**GDPR Compliance Questionnaire**

**The Sport and Recreation Alliance has produced a range of resources, advice notes and templates to help you on your journey towards compliance with the General Data Protection Regulation (GDPR).**

**This compliance questionnaire is designed to help you ask the right questions as you think about how your organisation uses personal data and whether you comply with GDPR.**

**The checklist of things to consider within each section should be seen as suggestions of measures and processes that might be relevant for your organisation to consider, rather than as an exhaustive list; the more broadly you can think about each question, the more helpful this questionnaire will be.**

**Questionnaire completed by Graham Urquhart, Octavian Droobers 18 May 2018 to guide GDPR preparation.**

|  |  |  |  |
| --- | --- | --- | --- |
| **No.** | **Question** | **Checklist of things to consider** | **How is compliance demonstrated?** |
|  | Data Protection Officer (DPO) | | |
|  | Has a DPO been appointed? | * Organisation has carried out an assessment to determine whether the triggers for appointing a DPO have been met i.e. either (i) the organisation is a public authority; (ii) the organisation’s core activities consist of processing special categories of personal data or information about criminal convictions and offences on a large scale; or (iii) the organisation monitors personal information systematically or regularly as part of its core activities on a large scale. If no DPO has been appointed, reasons why have been recorded. □ * If no DPO is appointed, GDPR working group has been implemented. □ * Job descriptions of those members of staff who have additional responsibilities for GDPR compliance have been updated. □ * Process established so that the organisation can continue to monitor and review its approach to personal data processing going forward, particularly where there is a change in systems and processes □ | The club has not appointed a DPO as none of the triggers apply. The Chairman of the club (or an appointed deputy) will be the point of contact for Data Protection issues  This is the OD committee.  The club has no staff and so this does not apply. Volunteers’ and officers’ responsibilities are set out in the Privacy policy  The use of data by the club is set out in the privacy policies and Data Privacy Notices. These will be reviewed as a part of the regular Clubmark renewal and this questionnaire is revisited at that time. |
|  | Processing Data | | |
|  | What uses does the organisation make of personal data? | * Data mapping process carried out to understand and record the personal data flows and uses to, within and from the organisation. □ * Data mapping template/record of processing activities documented □ * Record of processing activities documents what parts of the organisation process or hold special categories of personal data (i.e. data relating to an individual’s racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union activities, physical or mental health, genetic or biometric details, sexual life or details of criminal offences.) □ * Additional security measures for special categories of personal data have been implemented □ * Procedures implemented to ensure personal data is accurate and up to date □ * Organisation has determined how it is going to treat historic personal data it holds □ | The data flows are on Appendix 1 below.  In view of the simplicity, a template has not been used  Appendix 1  There are special handling measures for medical conditions and for volunteer clearance records.  The club relies on British Orienteering (BO) to maintain membership information for its members and relies on this as the system of record.  Results are held indefinitely but contain limited information.  Lapsed members data is held for up to 6 years. |
|  | Does the organisation systematically monitor publicly accessible data on a large scale? | * If yes, CCTV usage notice and associated privacy notice for the public have been prepared □ | Rarely. Where it is used (say to record an event start or finish) it is restricted to participants who consent. Covered in the Privacy Notices.. |
|  | Is personal data processed or accessed outside the EEA? | * GDPR compliance for offices/branches/group members outside the EEA has been considered □ * Necessary protections have been implemented i.e. binding corporate rules, privacy shield, adequacy decision or appropriate safeguards including data processor contracts □ | No |
|  | Policies | | |
|  | What policies does the organisation have in place in relation to data protection compliance and have these been updated to take account of GDPR? | The organisation has the following policies in place:   * Internal Data Protection Policy (to inform members what they can and cannot do with personal data and cover GDPR compliance (including right to be forgotten, subject access requests, objections to processing, consent withdrawals, verbal exercise of rights). | * This is set out in the privacy Policy. |
|  | What privacy notices are used by the organisation, do they satisfy the new requirement of transparency in processing and where are they featured? | * External Facing policy. * Privacy Notice – For participants □ * Privacy Notice – For Members □ * Timing and provision mechanism implemented to ensure privacy notices are sent out either at first point of contact if the personal data is collected directly or at first point of contact/within one month where data is collected indirectly □ | Yes  Yes  Yes  TDB – membership and entry form changes to make this clear. What about Fabian entries?  Fabian 4 has a privacy policy but I think it should be updated for GDPR. Worth an e-mail to ask him about it (we presumably won't be the first) |
|  | Security and IT | | |
|  | Does the organisation have adequate physical and IT security procedures to protect personal data and has it implemented technical and organisational measures to show that it has considered and integrated data compliance measures into its data processing activities? | * Physical security review carried out –both for IT systems and physical systems/records □ * Additional security measures implemented to restrict access to personal data to only those who need access. □ * Use of pseudonymisation to protect personal data considered where appropriate, i.e. processing personal data in a way which does not allow identification of the individuals without the addition of other data □ * Additional security for special categories of data/criminal history data implemented □ * IT systems and their compatibility with GDPR have been reviewed. □ * Process established so that all decisions regarding security are to be reviewed regularly by GDPR working group and recorded accordingly □ | The club maintains 3 IT systems:   * The web site is restricted to public domain information and contains published Personal Information. It has the potential for member registration which would then include member names. It is an external service managed by the webmaster and relies on the security of the provider. * The email service provides a method of contact for members and contains names and email addressed. This is an external service managed by the webmaster and relies on the security of the provider. * The event equipment is a specialised set of computer and other equipment for timekeeping. It contains member information (names, gender, age, contact details, entry details, performance and results.). This equipment is fully isolated and is never directly connected to an external network. Security relies on the physical security of the equipment and passwords. |
|  | Are all mobiles phones, laptops and tablets tracked in the asset register, pin or password protected, encrypted and remotely wipeable. | * Encryption/remote wipe measures for mobile devices implemented □ * Asset register updated □ * Relevant provisions about the use of remote devices and any remote access included within IT policy and staff handbook □ * Use of removable storage restricted □ | The club makes use of none of this equipment for its data.  Event equipment is covered above in 4.2 |
|  | What protections are there against accidental loss, damage or destruction? | * Robust and frequent back up and disaster recovery procedures are in place □ * Backups are retained for a sufficient period of time to protect against progressive corruption of data □ | Key data is shared with BO and will be recovered form there if necessary |
|  | Does the organisation use a public cloud provider to store or share data? | * Security arrangements for cloud or third party servers have been put in place □ * Data processing agreement is in place with cloud provider □ * Where there is a transfer/storage of personal data outside EEA, necessary protections have been implemented i.e. binding corporate rules, privacy shield, adequacy decision or appropriate safeguards including data processor contracts □ | The data placed into these services is in the public domain. |
|  | Data retention, classification and destruction | | |
|  | Does the organisation have documented data retention periods and are they followed? | * Data Retention Policy and matrix implemented □ * Data retention periods have been captured in all privacy notices □ | Yes. Data is retained 6 years after leaving the club; results are retained indefinitely. Some specialist data has short retention (event entries, medical conditions etc.). Set out in the Privacy Notices |
|  | Can the organisation distinguish between data held as a data controller and data held as a data processor? | * Distinction has been captured in the data mapping template/record of processing activities □ | Event data OD are controller.  Membership data we are processor and BO is controller |
|  | When physical data/records are no longer required, are they securely destroyed? | * Security of data destruction – both hard copy and electronic □ * Security of IT asset destruction □ * Distinction made between confidential waste and non-confidential waste □ | Paper forms and medical conditions are shredded (in organisers instructions)  No IT assets outside event system,  Event system: Ad hoc processes for disposal of data storage devices on a case by case basis. |
|  | Training | | |
|  | Do all staff and volunteers receive data protection training as part of their induction and at least once every 12 months? | * Implementation of a GDPR training programme (train the trainer) □ * Future induction GDPR training implemented □ * Ongoing GDPR refresher training implemented □ * Senior management and members of the main board have received training on GDPR □ | As volunteers only work occasionally, this training is provided on specific events.  We should add this to the organiser, membership, results and other instructions.  We need to do officers training for Chair, Membership secretary, Marketing, webmaster and results. |
|  | Do staff processing larger volumes of personal data or special categories of personal data (e.g. health and disability data for participants or details of any criminal offences) have more detailed training, e.g. HR, Coaching, Performance, Membership, IT? | * Enhanced GDPR Training has been undertaken by heavy/frequent personal data users □ | No |
|  | Is non-compliance with the various polices linked to the potential for disciplinary action in relation to staff? If so, how is this achieved, e.g. policies form part of staff handbook? | * GDPR compliance linked to potential disciplinary measures/staff handbook □ * Employment contract updated □ | The club has no staff. The ClubConstitution contains provisions for discipline of members |
|  | Data Protection Impact Assessment (DPIA) | | |
|  | Have any higher risk data processing activities been identified? | Assessment process carried out for any processing that is likely to result *“in a high risk to the rights and freedoms of natural persons.”* i.e. the organisation:   * Uses systematic and extensive profiling or automated decision-making to make significant decisions about people. □ * Processes special category data or criminal offence data on a large scale. □ * Systematically monitors a publicly accessible place on a large scale. □   *[The following nine criteria should be considered, in order to establish whether the organisation’s processing operations require a DPIA due to their inherent high risk. A data controller can consider that a processing activity meeting two of the below criteria would require a DPIA to be carried out:*   * *Evaluation or scoring.* * *Automated decision-making with significant effects.* * *Systematic processing* * *Sensitive data or data of a highly personal nature.* * *Processing on a large scale.* * *Matching or combining datasets e.g. originating from two or more data processing operations performed for different purposes and/or by different data controllers* * *Processing of data concerning vulnerable data subjects* * *Use of innovative technological or organisational solutions.* * *Processing involving preventing data subjects from exercising a right or using a service or contract.]*   Where it has been decided not to carry out a DPIA, reasons have been documented. ☐  New DPIA to be carried out if there is a change to the nature, scope, context or purposes of our processing. ☐ | The club does no activities of this nature requiring a DPIA at present.  No  No. Very small scale  No  No  No  No  No  No  No  Yes – very rare. Where vulnerable subjects are encountered (rarely) these are excluded from services by exception to protect location data  No  No  Yes  Yes if triggered by the nature of the new processing |
|  | Consent | | |
|  | Is consent required for any processing? | * Explicit consents obtained for all direct marketing ☐ * Privacy notices updated to ensure consents are obtained where needed in respect of special categories of data ☐ * Processes in place to deal with and action all requests for consent to direct marketing communications to be withdrawn☐ | Yes – on membership and entry forms  Subject initiates these activities  Yes. Via mail server (email) and membership secretary (paper mail) |
|  | If no consent is not required or obtained, which grounds for processing will be relied on?  Consider:  - for the performance of a contract to comply with legal obligations  - to protect vital interest of the individual  - pursuing legitimate business interests  If any of these apply please provide an explanation of the position. | * Data categorisation recorded in data mapping/ record of processing activities☐ * Future planned data processing activities added to record of processing activities ☐ | Entry form information is used to protect the vital interest of the individual and the data is used solely for the event duration. |
|  | Sharing/Receiving data from third parties | | |
|  | Does the organisation appoint any third parties as data processors? | * List of third party data processors added to record of processing activities☐ * GDPR supplier audit carried out ☐ * GDPR compliant data processing agreement in place with suppliers/contractors where commercially feasible ☐ | British Orienteering maintain their membership database and this is the primary record of OD club membership. They provide this information to the club as a regular update and this is our membership record and we use the membership details for other BO members. We rely on their GDPR compliance as data controller for this data.  Fabian4 gather entry details and pass these to OD. We rely on their GDPR compliance as data processor on our behalf. |
|  | Does the organisation act as a data processor for any third parties? | * Arrangements put in place where acting as a data processor for third parties ☐ | No |
|  | Does the organisation share or receive personal data with any other third parties where neither party is processing data on the other’s behalf? E.g. HMRC, pension providers, public registers etc. | * Organisation has determined how personal data is processed with another data controller i.e. as joint data controller ☐ * Terms with data controllers considered.☐ * Where personal data has been obtained indirectly from other sources, privacy notices include provisions confirming source of data. ☐ * Any framework contracts have been updated to incorporate new GDPR provisions☐ | No |
|  | Rights of individuals | | |
|  | Is there a Subject Access Request Policy? If not, does the organisation have a clear and known process to deal with Subject Access Requests (SARs)? | * Subject access right procedure developed/tested ☐ * Separate procedures manual for data subject rights considered. ☐ * Data protection policy updated to reference subject access requests☐ | SARs will be directed to the Chairman and responded to on an ad hoc basis. |
|  | What is the process for the organisation to respond to requests:  (i) to rectify inaccurate personal data about an individual;  (ii) under the right to be forgotten;  (iii) to restrict processing; or  (iv) for data to be ported? | * Subject right procedures developed/tested ☐ * Separate procedures manual for data subject rights considered ☐ * Data protection policy updated to reference subject access requests ☐ | Rectification of most data will be directed to BO, who are the data controller and maintain the data.  The right to be forgotten will exclude data already placed in the public domain., |
|  | Data Protection Supervisory Authority (DPSA) | | |
|  | Have you identified which DPSA will oversee your data processing activities? | * i.e. Information Commissioner’s Office | No. We would contact the ICO if necessary. |
|  | Children | | |
|  | Does the organisation hold or process personal data relating to children between 13 years - 16 years old? | * Child-friendly privacy notices prepared and provided☐ * Process implemented to obtain consents from parents or guardians of children if needed ☐ | No.  do we have this in place.  I believe we do as Junior activities outside of our events (coaching, travel to junior only events such as Peter Palmer Relays, Junior socials) all require parental consent forms. |
|  | Compliance programme | | |
|  | Does the organisation have regular GDPR compliance audits? | * GDPR compliance internal auditing function and frequency considered ☐ | No. GDPR compliance is a standing item on the AGM meeting.  After initial period can we say that this will be done as part of the annual Clubmark review ? |
|  | If so who is responsible for carrying out the audits? | * i.e. DPO or GDPR working group has been formed | N/a |
|  | What are the organisation’s processes for ensuring that policies are reviewed and updated on a regular basis? | * GDPR compliance internal auditing function and frequency considered ☐ | Linked to the regular update of the Clubmark processes |
|  | Are all records of the organisation collated or easily accessible to demonstrate the steps taken to ensure compliance with GDPR? | * GDPR accountability record/evidence holding system established ☐ | ? what should we do for this. Private area of the website?  Where are these records stored ? If they are currently private and only on Mike's laptop then any data stays there.  If it is the compliance process that is being demonstrated then this would not contaoin any personal data so could go on the web site or in the Committee and AGM minutes. I don't really like the idea of a private part of the OD website as this requires administering. |

# Appendix 1 – Data flows

# Membership data

Data is collected for the purposes of administering membership form the member on paper. This is shared with British Orienteering (BO) as the applications for both organisations. The data relates to name, gender, age, contact details and preferences. The paper is retained by the membership secretary. The data is entered by BO into their computer systems as Data Controller and is maintained there. OD receive extracts of this data and do not maintain a master copy. The extracts are used to:

* Prepare mailing address labels to contact members and provide the services included in membership. There is an opt-out capability to be excluded from this list ?.
* Maintain an email contact list for mail circulation relating to the club’s events and services. This has an opt-out capability to be excluded from this mail.
* Prepare a contact list which is published annually on paper to all members of names, addresses, telephone numbers and email addresses (where these have been supplied to the club). There is an opt-out capability to be excluded from this list.
* Validate membership (I would put this as the first item in the list)

# Data relating to members of affiliate clubs and British Orienteering

British Orienteering and online entry providers (such as Fabian4) provide the club with member data (see above) and also data relating to other competitors who are not club members (some of whom are members of BO), for the purpose of managing entries and validating BO membership. Struggling to word this better as entry information has both BO member and non-member data in it.

The BO data is transferred at regular intervals onto the club’s results equipment to maintain the accuracy of the data used at event. The online entry provider data is supplied in relation to a single event only.

The data is stored on the club’s event time keeping/entry management equipment. It is used to:

* Facilitate entries
* Associate entries with BO membership where relevant
* Publish accurate results
* Contact lost competitors as part of the safety procedures
* Retrieve equipment hired at the event that has not been returned.

# Data relating to members and non-members at specific events

Members of the club, BO and the public may enter events. The club collects information to facilitate the event and the safety of the competitors for each event either directly form the competitor or through a service partner who collects the information form the competitor and retransfers this to the club. Where the club collects the data, standard paper entry forms are used which also provide an opportunity for the entrant to receive further marketing information from the club on an opt-in basis. These form a part of the safety system for the event, and are stored by the event’s organiser or the results team leader. These are then destroyed after 60 days.

Data from the entry may be transferred into the club’s event systems and will be used to prepare:

* Printed results published at the event and on the club’s web site
* Result information for BO for publication
* Result analysis at a number of sites including RouteGadget and WinSplits

The club may retain results as published and the details in the club’s event systems indefinitely as a part of the club’s archive.

# Medical and other incidents

If an incident occurs at an event that results in injury requiring treatment or other disputes a record will be made of the details of the incident and the identities of people involved to support treatment, to maintain a record of actions and improve services. This may include sensitive medical information and the identities of several people. This information is passed to BO following the event for record keeping and insurance purposed and is not kept by club.

Entrants are offered the opportunity to provide details to the event organiser of any medical conditions that might impact their safety and to inform first aider’s in the event of illness or accident. This is provided in a sealed envelope by the competitor and is only opened in the event of an incident. If unopened the envelope is returned to the competitor at the end of the event or failing that destroyed within 7 days. If the information is used it will become part of the incident record.

# Marketing

The club may contact non-members (based on an opt-in) to encourage participation and membership.

Some personal details that are already in the public domain (including names and pictures) may be used by the club in its own publicity and in publicity provided to publications such as magazines, newspapers and event details.

# Officers and volunteers

The club makes use of records of the experience and skills of members in specific roles which are maintained by BO and may use this assess the qualification of members for these roles.

For some roles additional checks are made on suitability of volunteers. The club maintains the results of these checks and retains them for 6 years after the member has left the club. These are held by <who> I am pretty certain that the record of those that have been DBS checked for orienteering is held by BOF not by the club, and this list is accessible by those who need it.

I don't know of any other specific checks as First Aid would come under the first section as a qualification rather than a check.