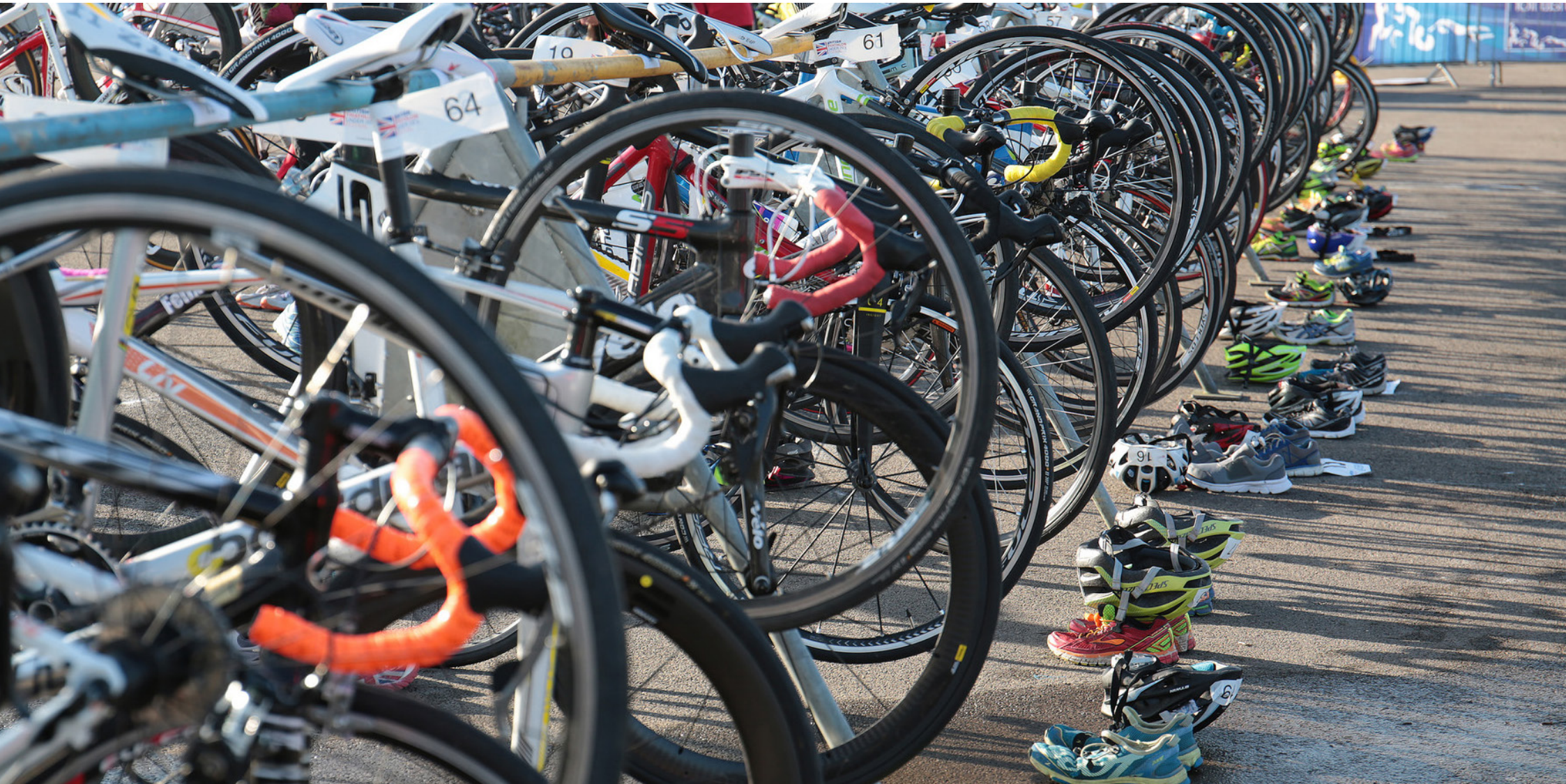
GENERAL DATA PROTECTION REGULATION [GDPR]

WHAT YOU AND YOUR CLUB NEEDS TO KNOW

BRITISH TRIATHLON



GENERAL DATA PROTECTION REGULATIONS

The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU). This change will be incorporated into UK law under the Data Protection Bill on the 25th May 2018.

For a full guide to the GDPR please go to the Information Commissioners Office (ICO) website
https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

The Government has confirmed that GDPR will not be affected by "BREXIT" i.e. you cannot ignore it.

This change in law is driving some significant changes around data protection and how organisations handle personal information, why this information is held and what action we take with such information.

Whilst it is easy to see why large multi-nationals need to adopt tighter controls on personal data, surely a small triathlon club doesn't need to worry about this? Wrong!

The GDPR applies to any data controllers or data processors, so if you collect any personal information in the running of your triathlon club then the GDPR WILL apply to you.

BRITISH TRIATHLON ARE COMMITTED TO SUPPORTING ITS CLUBS AND MEMBERS DURING THIS IMPLEMENTATION AND AS SUCH THE FOLLOWING PAGES WILL PROVIDE;

- Guidance and Advice
- Additional Sources of Support
- FAQ's

Whilst we will do all we can to support, we cannot offer a tailored compliance service to your individual club and you may need to seek independent advice and guidance.

SO, HOW DOES THIS APPLY TO YOUR TRIATHLON CLUB?

The GDPR applies to organisations that take personal data from its customers or members, for example via manual or electronic based formats e.g. member forms, online platforms or a club website.

It relates to how the club not only obtains personal information but how it then stores and uses this data.

ALL CLUBS NEED TO ENSURE THAT WHEN DEALING WITH PERSONAL DATA:

THEY PROCESS IT SECURELY

IT IS UPDATED REGULARLY AND ACCURATELY

IT IS LIMITED TO WHAT THE CLUB NEEDS

IT IS USED ONLY FOR THE PURPOSE FOR WHICH IT IS COLLECTED

IT IS ONLY USED FOR MARKETING PURPOSES IF THE INDIVIDUAL HAS GIVEN THE CLUB CONSENT TO DO SO

The principles of data protection set out within the existing Data Protection Act still exist and, therefore, if you are compliant with this, it is likely you will only have a few changes to make to fall in line with the new GDPR regulation.

HOW DO YOU KNOW WHAT IS PERSONAL DATA?

PERSONAL DATA CAN BE DEFINED AS ANY INFORMATION RELATING TO:

- A natural person*.
- The data subject, who can be directly or indirectly identified by the use of that data; for example, by their name, ID number, or online identifier such as an email address.

*A **natural person** is a **person** (in **legal meaning**, i.e., one who has its own **legal** personality) that is an individual human being, as opposed to a legal person, which may be a private (i.e., business entity or non-governmental organisation) or public (i.e., government) organisation.

SENSITIVE PERSONAL DATA CAN BE DEFINED AS:

- Any information consisting of racial or ethnic origin,
- Political opinions,
- Religious or philosophical beliefs,
- Trade union membership,
- Genetic data, biometric data,
- Data concerning health
- Data concerning a natural person's sex life or sexual orientation.

The GDPR relates to members who are participants at your club, coaches, referees, volunteers, parents and any individual that you request personal data from or hold data on.

BE TRANSPARENT

Personal data must always be processed fairly and lawfully and with transparency at the forefront of all processing.

All clubs should be aware that being transparent is a key requirement of the GDPR. Your Club will need to ensure they have solid and documented justification for how you use personal data e.g. keeping a record of consent from the member that they are happy to receive marketing/ promotional material from the Club.

DATA PROTECTION FINES

Under the GDPR, the potential values of fines have increased significantly. Under the current regime, the highest fine the ICO can levy is £500,000. Under the GDPR, they will be able to issue fines up to 20 million Euros or 4% of your annual turnover (whichever is the highest) for serious breaches. The fine could be 10 million Euros or 2% of your annual turnover (again, whichever is the highest) for less serious breaches.

THE 12 STEPS TO PREPARING FOR THE GDPR

The ICO recommends all organisations to take the following steps to help prepare for the GDPR implementation (as per the ICO website)
https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf

WE HAVE BUILT ON THE 12 STEPS BELOW TO GIVE MORE SPECIFIC ADVICE/GUIDANCE DIRECTED TOWARDS CLUBS.

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 and identify areas that could cause compliance problems under the GDPR. It would be useful to start by looking at your organisation's risk register, if you have one.

CLUB ACTION

EACH CLUB SHOULD;

1. Identify who will be your data protection lead;
2. Identify how you will communicate with your members and where relevant, your race entrants, the impact that the GDPR will have on your Club;
3. Agree and communicate who members should contact regarding data protection issues; you might consider having a separate committee post to cover data protection depending on the size of your club;
4. Make sure that your volunteers and coaches are also aware of the GDPR and data protection issues and that they know who to talk to if they were to receive a Subject Access Request (see point 5 below).

FURTHER READING

ICO Guide to the General Data Protection Regulation (GDPR)

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

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 across the organisation or within particular business areas. The GDPR requires you to maintain records of your processing activities. It updates rights for a networked world. For example, if you have inaccurate personal data and have shared this with another organisation, you will have to tell the other organisation about the inaccuracy so it can correct its own records. You won't be able to do this unless you know what personal data you hold, where it came from and who you share it with. You should document this. Doing this will also help you 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 and procedures in place.

CLUB ACTION

Each Club should establish whether your current policies and procedures are suitable to comply with the GDPR and if not, you should alter and update them.

EACH CLUB SHOULD START A REVIEW (OR DATA AUDIT) TO ASSESS AND IDENTIFY;

1. What personal data is held by the Club;
2. Is the data actually needed;
3. Where does the data come from;
4. Basis on which it was collected;
5. Is it shared with anyone and if so, how and why and in what format;
6. How is that data held, used, stored and disposed of;

Each Club should carry out a Data Audit which will help your Club to identify and document the above. It is key that you bring in key Club Members such as Memberships Officer, Coaches, Event Managers etc. This will allow your audit to be as thorough as possible. A sample Data Audit Template is provided in the Additional Resources section towards the end of this guide.

FURTHER READING

ICO DATA PROTECTION PRINCIPLES

https://ico.org.uk/for-organisations/guide-to-data-protection/data-protection-principles/

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. When you collect personal data you currently have to give people certain information, such as your identity and how you intend to use their information. This is usually done through a privacy notice. Under the GDPR there are some additional things you will have to tell people. For example, you will need to explain your lawful basis for processing the data, your data retention periods and that individuals have a right to complain to the ICO if they think there is a problem with the way you are handling their data. The GDPR requires the information to be provided in concise, easy to understand and clear language. The ICO's Privacy notices code of practice reflects the new requirements of the GDPR.

CLUB ACTION

1. If your club does not currently have a privacy notice/statement then you must create one. A template can be found below. You should consider how you are going to make this available to your members.
2. If you have a junior section, you will need to ensure you have a version that is suitably accessible and understandable to them.

FURTHER READING

ICO PRIVACY NOTICES, TRANSPARENCY AND CONTROL

https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/

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.

The GDPR includes the following rights for individuals:

- THE RIGHT TO BE INFORMED
- THE RIGHT TO RECTIFICATION
- THE RIGHT OF ACCESS
- THE RIGHT TO ERASURE
- THE RIGHT TO OBJECT
- THE RIGHT TO DATA PORTABILITY
- THE RIGHT TO RESTRICT PROCESSING
- 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. If you are geared up to give individuals their rights now, then the transition to the GDPR should be relatively easy. This is a good time to check your procedures and to work out how you would react if someone asks to have their personal data deleted, for example. Would your systems help you to locate and delete the data? Who will make the decisions about deletion?

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

- to 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.

You should consider whether you need to revise your procedures and make any changes. You will need to provide the personal data in a structured commonly used and machine readable form and provide this free of charge.

4 INDIVIDUALS' RIGHTS (CONTINUED)

CLUB ACTION

1. The GDPR gives far greater control over how, as a Club, you process a Member's details.
2. As a Club you should start to consider how you will respond to any Club Member or Event participant wishing to exercise their rights per the above list from the ICO.
3. Identify which individuals would be required to action any activities.
4. Devise a process flow and create templates ahead of any action required.

FURTHER READING

ICO GUIDANCE ON THE RIGHTS OF INDIVIDUALS

https://ico.org.uk/for-organisations/guide-to-data-protection/principle-6-rights/

5 SUBJECT ACCESS REQUESTS (SAR)

You should update your procedures and plan how you will handle requests to take account of the new rules;

- In most cases you will not be able to charge for complying with a request
- You will have a month to comply, rather than the current 40 days
- You can refuse or charge for requests that are manifestly unfounded or excessive
- If you refuse a request, you must tell the individual why and that they have the right to complain to the supervisory authority and to a judicial remedy. You must do this without undue delay and at the latest, within one month.

CLUB ACTION

1. Your Club must action a Subject Access Request.
2. Your Club should devise and document a procedure to follow for when you receive a Subject Access Request.
3. Ensure you are able to access copies of personal data held and remember it is both paper and digital formats.
4. SAR's are often contentious and can often lead to a complaint.

FURTHER READING

ICO RIGHT OF ACCESS

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/

6 LAWFUL BASIS OF 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. Many organisations will not have thought about their lawful basis for processing personal data. Under the current law this does not have many practical implications. However, this will be different under the GDPR because some individuals' rights will be modified depending on your lawful basis for processing their personal data. The most obvious example is that people will have a stronger right to have their data deleted where you use consent as your lawful basis for processing. You will also have to explain your lawful basis for processing personal data in your privacy notice and when you answer a subject access request. The lawful bases in the GDPR are broadly the same as the conditions for processing in the DPA. It should be possible to review the types of processing activities you carry out and to identify your lawful basis for doing so. You should document your lawful bases in order to help you comply with the GDPR's 'accountability' requirements.

CLUB ACTION

1. Complete your data audit and review what information you hold.
2. It is highly likely that consent will be the most commonly used **Lawful Basis** by your club along with **Legitimate Interest** and/or **Contract**.
3. Review each type and decide carefully which basis is relevant to your club.
4. Document this on your data audit and ensure this is clearly communicated within your privacy notice/statement.

FURTHER READING

ICO LAWFUL BASIS OF PROCESSING

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/

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. You should read the detailed guidance (see link below) the ICO has published on consent under the GDPR and use our consent checklist to review your practices. Consent must be freely given, specific, informed and unambiguous.

There must be a positive opt-in – consent cannot be inferred from silence, pre-ticked boxes or inactivity. It must also be separate from other terms and conditions, and you will need to have simple ways for people to withdraw consent. Public authorities and employers will need to take particular care. Consent has to be verifiable and individuals generally have more rights where you rely on consent to process their data. You are not required to automatically 'repaper' or refresh all existing DPA consents in preparation for the GDPR. But if you rely on individuals' consent to process their data, make sure it will meet the GDPR standard on being specific, granular, clear, prominent, opt-in, properly documented and easily withdrawn. If not, alter your consent mechanisms and seek fresh GDPR-compliant consent, or find an alternative to consent.

CLUB ACTION

1. From your data audit, identify which datasets rely on consent as their lawful basis.
2. Do you have the right, GDPR-compliant consent for holding this information?
3. In order to contact your members for marketing purposes, you will have to have gained explicit consent. Make sure you have obtained this if you intend to send out marketing communications to Members.
4. Put in a clear process to allow members to withdraw their consent at any given point.

FURTHER READING

ICO GUIDE TO GDPR CONSENT

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/

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. For the first time, the GDPR will bring in special protection for children's personal data, particularly in the context of commercial internet services such as social networking. If your organisation offers online services ('information society services') to children and relies on consent to collect information about them, then you may need a parent or guardian's consent in order to process their personal data lawfully. The GDPR sets the age when a child can give their own consent to this processing at 16. However, the age currently being proposed in the UK's Data Protection Bill is actually 13. The GDPR gives countries some opportunities to make small changes to some areas for how the GDPR applies to their country and this is one that, at the current time, it looks like the UK will apply. If a child is younger then you will need to get consent from a person holding 'parental responsibility'.

CLUB ACTION

1. Update your processes so that parental consent is obtained when processing the data of anyone aged under 13.
2. Consider how your Club engages with young people in the online world.

FURTHER READING

ICO GUIDE TO GPR AND CHILDREN

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/applications/children/

9 DATA BREACHES

You should make sure you have the right procedures in place to detect, report and investigate a personal data breach. Some organisations are already required to notify the ICO (and possibly some other bodies) when they suffer a personal data breach. The GDPR introduces a duty on all organisations to report certain types of data breach to the ICO, and in some cases, to individuals. You only have to notify the ICO of a breach where it is likely to result in a risk to the rights and freedoms of individuals – if, for example, it could result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage. Where a breach is likely to result in a high risk to the rights and freedoms of individuals, you will also have to notify those concerned directly in most cases. You should put procedures in place to effectively detect, report and investigate a personal data breach. You may wish to assess the types of personal data you hold and document where you would be required to notify the ICO or affected individuals if a breach occurred. Larger organisations will need to develop policies and procedures for managing data breaches. Failure to report a breach when required to do so could result in a fine, as well as a fine for the breach itself.

Examples of a potential data breach are:

1. Accidently sending someone's personal information to the wrong email contact.
2. Your Clubs must develop and document a process on how to investigate potential data breaches and should consider.
3. Losing a club file that contains all the member registration forms for members in your club.
4. A cyber-attack on the computer system that contains personal information.

CLUB ACTION

1. Ensure you have in place data protection measures to safeguard members' personal information.
2. Develop and document a process on how to investigate potential data breaches and should consider;
    - The need for the Club to inform the individuals concerned.
    - The need to notify the ICO.

Failure to report a breach could result in a heavy fine, as well as one for the breach itself.

Look at creating a data-breach log. This should be maintained and retained by the nominated Club individual and passed on within any change in individuals.

FURTHER READING

ICO GUIDE TO DATA BREACHES

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

10 DATA PROTECTION BY DESIGN AND DATA PROTECTION IMPACT ASSESSMENTS

It has always been good practice to adopt a privacy by design approach and to carry out a Privacy Impact Assessment (PIA) as part of this. However, 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.

A DPIA is required in situations where data processing is likely to result in high risk to individuals, for example:

- where a new technology is being deployed.
- where a profiling operation is likely to significantly affect individuals; or
- where there is processing on a large scale of the special categories of data.

If a DPIA indicates that the data processing is high risk, and you cannot sufficiently address those risks, you will be required to consult the ICO to seek its opinion as to whether the processing operation complies with the GDPR.

CLUB ACTION

Your Club should start to assess the situations where it will be necessary to conduct a DPIA and should consider;

1. Who will do it?
2. Who else needs to be involved?

If your Club is considering putting in place a new system or electronic portal, you need to consider upfront whether the service provider you choose has adequate security to protect personal data.

You should review your clubs potential need for a simple Risk Register.

- Consider potential risks such as how your member information is retained? You could be at risk if you keep member information in a folder that is left unattended at a session or using a computer data system for this information but not having the correct encryptions or security safeguards in place.

FURTHER READING

ICO GUIDE TO PRIVACY BY DESIGN

https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-by-design/

ARTICLE 29

http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358

11 DATA PROTECTION OFFICERS

Not all organisations will need to appoint an official "Data Protection Officer", however, even if your Club does not need to, it would be sensible to designate someone to take responsibility for data protection compliance within your Club and assess where this role will sit within your organisation's structure and governance arrangements.

CLUB ACTION

1. Identify whether you are required to appoint a Data Protection Officer – see the ICO website.
2. Either way, each Club is recommended that they identify an individual to take responsibility for data protection compliance.
3. It is important that this individual is fully supported by your Club's Committee in order to carry out their role effectively.

FURTHER READING

ICO GUIDE TO DATA PROTECTION OFFICERS

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers/

12 INTERNATIONAL

The GDPR imposes restrictions on the transfer of personal data outside the European Union, to third countries or international organisations. These restrictions are in place to ensure that the level of protection of individuals afforded by the GDPR is not undermined. It is unlikely that this will be relevant to your club unless it operates outside of the European Union.

CLUB ACTION

It is unlikely that this will be too relevant to your club unless it operates outside of the European Union, however, it might be that some technology systems you use will operate from outside the EU and so you should double-check that they will be complying with the GDPR. For example, cloud systems and websites might have their servers in the USA. Check any websites you use for things like club email addresses, file storage, email communications.

FURTHER READING

ICO

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/

FREQUENTLY ASKED QUESTIONS

WHAT IS THE GDPR AND WHAT DOES IT MEAN FOR GRASSROOTS CLUBS?

The GDPR is an important change in government legislation regarding data protection and stands for The General Data Protection Regulation. It effectively provides an update to the Data Protection Act, bringing in new requirements and increasing the penalties for breaches. Any organisation that is required by law to comply with GDPR must do so by the 25th May 2018 at the latest.

Within this legislation there are some key changes that will affect all grassroots clubs and need to be addressed.

DOES THIS APPLY TO OUR CLUB?

The GDPR applies to any "data controllers" or "data processors". Those are technical terms but, in essence, if you collect any personal data in running your club (which you will do if you have any members) then the GDPR will apply to you.

MY CLUB IS ONLY A SMALL ONE WITH A FEW MEMBERS: SURELY THIS WON'T APPLY TO ME?

Although the risk is lower, if you collect and store any personal data you will have to manage the data in accordance with strong data protection principles and be GDPR compliant.

WHAT ARE THE KEY THINGS TO CONSIDER FOR GRASSROOTS CLUBS?

The principles of data protection still exist. All clubs need to ensure that with regard to personal data:

- they process it securely
- it is updated regularly and accurately
- it is limited to what the club needs
- it is used only for the purpose for which it is collected;
- is deleted when the purpose for which it is collected ceases to apply and
- used for marketing purposes ONLY if the individual has given the club consent to do so.

ADDITIONAL SOURCES OF SUPPORT

The **Sports & Recreation Alliance** have been commissioned by **Sport England** to create a toolkit / suite of templates for Clubs to use. These can be found at **https://www.sportandrecreation.org.uk/pages/gdpr**

Data Audit Template

Data Breach Log Template

Privacy Notice Template

SPORT + RECREATION ALLIANCE

SPORT ENGLAND

FREQUENTLY ASKED QUESTIONS

WHAT IF MY CLUB ORGANISES EVENTS?

If your Club organises events that require the capture of personal information you will need to comply with the regulations by seeking explicit consent of all participants. You should be clear what the information will be used for and who will be responsible for managing the data captured.

DO WE NEED TO ADD ANYTHING TO THE EVENT BOOKING FORM?

Yes, as data regarding an individual's results will be passed to other organisations to publish, the individual entering the event needs to be aware of this. Therefore, if you organise an event, to comply with the GDPR, event organisers should include some variant of the following wording on event entry forms:

"You agree that we may publish your Personal Information as part of the results of the Event and may pass such information to any governing body or any affiliated organisation for the purpose of insurance, licences or for publishing results either for the event alone or combined with or compared to other events. Results may include (but not be limited to) name, any club/ home country/regional/county affiliation, results, age category, penalties."

"You also agree that in the event of a disciplinary or welfare incident that you are either involved in or witness, we may pass on your personal information to British Triathlon or any other relevant Authorities for the purposes of supporting any investigatory activity into that incident."

DOES ALL THIS ONLY APPLY TO DATA THAT IS HELD DIGITALLY (E.G. ON A COMPUTER) OR DOES IT COVER PAPER RECORDS?

This is a great opportunity for your Club to review its filing systems and to limit the amount of paperwork you have to manage. Personal data collected manually and stored in files as a hard copy still has to be managed in accordance with the data protection regulations.

As you can imagine, some of the legislation is more difficult to implement in relation to paper copies. For example, privacy of data is key to the GDPR. Paper documents can get into the wrong hands easily and this could easily become a data breach. Transportation of data in any format (including paper) should be seen as a threat to information security. One small slip and it's too late – an individual leaves sensitive paperwork on a train, a courier loses an archive box full of payment records, a member of committee has files stolen from their car. These are all real-world situations where paper documents can get into the wrong hands.

FREQUENTLY ASKED QUESTIONS

MY CLUB KEEPS ITS MEMBERSHIP RECORDS "IN THE CLOUD". WHAT DO WE DO ABOUT THAT DATA?

For example, via shared files on Dropbox or Google Drive, or via a bespoke or commercially available membership system.

Data security is fundamental and when storing anything online you need to ensure that you protect yourself. Taking valid sensible precautions will help you keep your data secure for example, by ensuring you keep passwords safe and ensure that files that contain personal data are encrypted.

Services such as Dropbox, OneDrive and Google Drive have built in security measures for the protection of files whilst in storage or in the process of being shared. When using third party software you need to ask for assurances over the security of the system. You have every right to ask the provider for an explanation of how data security is managed or ask if a Privacy Impact Assessment has been undertaken.

If the service you use ever transfers data outside the EU, make sure the service is still GDPR compliant

WE BELIEVE OUR CLUB IS COMPLIANT, DO WE NEED TO DO ANYTHING ELSE?

You will need to tell people about what you intend to do with their data at the point you collect it and not at some later date.

You also need to seek explicit consent that you can evidence.

All clubs should already have a privacy statement and policy, this outlines to an individual who is providing you with data the details of exactly how it will be used. If someone isn't clear and you do not manage data in accordance with the policy, you are increasing the risk of breaching data protection laws.

FINES - WHAT IS THE REALITY FOR CLUBS? THERE IS NO REAL TURNOVER SO IS IT DIFFERENT FOR CLUBS.

The introduction of the GDPR is new to everyone from multinational plc's, to charities, to sports clubs to a lone window cleaner. We have no history from which to make assumptions or draw conclusions. Guidance to date suggests that any breach would be looked upon more favourably if the organisation or club can show that they are making a start and have a plan.

IT ALL SEEMS SO DAUNTING FOR A SMALL CLUB SUCH AS OURS.

We totally understand this. As detailed above, this affects all businesses, organisations, charities and small sport specific clubs. Anyone who holds/collects data for whatever purpose is affected by this.

The reality is that Clubs do have certain pieces of data they hold. Take a little time out, identify the data and start by tackling it step by step. For example, Club Members will all need to be told why you request the data you do, how it is used, how it is stored and how it will be kept safe etc. Let current members know and for new members – incorporate it into their signing up process.

WHERE CAN I GET MORE INFORMATION ON DATA PROTECTION

The ICO website (**https://ico.org.uk/**) should be your first port of call. In addition, as an affiliated club, you have access to a free club helpline service who are able to provide advice on many aspects of running your club, including data protection. For more information, please go to **https://www.britishtriathlon.org/clubhelpline**.

BRITISH TRIATHLON

TRIATHLON ENGLAND | TRIATHLON SCOTLAND | WELSH TRIATHLON CYMRU | TRIATHLON TRUST

PO Box 25, Loughborough, Leicestershire, LE11 3WX

T +44(0)1509 226161

E info@britishtriathlon.org

BritishTriathlon

@BritTri

/BritishTriathlon