Sway Bowmen
General Data Protection Regulation Policy

-

Produced by Roger Lee

Contents

1. Introduction

1.1. Aim

The aim of this policy is make Sway Bowmen compliant with the new the General Data Protection Regulation (GDPR) which comes into play in May 2018.

Many of the GDPR's main concepts and principles are much the same as those in the current Data Protection Act (DPA), therefore most of our approach to compliance will remain valid under the GDPR and is a starting point to build from. However, there are new elements and significant enhancements. We will have to do some things for the first time and some things differently. The aim of this Policy is to identify our approach and reasoning to ensure compliance under the GDPR. We need to review our risk register against this.

Doing this will also help us to comply with the GDPR's accountability principle, which requires organisations to be able to show how they comply with the data protection principles, for example by having effective policies.

1.2. Scope

This Policy applies to all personal data used and recorded by the members of Sway Bowmen which is a Company Limited by Guarantee, a member of the Community Amateur Sport Club (CASC) and a member of Archery GB.

1.3. Update

This policy will be reviewed annually for update or when Data Protection legislation changes.

1.4. Document Overview

This document contains the following Sections

Section 1 Introduction
Containing the Aim, Scope, update timing and this Document Overview.

Section 2
Why Have a Data Protection Policy

Section 3 GDPR Requirements

- Identify the Information We Hold
- Communicating privacy information
- Dealing with Complaints
- Identifying Individuals' rights
- Subject access requests
- Lawful basis for processing personal data
- Consent (including Archery GB text)
- Children's Consent
- Data breaches
- Data Protection by Design and Data Protection Impact Assessments
- Data Protection Officer

Section 4 Application Forms

- Beginners Course Application Form
- Membership Application Form
- Membership Renewal

Section 5 Records Kept

- Beginners Course students – Course Coordinator
- Treasurer's Database – Treasurer
- Membership Records - Membership Secretary
- Achievements Records – Records Secretary
- Shoot for Gold Membership Records – Shoot For Gold Secretary
- Minutes
- Emails

Appendices

Contain Archery GB's Privacy Statement link and example Beginners Course, Membership and Renewal forms.

2. Background - Why Have a Data Protection Policy

This Policy informs the Directors and Committee that the law is changing to the GDPR and what we have to change. It details the Sway Bowmen approach to GDPR compliance and the requirements of Archery GB.

3. GDPR Requirements

3.1. Identify the Information We Hold

This Policy documents what personal data we hold, where it came from, who has access to it and who we share it with. We have completed an information audit across the organisation. This Policy also records our processing activities. We have to ensure that we have accurate personal data. If we find that we have shared inaccurate data with another organisation, we will have to tell the other organisation about the inaccuracy so it can correct its own records. We will record this.

3.2. Communicating privacy information

We have produced privacy notices and will review them, making any necessary changes in time for GDPR implementation. When we collect personal data we give people certain information, such as our identity and how we intend to use their information. Under the GDPR we need to explain our lawful basis for processing the data, our data retention periods and seek consent where necessary.

3.3. Dealing with Complaints

If someone thinks there is a problem with the way we are handling their data they need to complain in writing following the club's complaints policy contained the member's handbook.

3.4. Identifying Individuals' rights

Our policy cover all the rights individuals have, including how we would delete personal data and provide data electronically and in a commonly used format.

The GDPR includes the following rights for individuals:

- the right to be informed;
- the right of access;
- the right to rectification;
- the right to erasure;
- the right to restrict processing;
- the right to data portability;
- the right to object;
- the right not to be subject to automated decision-making including profiling

On the whole, the rights individuals will enjoy under the GDPR are the same as those under the DPA but with some significant enhancements. This is a good time to check our procedures and to work out how we would react if someone asks to have their personal data deleted, for example. Would our systems help us to locate and delete the data? Who will make the decisions about deletion?

The right to data portability is new. It only applies:

- personal data an individual has provided to a controller;
- where the processing is based on the individual's consent or for the performance of a contract; and
- when processing is carried out by automated means.

We will need to provide the personal data in a structured commonly used and machine readable form and provide the Preparing for the General Data Protection Regulation (GDPR

3.5. Subject access requests

We should update our procedures and plan how we will handle requests to take account of the new rules:

- In most cases we will not be able to charge for complying with a request.

- We will have a month to comply, rather than the current 40 days.

- We can refuse or charge for requests that are manifestly unfounded or excessive.

- If we refuse a request, we must tell the individual why and that they have the right to complain to the supervisory authority and to a judicial remedy. We must do this without undue delay and at the latest, within one month. If our organisation handles a large number of access requests, consider the logistical implications of having to deal with requests more quickly. We could consider whether it is feasible or desirable to develop systems that allow individuals to access their information easily online.

- Names should not be included in Club Minutes and Correspondence including emails, unless absolutely necessary as individuals can ask to see minutes and correspondence that contain their names. Especially where there have been reported problems discussed. List of attendees and actions will be included in the minutes.

3.6. Lawful basis for processing personal data

We use consent as our lawful basis for processing.

3.7. Consent

We are required to obtain member's consent to use their personal data. Sway Bowmen only use the data to enable us to contact members and in the running of the Club. We do not pass your data to anyone else other than Archery GB, HAA and SCAS.

We have reviewed how we seek, record and manage consent.

All our application forms will include details on how we will use their personal data, where and how it is stored, who has access to it and when it will be deleted.

Archery GB. *(Text from Archery GB*)

When you become a member of or renew your membership with Sway Bowmen you will automatically be registered as a member of Archery GB and the relevant County and Region. We will provide Archery GB with your personal data which they will use to enable access to an online portal for you (https://agb.sport80.com) which, amongst other things, allows you to set and amend your privacy settings. If you have any questions about the continuing privacy of your personal data when it is shared with Archery GB, please contact gdpr@archerygb.org."

"*Would you like to continue to hear from Archery GB about our latest news including our quarterly magazine, ways in which you can support us and membership benefits available? If so, please tick below to let us know how you would like to hear from us and confirm your contact details:*

1)	*Magazine*	*Yes [ ]*	*No [ ]*
2)	*Email Newsletter*	*Yes [ ]*	*No [ ]*
3)	*Membership benefits / offers by email*	*Yes [ ]*	*No [ ]*

We will keep your details safe, and you can unsubscribe or change your preferences at https://agb.sport80.com "

The Archery GB Privacy statement is at Appendix 1.

Children's Consent

The GDPR sets the age when a child can give their own consent to this processing at 16 (although this may be lowered to a minimum of 13 in the UK). If a child is younger then we will need to get consent from a person holding 'parental responsibility'.

3.8. Data breaches

We should make sure we have the right procedures in place to detect, report and investigate a personal data breach. We don't have to notify the ICO of a breach as it is unlikely to result in a risk to the rights and freedoms of individuals –for example, if it could result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage, we would also then have to notify those concerned directly in these cases. Failure to report a breach in the above case could result in a fine, as well as a fine for the breach itself.

3.9. Data Protection by Design and Data Protection Impact Assessments

The GDPR makes privacy by design an express legal requirement, under the term 'data protection by design and by default'. It also makes PIAs – referred to as 'Data Protection Impact Assessments' or DPIAs – mandatory in certain circumstances'

We don't need to complete DPIA because our data processing is not likely to result in high risk to individuals, for example:

- No new technology is being deployed;
- No profiling operation which is likely to significantly affect individuals; or
- No processing on a large scale of the special categories of data.

We need to complete basic PIAs for all data held. We need to familiarise ourselves with the guidance the ICO has produced on PIAs as well as guidance from the Article 29 Working Party, and work out how to implement them in our organisation.

.

3.10. Data Protection Officer

We shall designate someone to take responsibility for data protection compliance and assess where this role will sit within our organisation's structure and governance arrangements. We do not need to to formally designate a Data Protection Officer (DPO) as we do not meet the criteria that require one. We must however designate someone in our organisation, or an external data protection advisor, to take proper responsibility for our data protection compliance and has the knowledge, support and authority to carry out their role effectively.

4. Application Forms

4.1. Beginners Course Application Form

Include new text explaining how and what data we keep and for how long and what their rights are. Include consent tick box.

4.2. Membership Application Form

Include new text explaining how and what data we keep and for how long and what their rights are. Include consent tick box.

4.3. Membership Renewal

Include new text explaining how and what data we keep and for how long and what their rights are. Include consent tick box.

4.4. Mushroom Shoot Application form

We need to add the following statement to the application forms:-

I wish/do not wish for my details to be stored for future communication. I wish/do not wish for my name to be published

signed..... date.....

5. Records Kept

5.1. Beginners Course students – held by Course Coordinator

For each year's Beginners Courses the following data is entered into an Excel spreadsheet held by the Course Coordinator, as and when applications are received. The spreadsheet is held on the Course Coordinator's PC which is Password Protected and has antivirus software. This is held for 2 years so that students can be contacted especially the one's not joining the club. This data is not used by anyone else but the Course Coordinator. Hard Copy will be printed for course use and then destroyed on completion. All but Names and email address are then deleted.

- Name
- Address
- Telephone number
- Email Address
- Age when under 18
- Requested Course
- Amount Paid

5.2. Treasurer's Database – held by Treasurer

Excel spread sheets which are historic downloads from the old archived database which do contain names, addresses, emails and, in the case of juniors, dates of birth. In addition they have a list of members and the fees paid for club membership and GNAS but those really only contain names and status of club membership such as junior, senior or associate.

The treasurer now uses the club database online on the website to access member's details when necessary for checking on fees or sending off Shoot for Gold cheques, etc.

5.3. Club Online Database

The following data is held about individuals:

- Name
- Address
- Telephone (landline and/or mobile)
- Email
- DOB if under 25
- ArcheyGB membership number
- Website login name and password (Password is stored in a hashed format)
- Date membership was last renewed
- Fee paid
- Shoot for Gold number
- Subscription history
    - Membership plans (ie. GNAS Adult, Full Junior Club Member)
    - Fee Paid
    - Status (Pending, Active, Expired . . .)
- Newsletter subscription (Yes/No)
- Date registered on website
- Date last visit to website
- Website user group (Member, Committee Member)
- If they have renewed membership on-line:
    - Order number
    - Payment method (Credit card, PayPal)
    - Date
    - Order status (Created, Confirmed, Cancelled, Refunded)
    - User IP

Member's details are deleted if not renewed after a year.

Who has access:

- The committee members have access to the addresses and status of Current Adult Members
- The Treasurer and Membership Secretary also have access to addresses and status of Junior members
- The Treasurer and Membership Secretary have access to the membership database
- The Database Manager has access to everything

Where is it stored:

Currently the website and database are stored on servers in Equinix's Synergy House in Manchester. The site conforms to best practice ISO 27001 security and access controls (including CCTV, Double Skin entry) with 24x7x365 support with qualified Equinix security staff.

We will be moving the site to a new hosting provider later in the year and the site will then be located in Telehouse North in London.

Software:

The server is running under Linux on an Apache http server with PHP scripting and data stored on a MySQL database. The website is built using Joomla. The server and website software are all kept up to date. The website is backed up each month onto Amazon S3 secure cloud service.

The server is protected by a firewall and ModSecurity, Fail2Ban and virus scans are made using MalDet. (Might change when we move to a new host)

The website is protected against:

- SQL injection
- Cross Site Scripting
- Malicious User Agents,
- Cross Site Request Forgery
- Remote File Inclusion
- Direct File Inclusion
- All uploads are scanned
- Anti-spam, anti-hacker protection using Project Honeypot IP blocker directory
- Auto ban of IP's causing excessive exceptions
- Site uses HTTPS protocol using 256bit keys to communicate with the server

Old Database:

The Database Manager has an archived copy of the old database which is stored on Amazon's S3 secure cloud storage.

5.4. Membership Records - held by Membership Secretary

The Membership Secretary uses the Club's database for member information. They keep no membership information electronically. Paper records are supplied by Archery GB for GNAS renewals and that is kept for 1 year until next renewal.

We will provide Hampshire Archery Association with your personal data including name, address, Archery GB number and DOB. This is shared with the HAA treasurer who uses it to enable correct affiliation payments to both Hampshire AA and SCAS, then deletes the digital information we pass on and keeps paper copies for 6 years. The HAA treasurer passes your name and archery club details only to the HAA secretary in the event that a question is raised regarding affiliation or the club of a member. This information is kept in a password protected document and held for 2 years."

5.5. Achievements Records – held by Records Secretary

Club records are currently held in both Microsoft Excel and in Toxic Software Golden Records on a private Computer protected by Norton Security. We will not retain the DoB of any ex-Junior record holders.

The records pertaining to all current archers will be retained in the new software until they leave the club - unless they hold records when it will be held until they no longer hold any records.

These records are only available to the Club Records Officer.

- Name
- Date of Birth for Juniors if outdoor classification is required
- Achievements
    - Rounds shot
    - Scores
    - Dates
    - Bow type
    - Resultant Handicaps

5.6. Shoot for Gold Membership Records – held by Shoot for Gold Secretary

The following information is held by the by Shoot for Gold Secretary to enable winners to be contacted.

- Name
- Address
- Email Address

It is held on a Windows 10 Computer with Firefox, MS Office 7 and Malwarebytes.

The Shoot for Gold Secretary is the only person that has access to this computer.

5.7. Paying Membership by PayPal

If a member pays for membership fees using PayPal then the '*PayPal transaction id*' is stored in the database. It only means anything to PayPal but it is necessary if either side want to query the transaction. Credit Card numbers are not stored and neither is the members PayPal login. If a credit card is used the details are encrypted and tokenised on the members device and transmitted directly to the card processing company (Stripe) or PayPal.

5.8. Minutes

Names should not be included in Club Minutes and Correspondence including emails, unless absolutely necessary as individuals can ask to see minutes and correspondence that contain their names. Especially where there have been reported problems discussed. List of attendees and actions will be included in the minutes.

5.9. Emails

When sending emails to a group of people ensure the addressees are in the BCC so email addresses are not shared openly.

Appendix 1. Archery GB Privacy Statement Link

Here is the link to Archery GB's Privacy Statement

https://www.archerygb.org/privacy-policy/

Here is the Link to Archery GB's Data Protection Policy and Procedures

https://www.archerygb.org/wp-content/uploads/2017/05/OPP1001DataProtectionPolicyandProcedures-20284.pdf

Appendix 2. Example Beginners Application Form

SWAY BOWMEN

Archery Beginners Courses 2018

Sway Bowmen will be running a beginners courses in April/\May 201# at our grounds near Sway. No previous experience required and we supply all the equipment you will need for the course.

Course 1 - £60	**Course 2 - £60**	**Course 3 - £60**	**Course 4 - £60**
Saturday 7th April Sunday 8th April	• Saturday 21st April • Sunday 22nd April	• Saturday 12th May • Saturday 19th May • Saturday 26th May • Saturday 2nd June	• Saturday 23rd June • Sunday 24th Junel
10:00 – 15:30 each day	10:00 – 15:30 each day	10:00 – 12:00 each Saturday	10:00 – 15:30 each day

If you are interested please complete the form below for each person and forward it to:
Roger Lee 21 Bilberry Drive, Marchwood, Southampton SO40 4YR

We will get in touch with you before the course starts with further details.
Please DO NOT be tempted to buy any equipment at this stage. After the course has ended we will advise you of what you need.

Please enclose a cheque for £60.00 made payable to: **Sway Bowmen**

Name(s): Date of birth (If under 18)
Address: ....
.....
.....
.....
.....
Postcode: Cheque enclosed: £

Telephone: Mobile:

Email:

Consent ☐ No ☐ Yes

Due to the new General Data Protection Regulations we are required to obtain your consent to use your personal data provided above. Sway Bowmen only use your data to enable us to contact you. We will not pass your data to anyone else. This form and a spreadsheet containing its data will be held by the Course Coordinator securely. The forms and spreadsheet will be deleted within 2 years of your completion of this course. Your consent will be given by ticking the corresponding box.

If you don't want to give consent then we will not be able to contact you about the course.

Signed

.....(Parents must sign for children under 16)

Date .....

Appendix 3. Example Membership Application form

Sway Bowmen

Membership Application form

Name

Address

Post code

Telephone mobile:-

e-mail

Date of Birth

GNAS number

I have read, understood and agree to be bound by the rules in the Club Handbook.

In accordance with the General Data Protection Regulation I give permission for the above personal information to be held by Sway Bowmen Archery Club both manually and electronically. (Refer to the Club GDPR Policy on our website)

I understand that it will only be used for Club membership reasons and to keep in touch with me and will be held securely and only accessed by authorised Club Officers

I consent to this information being held Yes ☐ **No** ☐

Signed……(Parents must sign for children under 16)

Date

If consent is not given we will be unable to contact you

Appendix 4. Example Member's Renewal Form

Sway Bowmen

Renewal of Membership

Name

Address

Post code

Telephone mobile:-

e-mail

Date of Birth

GNAS number

I have read, understood and agree to be bound by the rules in the Club Handbook.

In accordance with the General Data Protection Regulation I give permission for the above personal information to be held by Sway Bowmen Archery Club both manually and electronically. (Refer to the Club GDPR Policy on our website)

I understand that it will only be used for Club membership reasons and to keep in touch with me and will be held securely and only accessed by authorised Club Officers

I consent to this information being held Yes ☐ **No** ☐

Signed……(Parents must sign for children under 16)

Date

If consent is not given we will be unable to contact you