West Lothian Sports Council

GDPR – a Primer for Sports Clubs

What is GDPR?

- GDPR = General Data Protection Regulation
- New EU regulation that replaces Data Protection Act
- Designed to give individuals better control of their data

- Implementation date: **25 May 2018**
- **Anyone who processes Personal Data must comply with GDPR from this date**

- Serious consequences for breaches (fines up to 20 Million Euros).
- Applies to “Processors” as well as “Controllers”
- Lots of guidance: https://ico.org.uk/for-organisations/
- **This presentation is not legal advice!** If in any doubt ask your governing body for help / support.

What is Personal Data

- "Personal Data" Information about a living person (called a 'data subject') who can be identified (directly or indirectly) from it, including:
  - Obvious things: names / addresses / phone numbers / DOB
  - Less obvious things: Registration numbers / race numbers / IP addresses
  - And even: physical / mental / physiological / cultural things that could be linked back to a specific individual
- Even stricter rules about (i) Children and (ii) Sensitive Personal Data.
- "Controller" = 'controls' the personal data and determines the purpose and method of processing
- "Processor" = 'processes' personal data on behalf of a controller
- "Processing" = anything you could do with personal data.
  - Includes: 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

GDPR – Data Protection Principles

- #1 Lawfulness, fairness and transparency
  Transparency: tell the subject what data processing will be done. Fair: what is processed must match up with how it has been described. Lawful: Processing must meet the tests described in GDPR.
- #2 Purpose limitations
  Data can only be used for a specific processing purpose that the subject has been made aware of and no other, without further consent.
- #3 Data minimisation
  The minimum amount of data should be kept for specific processing.
- #4 Accuracy
  Data must be “accurate and where necessary kept up to date”
- #5 Storage limitations
  Data should only be kept as long as actually required (and then deleted / removed.
- #6 Integrity & Confidentiality
  Keep it safe. Take appropriate technical and organisational measures to protect it. Notification to ICO (and possibly data subjects) on breach.
- Also … Article 5(2): Accountability
  Controller is responsible for, and should be able to demonstrate, compliance with the principles
- Also … Data Subject Rights
  A range of rights: informed / access / rectification / erasure / restrict processing / portability / object / automated decision making & profiling.

Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now

1 Awareness

You should make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have.

2 Information you hold

You should document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit.

3 Communicating privacy information

You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.

4 Individuals' rights

You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.

5 Subject access requests

You should update your procedures and plan how you will handle requests within the new timescales and provide any additional information.

6 Lawful basis for processing personal data

You should identify the lawful basis for your processing activity in the GDPR, document it and update your privacy notice to explain it.

7 Consent

You should review how you seek, record and manage consent and whether you need to make any changes. Refresh existing consents now if they don't meet the GDPR standard.

8 Children

You should start thinking now about whether you need to put systems in place to verify individuals' ages and to obtain parental or guardian consent for any data processing activity.

9 Data breaches

You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.

10 Data Protection by Design and Data Protection Impact Assessments

You should familiarise yourself now with the ICO's code of practice on Privacy Impact Assessments as well as the latest guidance from the Article 29 Working Party, and work out how and when to implement them in your organisation.

11 Data Protection Officers

You should designate someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements. You should consider whether you are required to formally designate a Data Protection Officer.

12 International

If your organisation operates in more than one EU member state (ie you carry out cross-border processing), you should determine your lead data protection supervisory authority. Article 29 Working Party guidelines will help you do this.

ico.
Information Commissioner's Office

ico.org.uk

What do we have to do in practice?

Requirement	Practical Steps
• Lawfulness, fairness and transparency • Purpose limitations • Data minimisation • Storage limitations • Accountability	Identify all personal data held by the club and what it is used for. Create a table or spreadsheet, which can be used to maintain the required records of processing activities.
• Lawfulness, fairness and transparency • Purpose limitations • Accountability	Create a privacy notice. Update club forms, websites, etc. to include the new privacy notices and issue these to current members, competitors, employees, etc. Harper Macleod: Sport Scotland template
• Accountability • Integrity & Confidentiality	Ensure that everyone in the club with access to personal data has a basic understanding of data protection and the club's obligations under the GDPR.

What do we have to do in practice?

Requirement	Practical Steps
• Accountability • Integrity & Confidentiality	Adopt higher standards of data security. E.G.: • create specific club email accounts to limit the use of personal email address for club business. • Store electronic data securely – passwords, encryption etc. • Store paper documents securely – lock it up. Don't work on it in public. • Don't share personal data by email
• Accountability • Integrity & Confidentiality	Ensure you have a contract with suppliers (processors who you might share personal data with ie; timing chip service providers) – some mandatory points they must cover. Harper Macleod: template wording
• Lawfulness, fairness and transparency	Make sure you get "opt in" consent for marketing Consider system for sending marketing emails

Example Data Audit

	A	B	C	D	E	F	G	H	I
1	Create a list of all data that you use in your role.	Processor or Controller	Where do you get this data from?	Legal basis identified or consent granted?	Where do you store this data?	What do you use this data for?	Do you share this data with anyone?	Retention Period	Comments / Actions
2	Club Senior Member Data: - Name - Address - Email - Phone Number - DOB - Gender - ICE contact name and phone number - Any relevant medical conditions that might affect training - Triathlon Scotland Number	Controller	Club members complete on membership application forms	Consent given and Legal basis identified: contractual and legitimate interest (health & safety). The data is used to administer club membership and ensure the safety of our members.	Google Drive - in the club membership register. We also store the member's names in the training register (in training folder and membership secretary's laptop). Hard copy forms are stored securely by the Club Treasurer.	Administration of the club membership: - club member database kept - contact member about club sessions - contact member about club event - renewal reminders - expiry notices - to track attendance and fees due etc for accounts	No, only the club office bearers have access to this data	For as long as that person remains a member. 3 years after the membership ceases.	Circulate privacy notice and attach it / refer to it in the application form for future years.
3	Club Junior Member Data: - Name & Parent/Guardian Name - Address - Email - Phone Number - DOB - Gender - ICE contact name and phone number - Any relevant medical conditions that might affect training - Triathlon Scotland Number	Controller	Club members complete on membership application forms. All junior member's forms have parental consent section	Consent given and Legal basis identified: contractual and legitimate interest (health & safety). The data is used to administer club membership and ensure the safety of our members.	Google Drive - in the club membership register. We also store the member's names in the training register (in training folder and membership secretary's laptop). Hard copy forms are stored securely by the Club Treasurer.	Administration of the club membership: - club member database kept - contact member about club sessions - contact member about club event - renewal reminders - expiry notices - to track attendance and fees due etc for accounts	No, only the club office bearers have access to this data	For as long as that person remains a member. 3 years after the membership ceases.	Circulate privacy notice and attach it / refer to it in the application form for future years.
4	Competitor (at one of our events) data: - Name - Address - Email - Phone Number - DOB - Gender - ICE contact name and phone number - Club affiliation - Triathlon Scotland (or other) number	Controller	Entry Central	Legal basis identified: contractual and health & safety. The data is used to communicate with competitors and run events, provide timing and results and make sure we have emergency contacts in case of any acidents.	Entry Central (who have GDPR compliant terms and policies), Google Drive and results (names and ages and event times) on our website and Facebook page. Data also stored on laptop to prepare for event and help facilitate registration at the event etc.	Set up, running and commucation about events. The data is used to communicate with competitors and run events, provide timing and results and make sure we have emergency contacts in case of any acidents.	Club office bearers have access to the master list of the data and on Entry Central. Some data is shared with the timing chip provider (see comments). Some limited data is displayed at the event (names, age categories etc) for the purpose of organising heats etc. Limited results data is shared publically and more detailed results are also shared with Triathlon Scotland.	12 months after the date of the event (to allow us to email previous year's competitors to inform them of the next year's event) Data deleted from laptop after event results processed.	Prepare and issue addendum/contract to timing chip company to cover off GDPR risk. Make sure that privacy policy is linked to from Entry Central and that it covers the uses described here.
5	Club Member (including guardians) mobile number and email addresses	Controller	Club members complete on membership application forms or club member tells office bearers this information	Consent given and legal basis identified: contractual.	Lots of club members share this information with each other and store on their personal mobile phones and email accounts etc.	Communicating between and with members about club business, including training, meetings, upcoming events etc. Members can join the GRC Facebook group and also the GRC WhatsApp group - but they can leave these at any time.	No.	n/a	None
6	Club email / messages on Facebook etc	Controller	Anyone who wants to contact the club may email us with queries etc and the contact may include personal data.	Consent given and legal basis identified: contractual.	Emails stored in Outlook.com. Facebook messages stored on Facebook.	Only used to reply to people who contact us and provide any follow on services or information etc.	No, only the club office bearers have access to this data	3 years for email. No control over Facebook messages.	Investigate rules / process to delete old emails etc.
7	Volunteer or Official (at one of our events or training sessions) data: - Name - Address - Email - Phone Number	Controller	Volunteer details usually passed to office bearer by club member. Official details normally sent by Triathlon Scotland.	Consent given and legal basis identified: contractual.	Google Drive - in the loist of volunteers / officials for each event	Set up, running and commucation about events. The data is used to communicate with volunteers and officials and run events.	No, only the club office bearers have access to this data	12 months after the date of the event (to allow us to email previous year's volunteers to inform them of the next year's event)	None
8									
9									
10									
11									
12									
13									
14									
15									