**General Data Protection Regulations – Hollowell SC Response**

From May 2018 General Data Protection Regulations come into effect. All organisations, irrespective of their status who process personal data are obliged to comply with GDPR. The penalties for not doing are severe and for Hollowell this would amount to a fine of between £2,500 and £3,000. To prepare for GDPR, as the processors of personal data, Hollowell SC will need to ensure that it has the policies and processes in place to comply with the regulations.

In particular we will need to:

1. Agree what personal data is required to run the club.
2. How we will use personal data.
3. Whether or not we will need consent for using the data.
4. Produce a Data Policy (currently we don’t have one).
5. Be ready to make changes to Web Collect for the collection of data and reference to the regulations.
6. Identify and record all ‘lists’ of qualifying records.
7. List of known ‘lists of data’.

**Possible Impact on Hollowell**

To help understand the impact on Hollowell I have made notes against the following headings. The complete RYA guidance is included and I would urge all General Committee Members to study the guidance as you are likely to be part of the data processing group and as such will have an obligation under the regulations.

1. Definitions:
	1. Personal Information
	2. Member
2. Need for (or not) member consent.
3. Data Controller
4. Data Processor
5. Retention of data
6. General Issues for Hollowell

I have then added a series of proposals for discussion at the next General Committee meeting (which I will be unable to attend due to holiday).

The key outcome of these proposals is to provide Nicola and Ruth with instructions on what, if any, changes are needed to be made to web collect in time for the annual subscription renewal. The important changes will be:

1. Changes to the declaration depending on the route that the GC recommend.
2. Making the grounds upon which we process data available to all members.
3. Amending the data collected at the renewal stage. This might necessitate a complete start from scratch.

--------------------------------------------------------------------------------------------

1. **Definitions:**

Personal Data. GDPR considers personal data as: *any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified directly or indirectly in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.*

Member. For the purposes of GDPR , a member will be any person who registers their personal data with Hollowell SC using any means of capture that is employed by Hollowell SC in the course of its business. This can include but is not limited to:

 Membership subscriptions via WebCollect.

 Event bookings such as training.

 Visitors to the club via booking-in sheet

 Open day booking-in

 Duty man database.

 Training group lists/squads

1. **Need for (or not) member consent.**

GDPR regulations requires organisations to seek consent from members to use their personal data where the use of that personal data extends beyond that required to effect the transactional business of the relationship between the individual and the organisation holding the data.

It is not sufficient to rely on a default position of presumed consent. Instead all members must actively indicate their consent and be provided with a personal copy of what that consent is[[1]](#footnote-1).

Need for consent is not always necessary. If the organisation is satisfied that the nature of the relationship is purely transactional and that the data will not be used by anyone outside of the organisation, or for any purpose other than conducting the business of the organisation then the ‘Legal Business Interests of the Data Controller’ principle may be relied upon. (See RYA guidance for further information.)

Hollowell SC may choose to adopt this principle. However, if so it should be done with caution. For example if the assumption is that the members data will only be used for the subscriptions and or events that the data was recorded for the purpose of securing then this would be acceptable. However, if that data is used for other means by Hollowell SC officials or other club members who access the data, then the limitations of ‘Legal Business Interests of the Data Controller’ may have been exceeded. For example:

1. The Club publicity Officer publishes race results in Yachts and Yachting and mentions the names of the participants – Consequence: The participants may not have consented to their details (personal data) being used for this purpose and is therefore a breach of GDPR. The club would have to decide if it was a Business Interest to publicise the club in this way. If that was legitimate, it would need to be made clear when the individual applied for membership.
2. A member decides to request a duty swap from another member via e-mail. The reply exposes the other member’s e-mail address. Consequence: The personal data recorded by HSC (email address) has been passed to another member without their consent. The requesting member now has acquired personal data that could be exploited. A breach of GDPR may have occurred unless it is an appropriate use of member data in conducting the business of the club. Once again clear guidance that e-mail addresses would be used for this purpose would have to be evident.
3. A national training squad is keen to communicate with promising members of the Hollowell SC youth squad and the Youth Team Captain sends a list of potential contacts and provides phone numbers, dates of birth and e-mail addresses. Consequence: In the absence of securing consent, this would be a breach of GDPR.
4. A Fleet Captain sends a list of all Fleet members to the Fleet Association for the purpose of the Association reaching out for new members. Consequence: The Fleet Captain, unless consent was given, does not have the authority to share data that will be used for marketing purposes by an external agency.

What must be understood is that the risk to the Club is not likely to be form an external agency audit such as the RYA or Sport England but from a complaint received by the Information Commissioners Office regarding the misuse of personal data. In such cases it would be the club who would have to rely on providing the burden of proof that the individuals rights were not infringed rather than the individual proving the case.

*Nicola Wilkinson, at the recent budget meeting where this matter was aired in advance, asked if the entity known as HSC encompassed the all the members. In which case the issue of consent might be irrelevant. This has some merit. However, if you take this approach there are a couple of pitfalls.*

1. *Those ‘members’ who are not subscription paying, non-members for training courses, APMYC members etc would be outside of the entity yet the data would still be in the hands of the club. So how would these people be treated?*
2. *If all members were considered users of the data then the club would be obliged to demonstrate that it had a means of explaining to all members their obligations re the handling of personal data. Typically, this is effected by an education programme and an act on behalf of each ‘user’ that they can comply with the regulations. Since a third of ‘members’ are children this might be impossible.*
3. **Data Controller**

The Data Controller means “the natural or legal person which alone or jointly with others determines the purposes and means of the processing of personal data”. In the case of Hollowell, this should mean the General Committee, with personal liability vested in the Officers of the club.

1. **Data Processing**

“Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, determination or otherwise making available, alignment or combination, restriction, erasure or destruction”.

1. **Capture and Retention of Data**

Only data should be collected for which there is a legitimate purpose.

Data should only be retained for the purposes intended and not kept as a just in case measure. This is particularly important in respect of non-subscription records.

A policy should be in place that determines how and when data will be destroyed.

All personal data will need to be held securely and evidenced to that effect.

1. **General Issues for Hollowell.**
	1. A data policy will need to be created.
	2. Decision taken on whether or not consent is required or we rely on the interests of the Data Controller alone.
	3. The nature of the information collected on a membership application and whether it is required or not.
	4. Produce a list of all sets of personal data, electronic or otherwise.
	5. Review accessibility of web collect data – who should have access.
	6. Understand purpose and consequence of the CCTV system as it captures images which are personal data.
	7. Produce a data ‘processing’ statement that explains to all people we gather personal data from what we will do with it.
	8. Give clear guidance regarding the use of, security and handling of personal data held on ‘personal’ systems.
	9. Understand how access to webcollect data and the downloads available should be controlled to aid data protection. (For example to produce the latest boat park master list, we download the boat park locations from web collect as these are included in the craft data forms. The way web collect works is that it combines personal data with craft data. This means we get the name and 2 separate e-mail addresses in the download. In this example, whilst the name is necessary for managing the boat park, the 2 e-mail addresses are not necessary. What this means is that sharing the master list without e-mails would be fine, but once e-mails are included, the handling of the data becomes more stringent. We should be working with Web Collect to understand how we can limit fields included in downloads.)
2. List of Data List

|  |  |
| --- | --- |
| Description | Held By |
| Member Data | Membership Sec/WebCollect administrator |
| Child Protection database | Child Protection Officer |
| Dutyman | Dutyman |
| Front page’ of the certificates for adults that lists the name and level achieved. Paper copy. For the year I keep the docs at home, then they go in the filing cabinet in the Naseby lodge. | Principal |
| Booking form for a course, for a period of 3 years. (RYA requirement). This info has personal details and any maladies that might affect their ability to sail. For the year I keep the docs at home, then they go in the filing cabinet in the Naseby lodge. | Principal |
| PB and SB qualifications. This is on my PC, shared with the Chief Powerboat instructor. It has names, date of course completion, and certificate number. Excel spreadsheet. | Principal |
| Course feedback’ forms. Again for 3 years. These have names and what they thought of the course. Paper. For the year I keep the docs at home, then they go in the filing cabinet in the Naseby lodge. | Principal |
| list of the names of children and the certificates they have achieved. Excel spreadsheet. | Principal |

**Suggested Proposals:**

1. The General Committee are invited to consider the GDPR requirements and determine which approach of the following should be adopted:
	1. That where personal information is collected, the provider shall be asked to give consent or not for the use of that data to enable the effective running of the club.
	2. That where personal information is collected, the provider will be advised that the data will be used only for Legitimate Business Purposes of the Data Controller.
	3. That the club believes its existing data protection protocols are adequate and no further action is needed.
2. The General Committee must appoint a member of the General Committee to introduce GDPR and report back to the GC at the next 2 GC meetings with an update.

**Appendix 1**

RYA Legal Guidance Aug 2017

Getting Ready for the General Data Protection Regulations (GDPR)

The GDPR comes into force on 25th May 2018 replacing the Data Protection Act 1998 (DPA).

The purpose of this briefing is to give you a simple overview of the new Regulations and to help you start thinking about what you need to do in order to ensure you are compliant when they come into force.

GDPR applies to all organisations that process data, regardless of size or legal status (e.g. incorporated or unincorporated) or tax status (e.g. charity or CASC). There are no exemptions and clubs should note the fines for getting it wrong are potentially huge.

What does processing data actually mean?

**Processing** – *means any operation or set of operations performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.* Thus the collection of member data, participant data from race entries, collecting visitor information on an open day all constitute the processing of data.

**Personal Data** – *means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified directly or indirectly in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.*

**Data Controller** – *means the natural or legal person which alone or jointly with others determines the purposes and means of the processing of personal data.*

The Information Commissioner’s Office (ICO) website has a specific area for [GDPR](https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/) which we suggest you consult, however, it is predominantly written with commercial business in mind - do bear that in mind and don’t be put off by it.

We recognise that complying with GDPR may seem like a minefield, however, if your club is already complying the DPA it is likely to be halfway there to compliance with the GDPR. And whilst at first glance the GDPR appear insurmountable, the best way to approach it is in bite sized chunks.

**First Steps:**

Whilst the Regulations do not come into force until 25th May 2018, as from that date you will be expected to be compliant. We therefore strongly advise that you get underway now.

**Data Audit:**

Start with a data audit to enable you to assess what personal data you hold, where it came from and who you share it with. You will need to document this. This will no doubt take some time but will form the basis of everything else you need to do.

**Appendix 2**

**RYA Update Oct 2017**

**GENERAL DATA PROTECTION REGULATIONS**

**INTRODUCTION**

Data Protection law in the UK will undergo some significant changes with the introduction of the General Data Protection Regulations (commonly referred to as the **GDPR**). The GDPR will replace the current Data Protection Act from 25 May 2018. (The Government has confirmed that "Brexit" will not affect the GDPR from coming into effect so you cannot ignore it.) Although May 2018 seems some time away, the changes require some forward planning and may require changes in your forms and procedures.

This guidance note gives an overview of how the GDPR is likely to apply to sailing clubs, class associations, and recognised training centres. The uses you make (and want to make) of the information about living individuals which you obtain will be governed by the GDPR and we recommend that you adopt now the policies and procedures you will need under the GDPR.

It is a good opportunity to assess what information you really need, make sure it is up to date and that you obtain it in accordance with the GDPR. Failure to comply with the GDPR will attract very much higher penalties than now.

**DEFINITIONS**

The GDPR relates to **personal data** and **special categories of personal data**.

**Personal data**

Any information relating to an identified or identifiable natural person (referred to as the **Data Subject**). A person is identifiable if they “*can be identified, directly or indirectly, in particular by reference to an identifier such as name, an identification number, location data, an online identifier or to one or more factors, specifically the physical, physiological, genetic, mental, economic, cultural or social identity of that actual person*”.

**Special categories of personal data (Sensitive personal data)**

Personal data “*revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation”*.

The special categories of personal data do not include personal data relating to criminal convictions and offences but there are similar extra safeguards in relation to those types of data.

**Processing**

“A*ny operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, determination or otherwise making available, alignment or combination, restriction, erasure or destruction*”.

**Data Controller**

*“The natural or legal person, public authority, agency or other body which, alone or jointly, with others determines the purposes and means of the processing of personal data”*.

**IN PRACTICE**

Most, if not all, the information you request on your membership application forms, event entry forms and which you collect from visitors, suppliers, staff and volunteers will be personal data. That will include names, addresses, dates of birth, telephone numbers, and e-mail addresses. However, personal data can also include opinions held about someone and can include references to them in emails or other communication. Information about health and physical disabilities will be sensitive personal data to which additional safeguards apply.

Given the extent of the definition of “processing”, you should assume that any use you make, or want to make, of the personal data, as well as your collection, storage and destruction of it, will be governed by the GDPR.

**NOTIFICATION / REGISTRATION**

The requirements for organisations to “register” with the ICO is being removed by the GDPR and replaced by the general accountability obligation to demonstrate compliance with the data protection principles.

**DATA AUDIT**

The GDPR is a more extensive piece of legislation than the existing Data Protection Act. However, if you are already complying with the Data Protection Act you are likely to be well on the way to compliance with the GDPR.

You should establish whether your current policies and procedures are suitable to comply with the GDPR. If not, you should alter them.

Start with a review to assess:

* what personal data you hold;
* whether you need it;
* where it came from and the basis on which it was collected;
* what you do with it and are planning to do with it;
* where and how you store it.

You will need to document this.

You may have obtained the consent of the individual to whom the data relates when you originally collected it. If so, you should have told them, at the time you collected the data, what you would use it for.

If you cannot clearly identify that you have consent (in accordance with the GDPR) then you should consider whether you can use the data on one of the other bases of processing (see section **Collecting and Keeping Data**). If not, then you will have to collect the data again, with the appropriate consent request. The most convenient time to do this is on renewal of the individual’s membership but if that is after 25 May 2018 you need to be aware that you risk not being compliant with the GDPR when it comes into force. It is very important that the data is only used for the purposes which were made clear to the individual at the time the data was collected. You cannot, therefore, collect data for the purposes of managing a member’s membership and then use it to, for example, send them marketing information. If your records are unclear or if you have held the information for a long time you may need to collect fresh data with appropriate consents so that you know that it is “clean”.

**ACCOUNTABILITY AND GOVERNANCE**

The GDPR makes the principles of accountability and transparency far more significant than under the Data Protection Act. You must be able to demonstrate that you comply with the data protection rules.

There are specific obligations on maintaining records which apply particularly to organisations with 250 employees or smaller organisations where the processing is not occasional or includes sensitive persona data or is likely to result in a risk for the rights and freedoms of the data subject. Whilst the obligation to maintain records is unlikely to apply to the majority of RYA affiliated organisations we advise

A prudent approach is to have a data protection policy which records:

* the purposes of the processing;
* the categories of data subject and the categories of personal data which relate to them;
* the recipients / categories of recipients of the personal data;
* any overseas transfers of the personal data;
* general indication of time limits for erasure of the different categories of personal data;
* description of technical and organisational security mechanisms you use.

You should identify this information in any event in order to decide what steps you need to take to comply with the GDPR.

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. Getting ready for the 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 organisation to take ownership of the process is likely to be necessary.

Data protection rules are enforced by the Information Commissioner. The Information Commissioner's Office (ICO) has a website (ICO.org.uk) which contains very useful information. This Guidance Note contains links to some of that guidance which is likely to be particularly relevant.

2017 Page 5 of 13

|  |  |
| --- | --- |
| **THE PRACTICALITIES**  | **THE LAW**  |
| **Membership Information** * Only collect the information which you need and be clear on the application form (whether paper or online) what you will use the information for. (See “**Collecting and Keeping Data**”).
* Store application forms securely. Consider:
* who needs to see them;
* how long they need to be kept;
* the relevance of the application form once the applicant has been accepted or rejected.
* 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.
* If the application is rejected, destroy the financial information – you no longer need it
* If your application form is online and you take payment electronically use a recognised online secure payment system.
* Make sure that you keep all membership information up to date. If you renew memberships annually, ask members to check their information at renewal and provide an easy method for them to give you up to date information.
 | **Types of data** * You are likely to collect all or some of the following data:
* Name, address, date of birth, e-mail address, phone numbers and other contact details of members.
* Names of children who live at same address as a member.
* Grade of membership.
* Name and details of the boats owned by members.
* Date of joining the Club.
* Name, address, e-mail address, phone numbers and other contact details of suppliers, staff, volunteers, coaches and trainers.
* Name, address, date of birth, e-mail address, phone numbers and other contact details of participants in events and regattas, plus details of the boats they own.
* Race results (which includes names and possibly other details of members).
* Health information of members and others (which may be necessary for risk assessments).
 |
| **Former members** * Store separately the information you hold about former members from the information you hold about current members (whether on paper or electronically).
* Securely destroy all financial information you have about them.
* Consider the purposes for which you need to retain information about former members and record the reasons and the time period. (See **Storing Data**).
* Destroy all information about former members in line with your Retention Policy.
 | **Collecting and Keeping Data** * Data can only be processed lawfully, fairly and transparently.
* You can only process (and therefore collect) personal data in certain circumstances:
* Consent of the Data Subject.
* The legitimate interests of the data controller.
* Necessary for the performance of the contract with the data subject.
* Compliance with a legal obligation to which you are subject.
* Necessary to protect the vital interests of the data subject or of another natural person.
* Necessary for performance of a task carried out in the public interest.
* We recommend that, as far as possible, you only collect data which is necessary for the performance of the membership contract with the member. You can rely on that basis where, for example, you use information on an application form in a way which is necessary for the purposes of the membership of the applicant. So you can use contact details to notify members of, for example, club events and mooring issues, without needing consent each time, but you are not able to include a member’s details in a club directory without their consent. You should not assume that you can rely on your “legitimate interests” as data controller for all processing. Although that reason may be available to you it should not be regarded as a “catch all” and it is highly unlikely that it will be a valid basis for compiling a membership directory which is made available to members.
* You must record the basis on which you collect and use data.
* You must only collect the data you need for the purposes you have specified.
* When you collect data you must provide the data subject with certain information:
* Your identity and contact details.
* How you intend to use their data.
* Your lawful basis for processing their data.
* Details of anyone who may receive the 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.
* You must make sure the data remains accurate and therefore you must keep it up to date.
* You must keep the data for no longer than is necessary for the purpose for which you obtained it. If you make sure that you dispose of data when you no longer need it you reduce the risk that it will become inaccurate, out of date or irrelevant and therefore reduce your security risk
 |
| **Member Directories** * Consider the purposes of your Members’ Directory. It must only contain the information necessary to fulfil those purposes (e.g. the usual purpose of a members’ directory is to enable members to contact each other so name of member and telephone number and boat name is likely to be sufficient). It is unlikely that there is a need to include members’ home addresses in the directory.
* You can only include a member's details in your Member Directory if they agree that you can do so.
* Your application form must contain a box for them to tick (or something similar) to show they have agreed. You cannot use a pre-ticked opt-in box nor an opt-out box.
* The form must therefore make clear the information to be included in the Members' Directory.
* They must be able to change their mind at any time and no longer be included in the Members' Directory.
* If your Members' Directory is online then updates should be made regularly.
* If your Members' Directory is in hard copy then you should update it and circulate it annually. In that case you should make clear, when you seek consent for a member's details to be included, that their details will be included for the whole year.
* You cannot make membership of the club or association conditional on a member agreeing to have their name in the Members' Directory.
 | **Using data** * You may only use personal and sensitive personal data you have collected for the purposes you specified at the time you collected it.
* If you are relying on Consent as the basis for your use of the data, you need to be aware that the GDPR requirement for consent is more stringent than under the Data Protection Act:
* Consent must be given freely, be specific, be informed and be unambiguous.
* There must be a positive opt-in - you cannot infer consent either from inactivity, silence or pre-ticked boxes.
* Consent must
* Individuals must be given the right to withdraw their consent at any time and this must be as easy to do as it was to give consent in the first place.
* The ICO has a 2 page checklist of things to consider and include when you are seeking consent. https://ico.org.uk/media/for-organisations/documents/1625126/privacy-notice-checklist.pdf
* Whilst you may have relied on obtaining the data subject’s consent for information which you already hold you need to check that the consent you have complies with the GDPR requirements.
* You must keep evidence of the consent.
 |
| **Entries for Regattas and Events** * Only collect the information which 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 relevance of the application form once the applicant has been accepted or rejected or the event completed.
* If your 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 the application is rejected, destroy the financial information – you no longer need it
* If your application form is online and you take payment electronically use a recognised online secure payment system .
* If a sponsor of the event or regatta wants the details of those taking part you can only provide that data to the sponsor if the individual entrants agree. The application form for the regatta or event needs to make clear that you wish to pass their data to the sponsor and must give them a box to tick if they agree.
* Consent requires a positive opt-in under the GDPR (you cannot use pre-ticked opt-in boxes or opt out boxes).
* Entrants must be able to change their mind at any time and you must provide an easy way for them to do so.
* You cannot make entry to the event conditional on a participant agreeing to allow their name to be made available to the sponsor.
* There is guidance from the ICO about consent *[to be inserted when final guidance published*].
 | **Storing data** * You should have a data retention policy that takes 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 organisation 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.
* There is useful guidance on IT Security from the ICO https://ico.org.uk/media/for-organisations/documents/1575/it\_security\_practical\_guide.pdf
* Personal data cannot be transferred to a country or territory outside the EEA unless that country or territory provides a suitable level of protection for data.
 |
| **Giving Data to others** * The basic rule is that you cannot pass any data you have about individuals to anyone else (e.g. sponsors of events, other clubs) without the agreement of the individual (See sections **Entries for Regattas and Events, and Expulsion of Members** for further information).
* If you are being asked to provide data about a member to anyone other than that member, you should seek legal advice.
* If another organisation (e.g. an insurance company) wants you to send out information about their services to your members, you are not able to do that unless you have the agreement of each person to whom you are going to send the information.
 | **Access to data you hold/Subject Access Request** * An individual can ask to see the data you hold about them. This is known as making a Subject Access Request.
* The GDPR allows one month from the receipt of the request to respond.
* The GDPR does not allow you to charge a fee for responding to a Subject Access Request unless it is manifestly unfounded, excessive or repetitive.
* The ICO has useful guidance on subject access requests. https://ico.org.uk/for-organisations/guide-to-data-protection/principle-6-rights/subject-access-request/
* We have produced a separate Guidance Note on Subject Access Requests.
 |
| **Expelling / Disciplining Members** * If you decide to discipline a 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 discipline / expulsion and any other personal data you hold about them.
* Data about the member's expulsion are data relating to that member so other members do not have the right to see that data.
* If others object to a member's discipline you cannot disclose the data to them – they must obtain it from the member (if the member is willing to provide it to them).
* There are issues of confidentiality as well as data protection.
* See Section **Access to Data you hold / subject Access Request**
 | **Individuals’ Rights** * Under the GDPR individuals have various rights, such as:
* The right to be informed.
* The right of access.
* The right to rectification.
* The right to erasure.
* The right to restrict processing.
* The right to data portability.
* The right to object.
* The right not to be subject to automated decision-making including profiling.
 |
| **Looking after Data / Security** * You have a responsibility to look after data which you hold.
* You must take particular care of financial information as there is a serious risk to the owners of that information if it falls into the wrong hands.
* Your security obligations must be taken equally seriously whether you hold data in hard copy or electronically.
* See the section Storing Data for a link to advice from the Information Commissioner.
* Data in hard copy form should be kept in a locked cabinet to which access is restricted. It is preferable for appropriate steps to be taken to provide secure storage at your club premises if that is practical and is likely to be safe. If that is not practical or if you don't have club premises and you have hard copy data then it must still be kept securely. Therefore if the data is kept at an officer's home it should still be in a locked cabinet to which access is restricted.
* If you store data electronically be very careful if it is stored in "the Cloud".
* Cloud computing means access to computing resources on demand i.e. access to hardware and/or software.
* Cloud computing carries data protection risks which are not always obvious. Generally you, as the cloud customer, will be the data controller and have overall responsibility for complying with data protection rules. Cloud computing is not a “one size fits all” and so the data protection issues which apply can vary. If you are using cloud computing you should ensure that you have a written agreement with the cloud services provider. You may need to seek legal advice on the agreement and the data protection provisions which it should contain.
* It is important you know in which country the cloud service provider stores your data. If it is outside the EU/EEA you have additional responsibilities.
* There is guidance from the ICO about cloud computing
* https://ico.org.uk/media/1540/cloud\_computing\_guidance\_for\_organisations.pdf
* Whether 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 other person in the event of an emergency if the Treasurer is ill or away.
* Data held electronically should be encrypted.
* If you have arrangements with suppliers who process personal data on your behalf (e.g. the printer of your members' directory) the GDPR requires you to have a written agreement with them containing certain provisions.
 | **Data Breaches** * You must have documented procedures to detect, report and investigate data breaches.
* A data breach is a breach of security which leads to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. A breach is therefore more than just losing personal data.
* 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 on 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 or any other significant economic or social disadvantage).
* If a breach is likely to result in high risk to the rights and freedoms of anyone then you have to notify the individuals concerned.
 |
| **CCTV** * 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 (e.g. crime prevention).
* There is extensive guidance from the ICO on the use of CCTV: **https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf**
 | **Penalties** * Under the GDPR the penalties for breach are significantly greater than under the DPA.
* The following are links to cases where the ICO has imposed fines on organisations for failing to follow data protection rules. These have been imposed under the Data protection Act 1998 but show the breaches in which the ICO may take action.
* https://ico.org.uk/action-weve-taken/enforcement/data-breach-by-historical-society/
* https://ico.org.uk/action-weve-taken/enforcement/bloomsbury-patient-network/
* https://ico.org.uk/action-weve-taken/enforcement/data-breach-by-barrister/
* https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/06/
 |

If you have any queries, questions or comments on the information contained in this leaflet, kindly contact the Legal Team on 023 8060 4223 or legal@rya.org.uk.

**RYA Responsibility Statement:**

The RYA Legal Team provides generic legal advice for RYA members, affiliated clubs and Recognised Training Centres. The information contained in this Guidance represents the RYA’s interpretation of the law as at the date of this edition. The RYA takes all reasonable care to ensure that the information contained in this Guidance is accurate and that any opinions, interpretations and guidance expressed have been carefully considered in the context in which they are expressed. However, before taking any action based on the contents of this Guidance, readers are advised to confirm the up to date position and to take appropriate professional advice specific to their individual circumstances.

1. A copy of the consent Ts & Cs can be included in a communication or via a link to a web page where the member is invited to download a copy of the Ts & Cs that they have consented to. [↑](#footnote-ref-1)