Bourne Town Harriers

Admin@bournetownharriers.org

www.bournetownharriers.com

Personal Data Policy

Last Updated 06/03/2019

Table of Contents

Introduction

The *General Data Protection Regulation* (GDPR), is effective as of 25th May 2018. Replacing the previous *Data Protection Act* (DPA), the GDPR introduces and prioritises key requirements regarding the storage and use of personal data and more.

At Bourne Town Harriers AC, as both a controller and processor of personal data, we prioritise the ethical and secure use of personal data. This document covers our personal data and privacy policies in regard to the GDPR.

Key Definitions

GDPR | '*General Data Protection Regulation';*

Personal Data | 'Any information relating to an identified or identifiable natural person ('data subject');'

Individual ('Data Subject') | 'An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;'

Data Processing | 'Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;'

Processor | 'a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;'

Controller | 'The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;'

Third Party | 'A natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;'

We have provided these key definitions as a guide. They have been referenced from "Directi§ve (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services". If required, further definitions can also be found in this directive using the link above.

Collection and Use

Collection

We collect personal data in several ways:

Personal Communication | Data collected when contacting or contacted by past, current or prospective clients and suppliers. This information is stored and processed to provide or receive services to/from these contacts. Data is not stored if it offers no further use to us or the contact in question.

Online Form | An online form is used to provide website visitors with a simple way to contact us. Name and e-mail address are requested to reply to the visitor submitting the form.

Website Mechanisms | Our website uses cookies and similar technologies to run and understand how visitors use the site. This data is collected automatically by Squarespace (the website host) and is used to monitor site traffic, usage patterns and analyse general demographic data. Some information is passed to analytics sites, including Google Analytics, to monitor data for search engine optimisation. Information is not used by us to identify individual users.

This data can be updated or removed upon request if possible and to a reasonable time-frame.

Lawful Basis

We ensure data is processed with a strong lawful basis. Data will only be processed by us if it represents one or more of the following criteria:

Consent | The individual has given clear consent for their personal data to be processed for a specific purpose.

Contract | It is necessary to process a person's data to fulfil or enter into a contract with that person or an organisation they represent.

Legitimate Interest | It is necessary to process a person's data for the legitimate interest of that person, their organisation or us.

Consent

We acquire consent in several ways:

Personal Communication - Email Footer | Emails sent by our accounts include a footer with information regarding personal data collection and use. Recipients are also given clear instructions regarding the update or removal of their data from our systems.

Website - Privacy Policy & Cookie Notice | Visitors to our website are presented with a cookie notice that describes cookie use and provides a link to the privacy policy page. The privacy policy page clearly describes personal data use and instructions for update or removal from our systems.

Online Form - Disclaimer | The online contact form includes a clear personal data policy overview that must be read before submitting the form. Data update & removal instructions are also given.

Legitimate Interests

Personal data is used by us for secondary business activities, such as self-advertising, accounts and records. Data is only passed on to third parties to aid these activities (such as search engine optimisation and website usage monitoring etc) and is never sold or disclosed to external bodies for their own purposes.

Third Parties

Third Party Disclosure

We use several third party software packages and services to aid our necessary business activities. As a result, personal

information that we process may also be processed using third party systems. These include the following:

Squarespace

Our website is hosted on Squarespace. They provide us with the online platform that allows us to promote our services to customers.

Personal data is processed with Squarespace's storage, databases and software.

Squarespace's Terms of Service and Privacy Statement can be found here:

https://www.squarespace.com/terms-of-service/

https://www.squarespace.com/privacy/

Analytics Providers

To optimise search engine behaviour, our website may be linked with search analytics providers (Google Analytics and Bing Webmaster). Please review the terms and conditions of these third parties below:

Google Policies:

https://policies.google.com/

Bing Policies:

https://privacy.microsoft.com/

MailChimp

We use MailChimp to organise mailing lists for past and current clients for contract obligations and future communication via email. MailChimp's Terms of Service and Privacy Statement can be found here:

https://mailchimp.com/legal/privacy/

Third Party Notices

In general, the third-party providers used by us will only collect, use and disclose your information to the extent necessary to allow them to perform the services they provide to us.

However, some third party service providers may have their own privacy policies regarding the information we provide them. Individuals should read the privacy policies of these providers to further understand the manner in which their personal information will be handled.

Some providers may be located in or have systems that are located in a different jurisdiction to us. If so, an individual's personal information may be subject to the laws of the jurisdiction(s) in which these systems are used.

Data Protection

Storage

Whilst it is necessary for us to process some personal information, it is not necessary for this information to be stored in anything other than a digital manner. Therefore, we do not use paper / hard copies to store personal information.

Security

We use several systems to keep digital personal information stored securely:

Database Limitation | Where personal information is kept within a database, the information stored is limited to the details necessary for our purposes.

Encryption | Our storage systems are encrypted. This protects any stored data as the entire volume/s cannot be accessed without an encryption key. Encryption is also used when accessing our systems externally using an internet connection.

Redundancy | Our storage systems use RAID technology to provide data with redundant, instantly attainable copies. This ensures that important information can be restored in the event of hardware failure to support any legal basis for data processing.

Backups | Our storage systems also use off-site backups to provide added protection to stored data. This allows personal data, recorded procedures and security systems to be restored in the event of local hardware failure.

These security measures are continually maintained and upgraded. However, no digital security system is infallible. It is therefore necessary for data processors to be selective about what data is stored and how it is accessed.

Retention & Maintenance

Personal information will inevitably become incorrect or irrelevant over time. It is therefore necessary to routinely evaluate the usefulness and quality of personal data stored by us. Upon evaluation, personal information will only be kept if it is deemed genuinely useful for current or future business activities.

If data is no longer useful or identified as incorrect, it will be permanently deleted or updated where appropriate. The frequency of these information assessments will be at least once every six months to ensure our databases remain correct and do not store unnecessary information.

Data Breaches

Our Obligations

The GDPR places obligations on us in relation to processing data lawfully and ensuring it is kept secure.

One such obligation is to report a breach of personal data in specific circumstances. This policy sets out our procedures for detecting and dealing with a breach.

Personal Data Breach

A personal data breach is a breach of security causing the accidental and/or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or processed.

Breach Detection

We use several methods to assist the detection of a personal data breach:

Paperless Systems | We do not keep personal data using paper-based storage as it is neither necessary or secure.

Secure Storage | Our systems use industry-standard security measures to prioritise the privacy and integrity of the personal data we store.

Data Integrity Checks | We perform regular checks on our stored data and security systems to identify potential data breaches. We assess:

I. Security hardware/software status
II. System Access Activity Logs
III. Data integrity

Investigating Suspected Breaches

In the event that we become aware of a suspected breach, an investigation will be carried out. This investigation will be conducted by one or more of our partners who will make a decision over whether we must notify the Information Commissioner. A decision will also be made regarding whether the individual(s) must also be notified.

Notifying the Information Commissioner

In accordance with the GDPR, we will notify the Information Commissioner of a breach which is likely to pose a risk to a person's rights and freedoms. A risk to a person's freedoms can include physical, material or non-material damage such as discrimination, identity theft/fraud, financial loss and damage to reputation. Notification will be done without delay and within 48 hours of discovery where possible.

Notification will include:

I. A summary of the personal data breach, including the type and amount of individuals/data involved, where possible.
II. The contact details of the partner/s handling the investigation/notification.
III. A breakdown of the potential consequences of the personal data breach.
IV. A description of the measures proposed, or taken, to deal with the personal data breach.

When a breach will be notified to the individual

In accordance with the GDPR, we will notify, without delay, the individual whose data has been involved in the breach if there is a high risk to their rights and freedoms.

Notification will include:

I. A summary of the personal data breach.
II. The contact details of the partner/s handling the investigation/notification.
III. A breakdown of the potential consequences of the personal data breach.
IV. A description of the measures proposed, or taken, to deal with the personal data breach.

Record of Breaches

We record all personal data breaches regardless of whether they are notifiable or not. Such records include the nature of the breach, its effects and the actions taken in response.

Rights regarding your data

Right to be informed

We make this policy publicly available to promote transparency regarding the use of an individual's data.

Our policy openly summarises:

I. The types of data we hold, how we collect them and why we process them;
II. Our legitimate interest for processing this data;
III. Information on the transfer of data to third parties and, where applicable, other countries;
IV. Our retention policy for the data we store;
V. The rights of individuals we keep data on;
VI. Information on consent and right to withdraw;
VII. Information on complaints and requests;
VIII. The use of any automated systems;
IX. Our name and contact details.

Right of access

Individuals have the right to request any personal data we store about them, where feasible. A formal access request can be made directly to us.

We will release the following information to the individual:

I. Whether their data is processed by us and the reasons for any processing;
II. The categories of any personal data we store about them;
III. how the data was collected;
IV. whether the data has been disclosed to third parties and, where applicable, other countries. As well as the security measures used;
V. Our retention policy
VI. Their rights regarding the use of this data;
VII. Their right to contact the information commissioner regarding the use of their data;

We aim to provide such data within 28 days. However, this process can take longer when complex storage or analytics systems are involved.

We will contact any individual whose data we cannot provide access to and they will be free to contact the Information Commissioner regarding this issue.

Right to correction

Individuals have the right to correct any personal data we store about them if it appears to be incorrect.

We aim to amend such details within 28 days. However, this process can take longer when complex storage or analytics systems are involved.

We will contact any individual whose data we cannot correct and they will be free to contact the Information Commissioner regarding this issue.

Right of erasure

Individuals have the right to request erasure of the personal data we store about them. A formal erasure request can be made directly to us.

We will endeavour to delete all our records of the stored personal data, including those kept by third parties. If this is not possible, we will contact the individual promptly.

Right of restriction

Individuals have the right to restrict the processing of any personal data we store about them. A formal restriction request can be made directly to us.

We may continue to hold restricted data for legitimate purposes, such as legal claims and obligations. We will also request that third parties restrict the processing of the data in question.

Right to data portability

Individuals have the right to transfer the data we process on them to another party, where feasible.

We aim to make such transfers within 28 days. However, this process can take longer when complex storage or analytics systems are involved.

We will contact any individual whose data cannot be transferred and they will be free to contact the Information Commissioner regarding this issue.

Right to object

Individuals have the right to object to the processing of any personal data we store about them. A formal objection can be made directly to us.

We may continue to process this data if required to do so for legitimate reasons, such as legal or safety concerns.

Right not to have automated decisions made about you

Individuals have the right not to have decisions with significant effects on them made using solely automated processes that have no human involvement. However, we do not use such decision-making processes.

Contacting Us

To contact us regarding our policies or use of personal data, please e-mail the following address:

admin@bournetownharriers.org