences of failing to comply

We take compliance with this policy very seriously. Failure to comply puts both you and the organisation at risk.

The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our procedures which may result in dismissal.

If you have any questions or concerns about anything in this policy, do not hesitate to contact the Chief Executive.