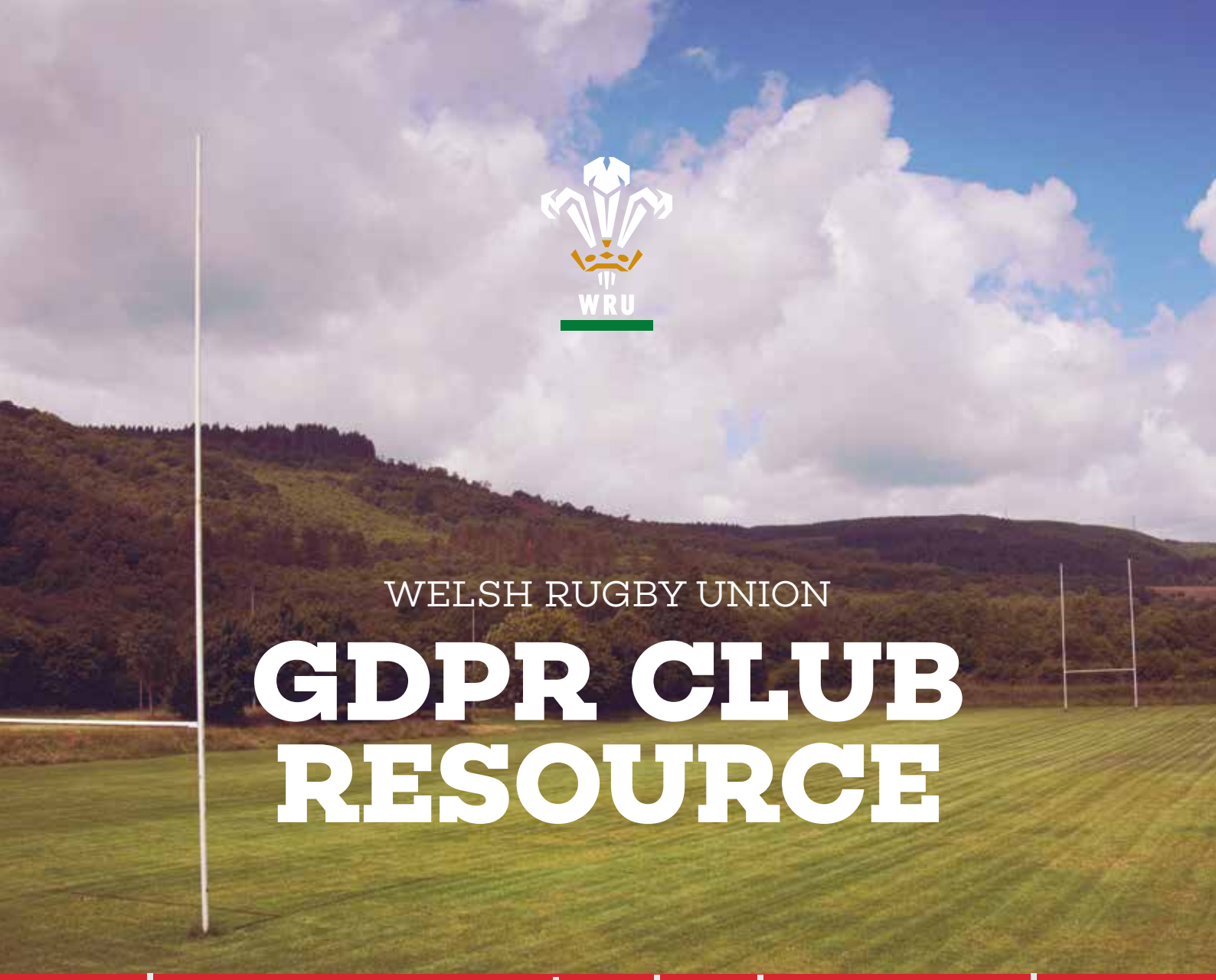
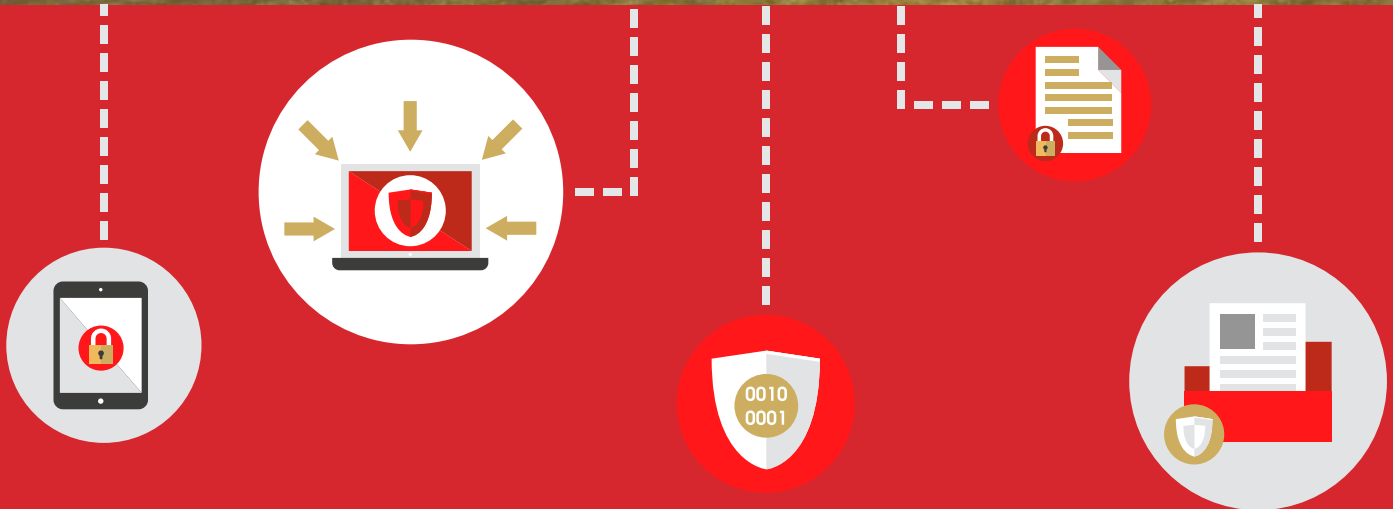


WELSH RUGBY UNION

GDPR CLUB RESOURCE



GENERAL DATA PROTECTION REGULATION

V1 MAY 2018

WELSH RUGBY UNION

GDPR CLUB RESOURCE

GDPR – What is it?

Data protection laws are changing. A new "General Data Protection Regulation" (commonly known as GDPR) will come into force on 25 May 2018, replacing the previous Data Protection Act 1998. This gives individuals more rights in relation to their personal data, whilst increasing the onus on organisations to keep personal data secure and only to use it for the purposes it is intended for.

All organisations will be required to comply with GDPR, including not-for-profit organisations such as rugby clubs, District Associations and the WRU. Whilst this GDPR Resource refers to 'Club' or 'Clubs' in a number of places, such references should be read so as to include any organisation that is involved in the delivery of rugby in Wales.

What is the GDPR Club Resource?

The WRU has devised this GDPR Club Resource in order to assist you as Clubs, District Associations or other organisations involved in the delivery of rugby in Wales in the following ways:

- to understand what the new data protection laws require and how to prepare for GDPR;
- to highlight the changes under GDPR and to provide practical steps to achieve compliance; and
- to demonstrate the next steps to achieving compliance.

This GDPR Club Resource is intended to provide a summary of what needs to be done to achieve compliance with GDPR. However, please note that this GDPR Resource does not and is not meant to constitute tailored legal advice, so if you are unsure about how to proceed then you should seek guidance from your usual legal advisers.

There are links at the end of this GDPR Club Resource to other resources (Including template documents) that you may find useful.

Key Terms used in this GDPR Club Resource:

- Data Subject – the individual whose data is held by an organisation.
- Data Controllers – the owner of the data, a controller determines the purposes and means of processing personal data.
- Data Processors - a processor is responsible for processing personal data on behalf of a controller. Processing simply means doing something with the data – for example, using it to contact someone.
- Personal Data - is any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. This provides for a wide range of personal identifiers to constitute personal data, including name, identification number, email address or telephone number.
- Sensitive Data - GDPR refers to sensitive personal data as "special categories of personal data". The special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual

Why does GDPR impact me and my Club?

You will no doubt hold, manage and use individuals' data for the day to day running of your Club. This would include obtaining and using data about players, club referees, administrators, other volunteers, employees and website users. You will need to ensure that all personal data collected, stored and used by the Club is kept in compliance with GDPR. This includes keeping it secure, lawfully processing the data and the erasure of data upon request.

Everyone within your Club is responsible for ensuring compliance with GDPR. It would be best practice to appoint an individual to have overall responsibility for data protection, but we appreciate that this may not always be possible. Please remember that your Club's Board of Directors or Committee have ultimate responsibility for ensuring compliance with the legislation.

All Clubs are different and what works for one Club, may not work for another. It is therefore important that you review your own processes and take steps, including obtaining independent legal advice, to ensure your compliance with GDPR.

The Information Commissioner's Office (ICO) is responsible for the guidance and enforcement elements of GDPR. They say that Clubs should, in all instances of data collection, ensure that privacy and data protection is at the forefront of their thinking and that this should continue during the period of data retention. The ICO has increased enforcement rights under GDPR.

The ICO has a large amount of guidance available on its website, which can be found here: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/.

We appreciate that there is much coverage of GDPR compliance in the media and that compliance may as if it is an onerous task. We hope that you find this GDPR Club Resource helpful and please remember that compliance is a continuing obligation.

What is new under GDPR?

Under GDPR, Clubs will, when collecting personal data, need to ensure that:

- data is only collected and held where necessary;
- data is kept secure; and
- they are transparent in the way in which they collect, hold and use such data.

When collecting personal data, it is important to ensure that individuals are made fully aware of the reason for collection, what will happen with the data once collected; and how long this data will be kept for. In addition, the personal data collected must be kept securely. For example, Clubs should, as best practice, use electronic means of storing data whilst ensuring this is password protected, backed up on a server and not shared with third parties unless there is a legal basis or legitimate interest in doing so (see further section '*Preparation and Compliance'* of this GDPR Resource).

Personal Data

Personal data can take many forms; however, it is simply any information held on an individual which makes that person identifiable. Such information can be an individual's name, address or even an email address. In addition to this, it could be information such as medical records or criminal records. There are a variety of ways this may be collected and/or stored, including electronically (via My WRU, spreadsheets, registration forms) and physically (e.g. via paper or player registration cards (Green and Red Cards)).

When collecting, storing and/or using personal data, you should consider the implications of GDPR and how this legislation will affect this going forward.

Preparation and Compliance

One key area of GDPR is that it will be up to a Club to demonstrate that it is compliant with the legislation. Consequently, there is a larger emphasis on record keeping. Therefore, it is vital that your Club takes steps to *'prepare'* itself for GDPR and to ensure it can demonstrate '*compliance'.*

1. Understanding and recording all data held by your Club

Your Club will likely hold a differing amount of Personal Data on individuals such as players, coaches, referees and other individuals.

Preparation

Your Club should ideally complete what is known as a 'Data Audit' to understand what data you currently collect and hold. In doing this you will have a greater understanding of the type of data you hold, who you hold data on and how this data is used.

Compliance

To be compliant with GDPR, your Club will need to keep records of:

- the name and contact details of the data controller *(i.e. the Club – in some cases you may be a joint controller with the WRU)*;
- the purposes of why you process data;
- how long you process data for;
- a description of the categories of individuals whose data you hold; and
- a description of how data is shared with, or obtained from, third parties and any international data sharing that goes outside the European Economic Area.

Once you have completed a 'Data Audit', you should maintain these records to demonstrate compliance with GDPR. This will typically be in a register or table format and will contain information on how your Club will use this data and the safeguards that are in place to protect such data.

Guidance on the documentation required from the ICO is available here: https://ico.org.uk/for-organisations/guideto- the-general-data-protection-regulation-gdpr/ accountability-and-governance/documentation/ .

2. Staff, volunteer, member awareness and training

Preparation

The responsibility of complying with GDPR falls to everyone within your Club. It is vital that Clubs ensure all staff, volunteers and members receive adequate training in how to collect, use and keep data in a way which complies with GDPR.

Compliance

Clubs should first look to share this GDPR Club Resource, the information from the ICO and the other resources referred to regarding GDPR within the Club (further information is available from the ICO at https://ico.org.uk/for-organisations/resources-and-support/).

3. Review and amend relevant documentation

Your Club must, when collecting and using data, act in a fair, lawful and transparent way so that the individual is clear on how its data is used and processed and why its data is used. This is a fundamental principle of GDPR. This is usually set out in a **Privacy Notice**, which can be hosted on a website or provided to the individual at the point of collection.

Preparation

Clubs must be clear on why it is collecting and using data and then only use it for those purposes. In collecting and using the data, the Club must act in a lawful way and the documentation, such as Privacy Notices should reflect the reasons for its use.

Compliance

Clubs will need to ensure they collect and use the data in accordance with at least one of the lawful purposes set out in GDPR. These are as follows:

- Legitimate interest

  In order to use an individual's data without consent, an organisation must be able to demonstrate that the use of the individual's data is in its legitimate interest or the legitimate interest of a third party. The Club must balance the rights and interests of the individual against the interest of the Club and/or third party.

  There are a number of processes which will be caught under the principle of 'legitimate interests'. However, to be able to rely on this, your Club will need to explain to individuals within the Privacy Notice that these processes are being carried out. Some of these processes may include (but are not limited to):

  - registration of players not captured by the My WRU Self-Registration process;
  - maintaining lists of players, members, parents of children at a club etc;
  - providing player information to a Club's insurer; and
  - providing an individual's details to the WRU for regulatory or disciplinary purposes.

- Legal obligation

  A Club may process an individual's data if there is a legal obligation to do so. An example of this would be where you are required by order of a court in England and Wales to process personal data for a particular purpose. In these instances, the Club must consider if it is necessary and reasonable to process the data.

- Performance of a contract

  A Club may use an individual's data where it is necessary for the purposes of performing a contract. An example of this would be using someone's contact and payment details in order to pay an employee.

- Consent

  In order to rely on consent, a Club must demonstrate that the consent is explicit, clear and specific. The individual must freely 'opt in' with a positive action (pre-ticked boxes are no longer acceptable under GDPR). In addition, the Club must provide the individual with the opportunity to withdraw consent as easily as it is given.

  Examples where consent may be required include, but is not limited to, the collection of sensitive data from players or other individuals, such as health and medical data, religion, ethnicity, sexual life or orientation, trade union membership or criminal records data.

  Further to this, where your Club wishes to use data for the purpose of e-mail marketing (this will not include genuine newsletter updates from your Club – it must contain advertising/promotion and be solely for the purpose of marketing to individuals), you will need the individual's consent to send such marketing or promotional material either from the Club or from the Club's sponsors. Where you need an individual's consent, it is important that you record that this has been given. Note that only those 13 years old or over can give consent for online services, like marketing – for those under 13, you will need to obtain parental consent.

More detail on direct marketing rules can be found on the ICO website: https://ico.org.uk/media/for-organisations/documents/1555/direct-marketing-guidance.pdf.

Preparation

Your Club may, in certain circumstances, need to conduct a Data Protection Impact Assessment (DPIA). These are generally required where new technologies are used resulting in a high risk to the rights of individuals. This means understanding whether the processing activity will negatively impact and/or breach the rights and freedoms of individuals. For example, the processing of data related to payroll will contain sensitive bank account details, which could potentially lead to financial loss if a data breach occurs. A club should ensure that these systems are safe and secure for the storage of data.

Compliance

Once completed, Clubs should record the results of a DPIA in order to demonstrate that it has been carried out and the risks have been identified.

Further details on when a DPIA must be carried out can be found here: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protectionimpact-assessments/

Further guidance on how to carry out a DPIA can be found here: https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

DPIAs may be required, however, if a Club has or installs CCTV on a large scale. The ICO has also produced a code of practice for CCTV, which can be found here: https://ico.org.uk/media/for-organisations/documents/1542/cctv-codeof-practice.pdf

5. Data maintenance and accurate data

Preparation

All Clubs must ensure that data is accurate and kept up to date. Clubs should ensure that inaccurate data is erased or corrected.

Compliance

Data should be reviewed on a regular basis and inaccurate data 'cleansed' to uphold this principle of GDPR. For example, if a player changes their surname the Club must update its records to ensure this is accurately reflected.

More detail on this principle can be found here: https://ico.org.uk/for-organisations/guide-to-the-general-dataprotection-regulation-gdpr/principles/

6. Data Minimisation

Preparation

All data collected by Clubs under GDPR must be for a specific, lawful purpose and the individual must be made aware of this purpose. The Club must only keep and use this data for as long as this purpose is present. Therefore, if the Club has no purpose for the storing or use of this data, then they must erase the data. This is linked to Data Minimisation and Clubs should, even where they have consent or a legitimate purpose, only collect such data if it is essential.

Compliance

In the first instance, Clubs should consider why they are collecting data and whether this data is essential to its organisation. Sensitive data collected by way of consent (as above) should only be collected when absolutely necessary for that particular purpose. Clubs should consider and weigh up the need for this sensitive data with the individual's rights and explore any ways to limit the risks associated with its collection.

Data should be collected and stored in a way which makes it easy for you as a Club to use according to its purpose – this reduces the possibility of data being used beyond what you have told individuals you will use their data for.
For example, if a player agrees to their data being held for the purposes of team management, you must not automatically use this data for marketing as this is not the purpose for which it was given.

The ICO has further details on this on its website, which can be found here: https://ico.org.uk/fororganisations/guide-to-data-protection/principle-2-purposes/ .

7. Time Periods and Retention Periods

Preparation

Data must only be kept as long as necessary and for a period for which the data is used and required, and for no longer. However, there may be certain circumstances where data may be held indefinitely for historical or record purposes (such as match results and team sheets).

Compliance

When drafting Privacy Notices or at the point of collection of data, make sure that you make individuals aware of the maximum time you will hold their data for. The policy should then be followed in all circumstances and data deleted at the expiry of the retention period. It would be sensible for Clubs to review its data each year and to 'purge' all expired data – this will minimise any risks.

The ICO has produced guidance on the retention of data, which can be found here: https://ico.org.uk/for-organisations/guide-todata-protection/principle-5-retention/

8. Security Controls

Preparation

Clubs should ensure that they have sufficient technological security controls in place to ensure data is sufficiently secure. The introduction of the My WRU Self-Registration System will reduce the risks to Clubs associated with data storage. In addition to this, there may be instances where Clubs store hard copy data. Clubs will also need to ensure there are security controls in place for this type of data.

Compliance

When considering electronically held data, the following security controls should be put in place:

- antivirus software is installed and kept up to date;
- computers have appropriate password protection and are stored securely when not used;
- databases or spreadsheets containing large amounts of personal data are password protected;
- where possible, storing on a central server (or a cloud-based server) with the appropriate security controls in place; and
- all personal data which is stored electronically is backed up, so it may be recovered in the event of destruction or loss of data.

The security of hard copy data may be achieved in the following ways:

- minimise the amount of hard copy data stored;
- back up hard copy data electronically and securely destroy the hard copy;
- do not leave hard copy data 'lying around' homes or offices; and
- place hard copy data in a securely locked draw or cupboard when not in use.

Data Transfer:

- if you send out spreadsheets or lists of individuals' data, consider whether you need to send these all out by email, and to each recipient; and

- where emails are sent out to large distribution lists and there is no need for others to reply to all, ensure recipients are bcc'd rather than cc'd to avoid disclosing others' contact details.

What else can I do?

The UK Government's Cyber Essentials Scheme can provide certain security assurances and help protect personal data in your IT systems. This will assist your Club in demonstrating compliance with GDPR.

There are two levels of Cyber Essentials:

- Cyber Essentials Standard – **Self Assessment.**

Complete an online application with questions that cover the most important areas to ensure you are taking the correct steps to protect the data you hold.

- Cyber Essentials Plus

Once you have achieved Cyber Essentials Standard, the next step to take is Cyber Essentials Plus, this provides independent verification of the level of your data security.

More information about the Cyber Essentials scheme can be found at https://www.cyberessentials.ncsc.gov.uk/.

The ICO has produced a basic guide to technology security here: https://ico.org.uk/media/fororganisations/documents/1575/it_security_practical_guide.pdf . It is aimed primarily at small businesses, but is likely to be a useful starting point.

9. Data Transfer

Third Party Providers

Preparation

If you, as a Club use any third parties to process data, or even hold data for you, then it is important that you ensure they too are GDPR compliant. This could be, for example, where they host a website for your Club which inputs personal data of players. In this case your Club will likely be the 'data controller' and the third party provider will be the 'data processor'.

Compliance

In these instances, Clubs should ensure that they have in place the relevant and appropriate contractual clauses to ensure that the personal data is being held and used in accordance with the GDPR including having appropriate technical and organisational measures to protect against unauthorised or unlawful processing of personal data.

This is an ongoing obligation for Clubs after the introduction of GDPR. Clubs must ensure going forward that these safeguards are always in place for third party providers.

The ICO intends to produce some model clauses that any organisation can use. These have not yet been published, and when they are, they will be available on the ICO's website. It is recommended that you seek your own legal advice when drafting these sorts of Agreements to ensure that your Club is properly protected.

Where you engage a third-party data processor (such as a website host), find out whether they will hold individuals' data outside the European Economic Area. If they do hold individuals' data outside the European Economic Area, then this will be classed as an International Data Transfer and specific legal advice should be sought.

Ongoing Compliance

Reporting data breaches

There is always a possibility that a breach of security may occur and that this breach may compromise data held by you. A data breach will occur where the security of data is breached and this affects the confidentiality, integrity or availability of personal data.

The GDPR introduces a much greater emphasis on reporting data breaches. Where a data breach occurs, Clubs should assess the following before reporting to the ICO:

- what is the potential detriment to individuals of the data breach?;
- what is the volume of data affected?; and
- is the affected data sensitive in nature?

There will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals. There may be a number of ways this can happen, such as a lost laptop, a file sent to the wrong recipient or a hack. It need not be technological; a lost hard copy file will also be a data breach.

What to do…

All Clubs will need to have in place a procedure to manage a data breach. This will need to include a decision whether to inform those individuals whose data may have been disclosed, or (where necessary) to inform the ICO. The key thing to consider is that you should act quickly.

How to do it…

More information is available from the ICO at:

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

https://ico.org.uk/media/for organisations/documents/1536/breachreporting.pdf

Data Subject Access Requests

An individual may request a copy of all data held by you. This is not a new right, but from 25 May 2018 organisations are no longer able to charge a fee for this, and the information must be provided within 30 days. More information also needs to be provided about how that data has been used and shared.

What to do…

This can be an onerous task, but it is an important one. You will need to have a documented process for responding to data subject access requests.

How to do it…

Ensure that there is someone who is responsible for managing this process on behalf of your Club. You will need to find all data held by the Club on that individual. If all of this data is held in one place (for example in a spreadsheet), this will be easier. You may need to go through e-mails, databases and other places where individuals' data is stored. If an individual requests his or her data, we recommend engaging with him or her fully as soon as possible. Often an individual will only want a specific set or piece of information. It may be helpful to find out if this is the case so that only that piece of information need be provided.

Where to find more information…

This is a complex area, as there are certain exemptions to a requirement to provide information; it may not always be possible to provide an individuals' data when it is intertwined with the data of another individual and it is not reasonable to disclose this data. There is extensive guidance on the ICO website, available here: https://ico.org.uk/for-organisations/guide-to-the-general-data-protectionregulation-gdpr/individual-rights/right-of-access/ .

Rectification

All individuals will have the right to have any data which is incorrect or data which is missing rectified by the data controller and/or data processor. Therefore, Clubs will need to ensure that data is kept accurately and in the event of inaccurate data this is rectified as soon as possible upon notice.

Erasure

Under GDPR, individuals now have the right of erasure or as it is known, the 'right to be forgotten'. Therefore, if one of the conditions apply (such as withdrawn consent or data is no longer necessary), then Clubs must erase that data.

The ICO deals with this right in greater detail in guidance available on its website, available here: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/.

Data Restriction

Individuals may decide that they do not want their data used in specific ways. Under GDPR, an individual can ask Clubs to restrict the way that an organisation uses their data. This is an alternative to requesting the erasure of their data.

The ICO has produced detailed guidance on its website, available here: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-restrict-processing/.

The GDPR gives individuals the right to object to the processing of their personal data. This effectively allows individuals to ask Clubs to stop processing their personal data. Importantly, individuals have the absolute right to object to the processing of their personal data if it is for direct marketing purposes.

The right of objection is discussed in more detail by the ICO here: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-object/.

Data Portability

An individual may in certain circumstances (as referred to above) ask to view the data held by Clubs on them. Under GDPR, individuals have a right to data portability and this gives individuals the right to receive personal data they have provided to a controller in a structured, commonly used and machine-readable format.

Given the change in legislation Clubs should now be taking appropriate steps to ensure compliance with GDPR. A failure to comply carries a risk of a fine from the ICO.

Practical Steps to Take

a) Allocate a suitable person(s) to deal with personal data within your Club. Ensure that they read this GDPR Club Resource and guidance on the ICO's website. Consider sending a message to your membership to see if anyone has had to consider GDPR as part of their working life as they may be prepared to help. Make relevant volunteers and staff aware of GDPR and their responsibilities.

b) If you have not done so already, put data protection on the agenda for an upcoming Board or Committee meeting, and ensure that the right people attend.

c) Consider what personal data you hold within your Club and how this data is used (which might be for general administrative, disciplinary or marketing purposes). Cross-check against the reasons why you obtained this data – do you need the data for these purposes? Are these the purposes which you told people about when you collected the data, or are you using the data for additional purposes?

d) Review your privacy notice and any existing policies you have – what (if anything) do you need to add to these?

- Does the privacy notice cover all activities undertaken by your Club? If not, you will need to include the additional activities.
- Will the processes for dealing with data breaches match relevant responsibilities within the Club?

e) Review who in your Club has access to records containing personal data and determine whether it is necessary for everyone who currently has access to retain it. Consider password protecting and/or encrypting documents which contain personal data.

f) Ensure that contracts that require personal data to be transferred to another organisation – which happens where you use a cloud-based software system, for example – are GDPR-compliant

Remember, all Clubs are different and what works for one Club, may not work for another. It is important that all Clubs review their own processes and take steps which they determine are necessary and appropriate for their own circumstances, including obtaining independent legal advice, to ensure compliance with GDPR.

Useful Policy Guidance

The Welsh Sports Association has created a useful online resource for sporting organisations to assist them with their GDPR compliance, including some template documents which can be used to create data protection policies. This can be found at http://wsa.wales/our-services/gdpr/. Please use the username - WRU001 and password - WSAWRU2017 to access these documents.

The Sport and Recreation Alliance has also produced a number of useful GDPR template policies and a number of other helpful resources that Clubs may use to ensure compliance. These can be found at https://www.sportandrecreation.org.uk/pages/gdpr-clubs. Clubs will need to register by providing their email address and name of organisation in order to access the template documents.

Remember that you will need to tailor your documentation as appropriate and applicable to your Club. Not everything in the template documentation may be applicable and therefore will need to be amended.