RLSS UK and the General Data Protection Regulation (GDPR)

Information and Guidance for Clubs

Dear RLSS UK affiliated Clubs,

The Data Protection Act 1998 is due to be repealed in the UK and will use the EU's General Data Protection Regulation (GDPR) as its basis for law. This will place certain obligations on any organisations, clubs, societies who process individual's personal data. It regulates how personal information should be used and protects people from the misuse of their personal details.

May 25th 2018 sees the new Data Protection regulations come into effect and RLSS UK has engaged a Data Protection Consultant to help ensure that we are on the road to compliance.

Data protection applies to every organisation from large multi-nationals, charities and clubs. In the smooth running of a Club it is essential that data is used and kept securely to ensure safe and effective practice; this could include names, addresses, dates of birth and financial details. The storage of this data can be a complicated matter and may take many forms. It is often stored on a personal computer in the homes of the very volunteers who give tirelessly to train essential lifesaving skills. If this data went missing, perhaps through criminality or personal error, this would result in a 'data breach' which has serious implications not just for the Club but for the whole charity and could result in serious fines.

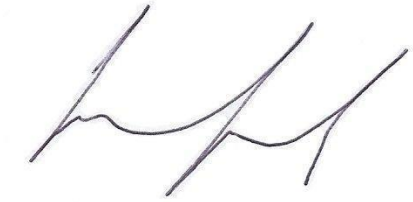
All RLSS UK affiliated clubs will need to comply with the regulations. GDPR will apply to you whether you are paid staff or are volunteers, whether you have 10 members or 1000 members - there are no exemptions.

To help guide you through the GDPR regulations RLSS UK has put together this guidance and templates will be available online to help you and your Club be Data Protection compliant.

The team at RLSS UK are ready and willing to support you through this process.

I would like to thank you for your support and compliance in this matter, which is required by law.

Yours Sincerely,



Lee Heard

Head of Volunteering

Table of Contents

Using this Guide

This guide is set into two flowing sections. The initial section is taken directly from the Information Commissions Office (ICO). It is extremely important that you read and familiarise yourself with this information as it provides the context for GDPR. Secondly, we have provided more practical guidance for Clubs. This section will be extremely useful for you to help to action different requirements of GDPR.

RLSS UK will also provide a series of useful templates in supporting with any changes to be GDPR compliant and these can be found online.

Introduction to GDPR

General Data Protection Regulations (GDPR) demands more of organisations who hold data to act in a way that protects the individual. GDPR gives the individual more control over their personal data and strengthens the requirements for children's data; the approach is not much different to the data protection laws we are currently guided by. Rather than an afterthought, data security and privacy needs to be at the forefront of everything we do.

GDPR requires some common sense and asking a few questions before forging ahead in the collection and storing of personal data. Included below are some of the general 'terms' used within Data Protection.

What is Data Protection?

In basic terms, Data Protection's main purpose is to ensure that personal data is 'reasonably safeguarded' against unintended use, distribution or loss. It regulates, amongst other things, how individuals and organisations may obtain, use, store and erase personal data.

What is considered personal data?

As per the new GDPR regulations, personal data is any information relating to an identified or identifiable individual; meaning, information that could be used, on its own or in conjunction with other data, to identify an individual. It is any information relating to an individual, whether it relates to her or his private, professional or public life. It can be anything from a name, a home address, a photo, an email address, bank details, posts on social networking websites, medical information, or a computers IP address.

What is considered 'Sensitive' Personal Data?

Sensitive Personal Data means personal data consisting of information as to:

a) The racial or ethnic origin of the data subject
b) Their political opinions
c) Their religious beliefs or other beliefs of a similar nature
d) Whether they are a member of a trade union
e) Their physical or mental health or condition
f) Their sexual life
g) Any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings

What is considered 'Processing'?

Processing, in relation to information or data, means obtaining, recording or holding the information or data. This also could be the carrying out of any operation or set of operations on the information or data including:

a) Organisation, adaption or alteration of the information or data
b) Retrieval, consultation or use of the information or data
c) Disclosure of the information or data by transmission, dissemination or otherwise making available, or
d) Alignment, combination, blocking, erasure or destruction of the information or data

What is a 'data subject'?

An individual who is the subject of personal data. In other words, the data subject is the individual whom personal data is about.

What are the eight basic principles for Data Protection?

There are eight basic principles for Data Protection which ensure that personal data is reasonably safeguarded against unintended use, distribution and loss.

1. Lawfulness, fairness and transparency	Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject
2. Purpose limitation	Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
3. Data minimisation	Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
4. Accuracy	Personal data shall be accurate and, where necessary, kept up to date
5. Storage limitation	Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed
6. Integrity and confidentiality	Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

7. Accountability	The controller shall be responsible for, and be able to demonstrate compliance with the GDPR
8. International	Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

What does all this mean for RLSS UK Clubs?

Principle 1

In order for you to process data 'fairly', you should:

- Ensure that you have a legitimate reason to obtain or process the data – this could be simply that they are a member of your Club
- The Data Subject must be made aware that their data is being used and their consent obtained. They must never be deceived or misled - they must have a clear understanding of the reasons for which it is proposed that their data be used. This can be clarified in a Club Membership Form informing the member that their data will be used in the management of the Club
- If any sensitive personal data is involved Data Subjects must have provided their express consent to the processing – again this could be consent given on the Membership Form
- Care needs to be taken to ensure that personal data is only ever obtained from a person who is legally authorised to supply it i.e. Parent/Guardian/Individual

Principle 2

The main issues raised by this principle are:

- All personal data processed by RLSS UK Clubs must be covered by a Data Protection Policy. A template of a Data Protection Policy can be found online for you to adapt should you need one. **Adopt this into your working practices at the Club just like the Safeguarding Policy!**
- Ensure that data held for one purpose is only ever used for that purpose. For example; if you use a set of data to enter someone for an event or competition this data should only be used for that purpose and should not be used to create a Club Directory
- Personal data should never be disclosed to any third party (other than those covered in your Privacy Policy – this is discussed later in this document)

Principle 3

To ensure compliance:

- You should not collect any personal data that is deemed unnecessary. You should have an adequate reason for the collection of every piece of data you collect; i.e. it is perfectly acceptable to obtain date of birth as the age of candidates reflects which awards and qualifications they

would be able to take, but you would not be able to collect data on any previous addresses as this would be deemed unnecessary

- Proper care should be taken to consider the necessity of obtaining or holding any sensitive personal data

Principle 4

Personal data must not be inaccurate or misleading. This applies to any information from a third party. Where the information was obtained from should always be included on records. This principle may not apply to many clubs.

Principle 5

Data should only be held for the period set out in the Clubs Data Retention Policy and should be destroyed as set out in the Clubs Policies and Procedures. Failure to remove data that is no longer relevant is a breach of Data Protection Regulations.

Principle 6

RLSS UK Clubs must ensure that all personal data is processed in accordance with the rights of Data Subjects, who can:

- Make Data Subject access requests to find out what information you hold about them, the purposes for which it will be used and to whom it has been disclosed. For example; a member of your Club may ask you to release all of the information that you hold about them, what you have done with that data and who you have sent the data to, such as using the data to complete paperwork for an assessment form and then sending it to RLSS UK to be processed
- Prevent data processing for the purposes of direct marketing or the processing of data which is likely to cause them substantial damage or distress
- Ask, if appropriate, to have the data corrected or deleted
- Be informed about automated decision-making processes that affect them and prevent significant decisions that affect them from being made solely on automated processes

As an RLSS UK Club you will also need to have a procedure in place to be able to respond to these rights of Data Subject. A template procedure can be found online but will need to be altered to your Club specifics.

Principle 7

Access to personal data will only be granted to RLSS UK Club Volunteers insofar as is necessary for legitimate operational purposes. The personal or private use of personal data held by the Club is strictly forbidden.

All volunteers with access to personal data must be mindful that they play a role in ensuring that it is always kept securely. They must familiarise themselves with RLSS UK Data Protection Policy and ensure that they adhere to it at all times.

Principle 8

Personal data must not be transferred to a country outside European Economic Area unless:

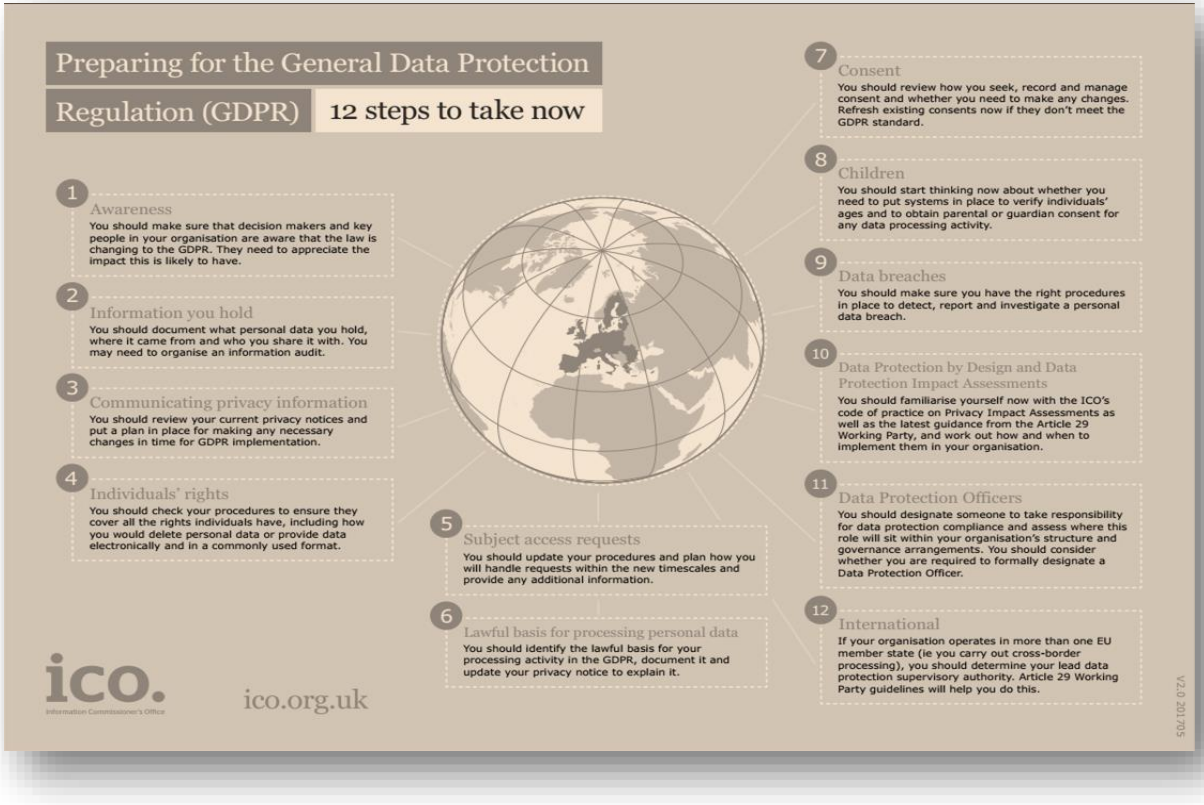
- Explicit consent has been obtained from the Data Subject(s)
- The data has been completely anonymised
- That country ensures an adequate level of protection for Data Subjects
- A contract is in place with the recipient of the personal data, which puts the necessary safeguards in place. This will usually be put in place by RLSS UK as the governing body

For those Clubs that have connections with Worlds and Commonwealth Events the data sharing arrangements and contracts will usually be arranged by RLSS UK.

Special care should be taken when travelling with a laptop or other mobile device which contains personal data and should always as a minimum be password protected.

Where do RLSS UK Clubs start ensuring that they are GDPR compliant?

The Information Commissioner's Office has introduced a 12 step guide to prepare for all the new Data Protection regulations. This may appear daunting at first, but is a very good starting point to consider what needs to be reviewed, changed and new working practices that need to be adopted.



12 Steps to take in Preparation for GDPR:

1. *Awareness*

Key individuals within your Club should be made aware that the law is changing to the GDPR. They should understand that any data breaches could have a detrimental effect on your Club and the whole charity. You could start by creating a risk register. Implementation of GDPR could have significant resource implications. You will most likely find compliance extremely difficult if you leave preparations until the last minute.

2. *Information you hold*

Any personal data that you hold should state where it came from and who you share it with. You may find an information audit to be useful. You will need to maintain records of your processing activities under the GDPR. For example, any inaccurate data that has been shared with another organisation will have to be updated everywhere that it is held. So you will have to tell the organisation that you shared the data with about the inaccuracy, so that it can correct its records. You won't be able to do this unless you're fully aware of what personal data you hold, where it came from and who you share it with.

3. *Communicating privacy information*

Your current privacy notices should be reviewed and a plan should be put in place for making any necessary changes. When you collect personal data under current legislation, you must inform people of certain information such as your identity and the intended use of their data. This is usually done through a privacy notice. Under the GDPR there are additional things to tell people. For example, you will need to explain your lawful basis for processing the data, your retention periods and that individuals can complain to the ICO if they think there is a problem with the way you're handling their data. A copy of RLSS UK's Privacy Policy can be found on the website at www.rlss.org.uk

4. *Individuals' rights*

You should review your procedures to make sure they cover individuals' rights.

The GDPR includes the right:

- To be informed of access
- To rectification
- To erasure
- To restrict processing
- To data portability
- To object
- Not to be subjected to automated decision-making including profiling

These rights are the same as those under the Data Protection Act but with some significant enhancements. Now is a great time to check your procedures and work out how you would react if someone made a request about their personal data.

5. *Subject access requests*

Your procedures should be updated and you should plan how you will handle requests in line with the new rules:

- You will usually not be able to charge for complying with a request
- You can refuse or charge for manifestly unfounded or excessive requests
- You will have one month to comply rather than the current 40 days
- If you refuse a request, you must be able to tell the individual why and inform them that they have the right to complain to the supervisory authority. This must be done within one month

6. *Lawful basis for processing personal data*

The lawful basis for the processing activity should be identified, documented and your privacy policy must be updated to explain it.

Under current law, not having a lawful basis for processing personal data does not have many practical implications; this will change with the GDPR as individual's rights will be modified depending on your lawful basis for processing their data.

Your lawful basis for processing must be explained in your privacy notice and when you answer a subject access request. For Example, if someone becomes a member of your Club then they enter into a contract with that Club and this then becomes the lawful basis for processing their personal data.

7. *Consent*

You should review your process for seeking, recording and managing consent and make any necessary changes.

You should refresh existing consents if they don't meet the GDPR standards. The ICO has published detailed guidance on consent under GDPR, you should read this and use their consent checklist to review your current practices.

Consent must be given freely, it must be specific, unambiguous and informed. There must be a positive opt-in – consent cannot be inferred from silence, pre-ticked boxes or inactivity and you will need a simple way for people to withdraw consent.

8. *Children*

You will need to consider putting systems in place to verify individuals' ages and to obtain parental or guardian consent for any data processing activity.

GDPR will bring special protection for children's personal data, particularly in the context of commercial internet services like social networking. If your Club offers online services such as a website that children need to log into to access or complete event entry forms, then you may need a parent/guardian's consent to process their personal data lawfully.

The GDPR states a child can give their own consent to this processing at the age of 13. Consent will need to be obtained from a person holding 'parental responsibility' in the case where a child is younger than this age. It may be an idea that if a child (under 13) wishes to join your Club that you have a section on your application form for a parent/guardian signature.

9. Data breaches

You should check that you have the right procedures in place to detect, report and investigate a data breach.

The GDPR introduces a duty on all organisations to report certain types of data breaches to the ICO and in some cases, to individuals. You only need to notify the ICO (and individuals involved) of a breach where it may result in a risk to the freedom of individuals, for example if it may result in: • Discrimination

- Damage to reputation
- Financial loss
- Loss of confidentiality
- Other significant economic or social disadvantages

Procedures should be put in place to detect, report and investigate a personal data breach. You may like to assess the types of personal data you hold and document where you would need to notify the ICO and affected individuals if a breach occurred.

10. Data Protection by Design and Data Protection Impact Assessments

GDPR makes 'privacy by design' an express legal requirement, along with making 'Data Protection Impact Assessments' (DPIAs) mandatory in certain circumstances. Privacy by Designs holds that organisations need to consider privacy at the initial design stages and throughout the complete development process of new products, processes or services that involve processing personal data.

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

- When a new technology is deployed
- When a profiling operation is likely to significantly affect individuals (this is unlikely to affect Clubs as it is about analysing data and making predictions about individuals)
- When there is processing on a large scale of the special categories of data, (this is unlikely to affect Clubs as it is unlikely that Clubs are processing special categories of data to the extent needed to make it large scale)

If data processing is flagged as high risk by the DPIA and you cannot sufficiently address those risks, you are required to consult the ICO to seek opinion on whether the processing operation complies with the GDPR. This is highly unlikely in the cases of RLSS UK Clubs.

11. Data Protection Officers (DPO)

Whilst it is not mandatory for Clubs to appoint a Data Protection Officer it would be prudent for someone at the Club to take ownership of the role – this may form part of the Secretary's role. Getting ready for GDPR is likely to take some time and will require considered thought to develop suitable processes and policies and, thereafter, ongoing management. Appointing someone or a team of volunteers within your Club to take ownership of the process is likely to be necessary.

12. International

This shouldn't apply to most RLSS UK Clubs as data is usually not shared with others outside of the EEA.

If Clubs do share data outside of the EEA due to the Worlds or Commonwealth Events then this will usually have been covered by RLSS UK. If you require further guidance on sharing data outside of the EEA then the RLSS UK Data Protection Officer will be able to help.

	Suggested things for you to do within your Club	Further Assistance available
Information Governance		
Formalise who within your Club might wish to oversee data.	Whilst it will not be mandatory for Clubs to appoint a Data Protection Officer it would be prudent for someone at the club to take ownership of the role. This does not necessarily have to be a Data Protection Officer, but someone (or a group of people) who can have overall responsibility for data obtained by the Club. **Appoint someone or a team of volunteers within your Club to take ownership of the processes is likely to be necessary.**	**Data Protection Policy and Procedures** RLSS UK will provide templates for essential Policies and Procedures as guidance for all Clubs.
Policies and Data Protection	GDPR is a more extensive piece of legislation than the existing Data Protection Act. **You should establish whether your current policies and procedures are suitable to comply with the GDPR. If not, you should re-write your policies so that they do comply.** This will be the beginning of your Clubs Data Protection Framework. Over the next couple of months RLSS UK will be developing and updating their own policies and procedures.	**Data Protection Policy and Procedures** RLSS UK will provide templates for essential Policies and Procedures as guidance for all Clubs.
Information Assets	Clubs should maintain a record of all information assets. This could be in the form of an Excel spreadsheet and should contain any information that if it was lost or stolen, destroyed, etc., would have a detrimental effect to the Club i.e. a membership list for the Club. **You should review all of the Club's information assets and produce a register of these assets.**	A sample of RLSS UK's Information Asset Register can be found online on the Club page.
Data Collection and Handling		
Data we are concerned about includes 'personal data' and 'sensitive personal data', the processing of this data and ensuring that it is collected lawfully and for legitimate purposes.		

Familiarise yourself with the data you collect and how it flows in and out of your Club	**Create a simple table that shows the data you collect, the reason you collect it, and who the data flows to**.	

	Types of Data	**Reasons for collecting data**	**Who the data flows to**	
	○ Name, address, date of birth, email address, phone numbers and other contact details of Club members ○ Type of membership ○ Date of joining the Club ○ Name, address, email address, phone numbers and other contact details of trainers, instructors, assessors used for awards and qualifications ○ Names, address, email address, phone numbers, date of birth etc. of participants in events/championships ○ Results from events/championships ○ Health information of members ○ Bank/Financial information	○ To become a member of the Club ○ To train/assess a candidate for an award	○ RLSS UK to process the awards/qualifications ○ Other clubs to enter events/championships ○ RLSS UK Branches ○ Club Management/Instructors	
	*These lists are not exhaustive.			

Collecting Data	When you collect data, you must provide the data subject with certain information: ○ Your Club identity and contact details ○ How you intend to use their data ○ Your lawful basis for processing their data ○ Details of anyone who may receive their data ○ Your data retention policy ○ The individual's right to complain to the ICO if they believe there is a problem with your handling of their data	**Privacy Policy** RLSS UK will provide templates for essential Policies and Procedures as guidance for all Clubs.

	All of this information could be included on your Membership Form. **This should also be held within your Privacy Policy.**	
Membership Forms and other Data Collection Forms	You should only collect the information that you need and be clear on the application/data collection forms what you will use the information for. **Ensure that all the forms used by your Club have consistent field names. Conduct a review of all forms used within the Club environment.** For example, one form may use the term 'surname' whist another uses the term 'last name'. This could be confusing for users and volunteers.	RLSS UK are also looking at the assessment report forms to adopt the use of standardised terminology across all of the awards and qualifications.
Forms Containing Financial Information	**If your application form asks the applicant to provide bank details (e.g. for direct debit purposes) separate the financial information from the rest of the application.** **Store financial information separately from the application form.** Make sure that you keep all membership information up to date. When you renew memberships ask members to check their information and provide an easy method for them to give you up to date information. You could do this as part of an annual update. Destroy all financial data in line with your Data Retention Policy and Procedure.	**Data Retention and Disposal Policy and Procedure.** RLSS UK will provide templates for essential Policies and Procedures as guidance for all Clubs.

CCTV	**This will only affect those Clubs that have their own premises as CCTV at a pool will be the responsibility of the operator.** The images of individuals obtained through CCTV are personal data and therefore subject to the GDPR. The general principle is that you must be clear about the purposes for which you are using CCTV and can then only use the images for that purpose i.e. crime prevention at the beach hut. Further guidance from the ICO on the use of CCTV can be found at: https://ico.org.uk/for-organisations/guide-to-data-protection/cctv/	

Disposal of Forms with Personal Data	Any forms such as registration forms, course registers, session forms, candidate assessment forms, membership forms, etc. need to be stored securely. Ideally this information once dealt with and no longer needed should be destroyed using a document destruction service or home shredder. **Never place data to be destroyed with the rest of the household recycling.** **Review the forms currently held at your Club and using the Data Retention Policy set out by your Club securely destroy any data that you should no longer have in your possession.** **It may be an idea to introduce a retention policy for candidate assessment forms and course registers where by once the certificate has been received by the candidate the assessment paperwork is securely destroyed. It is good practice to delete any help forms which have already been processed**	**Data Retention and Disposal Policy and Procedure.** RLSS UK will provide templates for essential Policies and Procedures as guidance for all Clubs.

Data Retention and Disposal	All data should have a retention period and only held for as long as required by legislation/regulation or to carry out the task that the data was originally collected. Your Club Data Retention and Disposal Policy and Procedure should take into account the purposes for which the data is kept, for how long the data needs to be kept (and why) and how the data will be destroyed. **You should not be tempted to keep all data indefinitely "just in case".** General correspondence between your Club and a member may only need to be kept for a short period. Correspondence relating to a potential claim or disciplinary matter may need to be kept for a number of years. Personal and sensitive personal data must be kept securely. You should consider the risks and decide on your levels of security accordingly. You must take appropriate measures to prevent unauthorised or unlawful processing of the data and against accidental loss or destruction of, or damage to, the data. **Review or produce a Data Retention and Disposal Policy and Procedure and ensure that all the data currently held within your Club environment is in line with the policy.**	**Data Retention and Disposal Policy and Procedure.** RLSS UK will provide templates for essential Policies and Procedures as guidance for all Clubs.
Previous Volunteers and Members of your Club	You should store separately the information you hold about former volunteers/members from the information you hold about current members (whether paper or electronically). **Consider the purposes for which you need to retain information about former members and record the reasons and the time period. This should be set out in your Data Retention and Disposal Policy**. **You should securely destroy all financial information you may have about former volunteers/members.**	**Data Retention and Disposal Policy and Procedure.** RLSS UK will provide templates for

	In line with your Data Retention and Disposal Policy you should destroy all information about former members and volunteers once required.	essential Policies and Procedures as guidance for all Clubs.

Entries for Events and Competitions	Only collect the information that you need and be clear on the application form (whether paper or online) what you will use the information for. Store application forms securely. Consider: • Who needs to see them • How long they need to be kept • The data retention of the application form once the event has been completed If the application form asks the applicant to provide bank details for payment purposes, separate the financial information from the rest of the application. **Store financial information separately from the application form.** If data regarding results will be passed to other organisations to record or be published online (via social media etc.), the individual entering the event needs to be aware of this. Therefore, if you organise an event, to comply with Data Protection, race organisers should include the following wording on entry forms: *"You agree that we may publish your Personal Information as part of the results of the Event/ Competition and may pass such information to the governing body or any affiliated organisation for the purpose of award verification, membership 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 affiliation, race times and age category."*	
Data Sharing and Use of data Processors		
Central Register of all Areas you Share Data Outside of your Club	This is an important area that needs to be controlled. **Create a simple Excel spreadsheet showing details of any organisations, and the data being shared. This should be regularly maintained. This maybe with:** • **RLSS UK** • **Swimming Pool operator** • **Local sports partnership**	**Data Sharing Agreement Template** RLSS UK will provide templates for essential GDPR compliance.

	It is a legal requirement to have a written agreement with written instructions outlining the agreements in place regarding the data being shared. These templates can be accessed from RLSS UK.	

Club Directory/Telephone Lists/Numbers Stored on Mobile Phones	Consider the purpose of your Club Directory. It must only contain the information necessary to fulfil those purposes. It is unlikely that there is a need to include member's home address in the directory. You can only include member's details in your Club Directory if they agree that you can do so. Your application form must contain a box for them to tick to show they have agreed. You cannot use an opt-out box. The form must therefore make clear the information to be included in the Club Directory. They must be able to change their mind at any time and no longer be included in the Club Directory. If your Club Directory is a hard copy (paper format) then this should be updated annually. In this case it should be made clear when you seek consent for a member's details to be included, that their details will be included for the whole year. If your Club Directory is online then updates should be made regularly. If you hold numbers on a mobile phone then these should be updated as necessary. You cannot make membership of the Club conditional on a member agreeing to have their name in the Club Directory. **Ensure that you have the consent of the members listed in your Club Directory, telephone list or numbers stored in a mobile phone. Ensure that these are kept up to date and maintained regularly. Ensure that numbers are erased from all sources if a member leaves the Club (this includes the erasing of numbers from mobile phones).**	
Request for Information	All requests for information should be handled with speed and efficiency. In order to do this, you should have a well organised system in place to minimise the amount of time and effort it take to facilitate a request. **Create a log to record all requests that can be managed by the appropriate members of the Club. Appoint one person who would have the overall responsibility to manage and coordinate these requests – this maybe the Club Secretary.**	

Data Transfers	The basic rule is that you cannot pass any data you have about individuals to anyone else (e.g. other Clubs) without the agreement of the individual unless this is specifically noted in your Privacy Policy. For example, you can send data of your Club members to RLSS UK as this will be noted in your Privacy Policy. If you are asked to provide data about a member to anyone other than that member, then you should seek advice from RLSS UK. If you are transferring data via email, then these need to be encrypted or password protected to minimise the potential for accidental loss of theft. If you use a third party transfer site e.g. DropBox, Google Drive, Wetransfer, One Drive, etc., ensure that the data resides within the EU and all data should be password protected. **RLSS UK suggest the services such as Apple's iCloud, Box.com/en and Microsoft OneDrive as they can all provide such a service and are held within the EU.** If anyone in your Club is processing data outside the EU then additional safeguards may need to be put into place. For example, if your Club Secretary spends the winter in the Caribbean and has the organisations data on their laptop, then this would need to be reviewed to ensure that appropriate safeguards are taken.	**Privacy Policy Template** RLSS UK will provide templates for essential Policies and Procedures as guidance for all Clubs.
Information Security Controls		
Saving and Storing your Club's Data	**Does your Club use a central area for documents, or does everyone have copies of data held on personal laptops?** **Review how your Club saves and stores personal data.** You may as a Club elect to invest in Cloud storage so that everything is stored centrally and therefore people do not need to have a local copy. **Ensure that whatever platform you select for your Club that their Cloud servers are located within the EU Services such as Apple's iCloud, Box.com/en and Microsoft OneDrive can all provide such a service.** Be wary of using services such as DropBox, they often do not store data on servers in the EU. You must take particular care of financial information as there is a serious risk to the owners of that information.	**Data Sharing Agreement Template** RLSS UK will provide templates for essential GDPR compliance.

	Your security obligations must be taken seriously whether you hold data in hard copy of electronically.	

	Ensure that data in hard copy form is kept in a locked cabinet to which access is restricted. If the data is kept at a Club members home it should still be in a locked cabinet to which access is restricted. **Whether your data is stored in hard copy or electronically you should consider who should be able to access which data e.g. the Treasurer may be the only officer who needs access to financial information. If so, the financial information should be stored in such a way that only the Treasurer can get access to it plus perhaps one person in the event of an emergency if the Treasurer is ill or away.** Data held electronically needs to be encrypted. If you have arrangements with suppliers who process personal data on your behalf (e.g. the printer of your Club Directory) the GDPR requires you to have a written agreement with them containing certain provisions. **Ask all your Club volunteers to password protect their computers, tablets or phones so that files or data cannot be easily accessed. These should use biometric, key code access or passwords.** **Ask your Club volunteers that when they move to a new laptop, tablet or phone that they securely wipe the device so that no data can be retrieved.** **Ask your volunteers to limit the use of pen/USB drives as these can be easily lost, stolen or forgotten about. Treat the data on these as you would your other electronic devices.** Under Windows 10 they can now be encrypted, so that if they are lost or stolen they cannot be read. http://www.intowindows.com/how-to-password-protect-usb-drives-in-windows-10/ You can also purchase encrypted USB drives, but we acknowledge there is an additional cost to this.	
Security Events, Incidents & Breach Management		
Does your Club have any procedures outlining what needs to happen in the event of a data breach?	It can be difficult to determine if a breach has occurred. A data breach is a violation of security which leads to the destruction, loss, alteration, unauthorised release of personal information, or access to personal data. A breach is therefore more than just losing personal data. **Should a breach become evident, you should contact RLSS UK who will to assist you to minimise any problems and to help you deal with the incident.**	**Data Breach Policy and Procedures** RLSS UK will provide templates for essential GDPR compliance.

	If the breach is likely to result in a risk to the rights and freedoms of anyone, you have to notify the ICO. This has to be considered in a case by case basis. You need to consider the potential detrimental effect on the individual (for example discrimination, damage to reputation, financial loss, loss of confidentiality). If the breach is likely to result in high risk to the rights and freedoms of anyone then you have to notify the individuals concerned.	
Retention and Destruction/Disposal		
What are appropriate retention periods for records?	RLSS UK will be producing guidance on the appropriate data retention timelines and publish these to assist our Clubs, Branches and ATC's to develop the relevant local policies. **You should speak with your Club's volunteers and see what data they currently hold and ask that they delete any records that are no longer required. Holding data for longer than is necessary is no longer allowed under the new rules. This includes paper and electronic records.**	
Upholding Data Subjects Rights		
Right of Access	Individuals have a right to access their own data held at a Club and when this requested it comes in the form of a Subject Access Request (SAR). **You should ensure that your Club has an adequate policy and procedure on how these should be handled.** There is no cost to the individual for requesting this data and Clubs have 30 days in which to respond. Therefore, it is important that you have a process in place and that it is followed so that you ensure you meet the regulatory deadlines. RLSS UK will be able to provide a template for this policy and procedure.	**Data Subject Access Request Policy and Procedures** RLSS UK will provide templates for essential GDPR compliance.

An individual has submitted a Subject Access Request (SAR). What does this mean and what do we need to do?	Using the SAR procedure, you will need to pull together all data that includes the individual's name in any paper based or electronic documents and log these into the SAR document register. You are only required to supply documentation where the individual is the central focus of the document or email. For example, if the person is named on a team list, then they are not the central focus and therefore you do not need to supply documentation. **Ensure that you create an adequate policy and procedure and follow the procedure at all times. Make sure that the person(s) responsible in your Club signs off the documents that are to be supplied and sends them off to the requestor by the deadline.** Collating all of the information can be time consuming but if you follow the process, document your decisions and meet the deadlines the SAR process is relatively simple to follow.	**Data Subject Access Request Policy and Procedures** RLSS UK will provide templates for essential GDPR compliance.
Disciplinary action and Club Members		
Disciplinary Action Against a Club Member	If you need to take disciplinary proceedings against a club member: • Opinions about a member are personal data and so the member could require to see that data through a Subject Access Request • The member is entitled to make a Subject Access Request and ask for the data you hold about their disciplinary case and any other data you hold about them • Data about the member's disciplinary are data relating to the member and therefore other members do not have the right to see the data If others object to a member's disciplinary you cannot disclose the data to them – they must obtain it from the member (if the member is willing to provide it).	
Children's Data		

Privacy Policy	If your Club offers awards and qualifications to children, you must ensure that your privacy notices (including your privacy policy) is written in a clear, plain way that a child will understand. **On any forms where you collect data from children, you will need to ensure that a child understands why you are collecting that data, how it will be used and who will use the data.**	**Privacy Policy Template** RLSS UK will provide templates for essential GDPR compliance.
Online Services to Children e.g. Online Processing	If you offer online service to children, you may need to obtain consent from a parent or guardian to process the child's data. If consent is your basis for processing the child's personal data (this is not the case for candidate assessment forms as they are entering into a contract when completing an award of qualification), a child under the age of 13 cannot give that consent themselves and instead consent is required from a person holding 'parental responsibility'.	

In Conclusion

The message for RLSS UK Clubs is that Data Protection will become more demanding and require new ways of working to ensure that you are compliant with the new legislation. We recognise that this will undoubtedly put more pressure on the very volunteers that help to run our Clubs and deliver our awards and qualifications. Clubs should begin as soon as possible to look at their processed, technologies and the way they are working to determine how these can be improved and to minimise any data protection issues.

RLSS UK is working their way through this process and will be able to provide guidance and templates that can be used to help with your compliance. This is an area that is continually evolving and requires a constant review of the changing landscape.

The ICO is busily interpreting the EU GDPR and making it ready for the UK. The Data Protection Bill is currently going through Parliament and once this has been passed, more clarity will become available.

Where can you start?

No doubt the task of becoming GDPR compliant can appear daunting. We appreciate that and want to help by providing a few first steps. If these are done then you will have invested some good time as a starting point.

Top 5 areas you can start with:

1. Understand where your data is stored, who holds what and on what system?
2. How is your data safeguarded against theft, accidental loss? Recommend some of the best practices listed in the above Information Security Controls section
3. How are you destroying data when your volunteers discard physical lists, registration forms, and how do you manage the return or destroying of data when volunteers move on?
4. How are you managing data related to children?
5. Review your policies and procedures and ensure that they are in line with GDPR requirements

This is only the beginning of the journey, but if you invest now it will pay dividends down the road as we improve on the ways we work to provide a first class experience.