General Data Protection Regulation (GDPR) & Gliding Clubs – part II of III

The new GDPR comes into force on 25th May 2018, replacing the Data Protection Act 1998 (DPA).
All organisations that handle personal data will need to comply with the new regulations. GDPR will continue to apply after Britain leaves the EU.

The UK's independent authority set up to uphold information rights is The Information Commissioner's' Office (ICO).
The ICO website contains a great deal of useful information including a myth busting blog.

The purpose of this document is to give you:

- a brief recap to give context to the notes in this document (but please also re-read the Phase I notes)
- a detailed look at personal data with respect to gliding and the legal bases for collecting and processing it; consent.
- sources of IT solutions whilst keeping processes simple and proportionate
- actions to be taken now (and an outline of development phase III)
- links to further information

GDPR opportunities: Fully understanding the data collected through the normal business of running of the club will:

- help you to run the club more effectively;
- highlight opportunities for communicating with the people on your database;
- increase participation by helping and encouraging people to join in more frequently i.e. getting more people to have more fun gliding.

Recap on background information and definitions

Definitions	*Taken from the ICO guide*
'Personal data'	Any information relating to an identifiable person who can be directly or indirectly identified, in particular by reference to an identifier.
'Data controller'	A controller determines the purposes and means of processing personal data.
'Data processor'	A processor is responsible for processing personal data on behalf of a controller.

- The GDPR applies to both 'controllers' and 'processors'
- The GDPR applies to processing carried out by organisations operating within the EU.
- The GDPR does not apply to certain activities including processing covered by the Law Enforcement Directive, processing for national security purposes and processing carried out by individuals purely for personal/household activities.

Full information from the 'Key Definitions' section of the ICO guide

Action area 1: Mitigating risk

Following on from the Phase I notes, you should already have mapped:

- Personal Data held;
- Data handling processes in use;
- Existing data safeguards;

This exercise should have identified the potential leak points in your systems.

To reduce the potential for leaks:

1. Make sure people who no longer need to hold people's personal data:
    a. have removed it from their machines;
    b. have had their access to club based records removed.

2. Make sure anyone who needs to hold copies on their machines has:
    a. Security patches – up to date now and processes in place to keep them updated;
    b. Antivirus – up to date now and processes in place to keep them updated;
    c. Password protected – their machines AND the data itself e.g. individual Excel spreadsheets;
    d. Has been trained and does not click on emails and links on social media that may be infected with malware and ransomware;
    e. Uses 'BCC' (blind carbon copy) on group emails to people on the club's database(s).

3. Look at what is available to improve security:
    a. Neither the BGA nor the person writing these notes is an IT expert, so we've tracked down some start points for you to use:
        i. There is a handy guide from the ICO 'A practical guide to IT security';
        ii. The possible solutions in Appendix A came from the Microtrading presentation at the November S&RA conference;
    b. We suggest you get expert IT input. Most gliding clubs have IT professionals within their membership who will be able to suggest appropriate people to work with. They may also be happy to volunteer to help out. Test the solutions on busy IT-phobes.
    c. Ensure any processes and solutions put in place are simple to use, especially by the average busy volunteer - don't make avoiding the safe route the easier option as this will simply increase your club's exposure to risk.

4. Think about how you will keep tabs on all areas of your 'data map' in the future:
    a. Set up a review process that will be simple to work through. Include notes for your successors;
    b. Set the next review date now;
    c. Think about the eyes and ears you have around your 'map' already – use the people in it to help keep things as leak proof as possible. (You have trained them / talked to them about how to do that).

Use this time as an opportunity to review the purpose for doing things the way you do – it may have been the answer 8 years ago, but does it still serve your club now? Could it (should it) be done differently? Do you still need it? (e.g. webcams/cctv in the bar)

Action Area 2: Legal Bases and when to get additional consent

Phase I notes set out the 6 legal bases for collecting, processing and holding data, of which two, *Contract*; and *Legal obligation*, cover most gliding scenarios. As far as we can work out at present, only one reason to ask for *Consent* (which is keeping ex-members & old friends up to date with club news and events).

From ICO the lawful bases for collecting and processing personal data are set out in Article 6 of the GDPR (full details in the ICO guide).

The three legal bases that concern us are:

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose

(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

ONLY ASK FOR CONSENT WHERE YOU NEED IT – NOT WHERE YOU DON'T!

If the personal data is collected and used to fulfil a legal basis, then that is the consent – there is no need to get consent again.

Types of data clubs might collect and process, by basis (some e.g. financial fall into 2 areas)

FULFILLING A CONTRACT

- Membership database
- Members accounts & financial records
- Instructing & coaching records
- Volunteer database & skills audit
- Club events

Sporting activity:

- Ladder
- Website & social media
- Articles in local press, S&G etc
- Interclub league
- Competitions

LEGAL OBLIGATION

- Flight logs
- A/C logbooks
- Medical information
- CP / VA
- HR & Employment
- Financial accounts

CONSENT

News & events for:

- ex-members
- Non-members

?! Club events – ICO say this could be marketing

This list may not yet be complete.

PLEASE LET US KNOW IF YOU IDENTIFY ANY OTHER TYPES OF DATA!

Club events: has been discussed with the ICO. They make a good point – that some people might not like getting emails about events, even though those events are part of club life (and membership). We will discuss this further ahead of Phase III because at the moment it feels grey-ish.

However, there are alternatives to a blanket direct email to all club members:

- Put notices in the club newsletter;
- Post on club social media;
- Give people an opt-in to be added to a mail shot list of emails.

Action Area 3: Responding to Individuals' Rights – the right of access; the right to erasure

The 6 GDPR principles
Down from eight under Data Protection Act and broadly equivalent, but with a couple of critical new features:

- inclusion of the accountability principle (increased transparency)
- inclusion of the right to erasure

Responding to an individual's requests: right of access. *What is the process for producing a soft copy of an individual's personal data?*
Under the new regulations an individual can access their personal data so that they are aware of and can verify the lawfulness of the processing. Within 1 month of receiving the request, someone from the club will need to gather together a copy of that personal data and send a soft copy to the person who made the request.

This may involve making hand-written notes and typing them up in an email; or using a screen print of their data; or exporting a data record to a document, which can then be sent by email. Identify how your club would meet such a request, who would field the request, who else (if anyone) needs to know that a request has been made, and who is responsible for ensuring the request is met within the time allowed.

Write briefing notes for other club volunteers. Detailed ICO information on the right of access to information.

Keeping data accurate
Leaving the club: Membership provides the legal basis (purpose) for much of the personal data the club holds. When someone's membership comes to an end, so does the legal basis for keeping their contact information. After that, you can only keep the personal data if you ask for consent to do so. This need for this purpose is likely to reduce to just their name and contact details, so there will need to be a process to safely discard of details such as date of birth and postal address.

As membership comes to an end, there should be a process in place that involves a communication with the individual to ask:

1. Would you like to renew your membership?
2. If not, would you like us to stay in touch with you about club news and events? (If yes, move them across to the club's legacy database)
3. Let them know they can stay in touch through the club's social media and will be welcome to attend club events, or to come and see you, come back for a flight, use the café facilities etc etc

You can then keep their (probably slimmed down) contact details until such time as they either renew their membership, or tell you that they no longer wish you to contact them. We'll give an indication in Phase III about the level of permission you need to go into e.g. an email tick box, or a new personal details form.

Keeping personal data up to date How does your club do this now? How will you do it in the future? This may be completing a membership form at renewal time and giving members the means of updating the club if details change during the year. Or perhaps a membership web area so club members can keep their own details up to date (but this relies on them taking the action). Understand the club's options. We will cover the length of time you need to hold different classes of data (e.g. flight logs) in Phase III.

Responding to an individual's request: deletion of data. *What is the process for deleting an individual's personal data?*
Under certain circumstances, an individual can request, verbally or in writing, that the club removes the data held. The club should respond to that request within one month. Full details of 'right to erasure' are on the ICO website and on receiving a request you should read that carefully.

In preparation, go through a similar set of questions and thought processes as above for producing a copy of the data held to identify the process(es), with notes, of responding to such a request. It is probably similar to the processes you will use when someone leaves the club.

Please dispose of personal data safely! Shred it.

It is important to understand that the right to erasure is not absolute and only applies in certain circumstances. For instance, the club's compliance with a legal obligation will override an individual's request.

What you don't need to delete – because the data is embedded in records and publications, is not being processed or it is impractical to do.

- Club publications, including on websites and social media (unless they are focus on them solely and/or they are recent and/or the individual(s) affected are requesting that because it has caused upset, offence or is affecting them in some other way)
- Competitions: competitor lists; results; news (someone taking part should expect these to be publicised)
- Club historical documents and archive – gliding heritage matters

Remember: lists of trophy winners, record holders, post holders, club members in any particular year etc should not include dates of birth, addresses, opinion on skill levels, and so on.

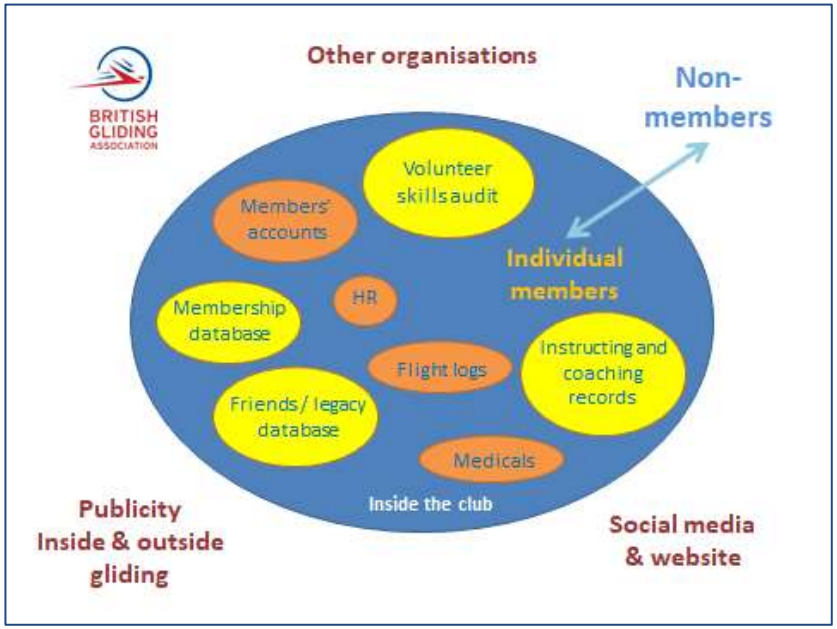
To put things in perspective – it is all about what happens on the boundaries.

When someone joins or leaves the club, that should trigger a data handling process.

When information about a club member is sent outside the club, there should be some thought about that:

- Is there a legal basis – is it to help you provide club (sporting) facilities; do you have consent?
- Are you over sharing? If it is about someone taking a flight, have you accidentally mentioned their name AND that it was their 80th birthday last Saturday and that they live in Little Marsh village
- Is what you are doing reasonable?

We'll cover the practicalities in more detail in Phase III



Actions to be taken now

Working towards GDPR compliance is an iterative process, we are now moving into the more detailed practical phase, with more detail to follow shortly about compliance documentation. Various sport organisations are working together to create sport specific compliance information and starter documents. The BGA will circulate these as soon as they become available.

The BGA will bring details to you as soon as they are made available and run training & discussion workshops if required.

Mitigate the risk for potential leakage of personal data held by the club (including the club's volunteers)	•From the data mapping you carried out at Phase I: •Is the data password protected everywhere that it is held? •Have all machines where data is held got security patch management in place? •Is antivirus installed and kept updated? •Do ALL the data holders know not to open odd emails / click on suspect links?
Developing good data processing habits	• What will be the process to produce an electronic copy of the data held for an individual? • What will be the process to delete an individual's personal data if they request it? • What will be the process for safely disposing of out of date data? • What will be the process for contacting temporary members to ecourage them back?
Review processes and succession planning	•You are up to speed on your club processes now - write guidance notes for next time •Who will be the Club's Data Protection Lead? •Look at your data map and identify methods for monitoring, evalaution and feedback •How will a review work? How will a review be triggered? Set date for the next review.
Legal bases - identifying other gliding purposes	• Are there any other purposes for collecting, holding and processing personal data? • Let Alison Randle know ASAP via alison@gliding.co.uk if you think of anything

Iterative phases for becoming GDPR ready
The BGA will be issuing notes for gliding clubs for each of these phases, using information shared and adapted from the sport sector and ICO.

Phase	Types of work	Likely timing of BGA notes	Factors affecting your action
1	The 4 sets of actions set out in this document – to map existing personal data that is collected and held; look at data flow around the club; sort out who's data you can continue to hold	Published	This requires volunteer time and office admin time (if your club employs someone)
2	Drill down into the legal bases; Look at systems required for managing data with respect to GDPR compliance and minimum drama; Consider which IT tools and resources can be usefully included in club processes	Published	Requires volunteer time. Care required to keep IT solutions straightforward for the IT 'less literate' volunteers
3	Adapt and adopt generic compliance policies and notices	Late April	Dependant on sport version availability
4	Workshops – for discussing aspects of implementing GDPR compliance	May	Depending on club need

Further information
The ICO website www.ico.org.uk
Information Commissioner's Office Overview of the General Data Protection Regulation
The ICO have taken the full 300 page monster original GDPR rules and got it down to about 20 short sections; you can jump via the index to the bits you're interested in.
Information Commissioner's Office Blogs
Series of blogs to dispel a few GDPR myths, key message is 'don't believe all you read about GDPR'.
Information Commissioner's Office Self assessment toolkit
Checklists help to assess your compliance with the Data Protection Act.
Information Commissioner's Office data protection guidance for small businesses
Some really nice resources for small organisations - practical and plain English.
BGA: to discuss gliding specific issues in relation to GDPR contact Alison Randle via alison@gliding.co.uk 01453 882 720 or 07910 300 246

Appendix A - From the Microtrading presentation at the Sport & Recreation Alliance conference in November 2017
Here are some of the main tools we (Microtrading) are using to help organisations get ready for the GDPR:

Azure: Microsoft's cloud platform that allows you to manage user identities and credentials and control access to your data with built-in capabilities that safeguard data and identify breaches.

Office 365: A cloud service offering a suite of applications and services to discover and control what personal data you hold and where it resides.

Enterprise Mobility + Security: A bundled offering from Microsoft providing some of the key tools needed to implement identity-driven security technologies that help you discover, control, and safeguard personal data

Windows 10 and Windows Server 2016: Industry-leading encryption, anti-malware technologies and identity access solutions

Managed IT Services and Security: Automated patch management and security updates to protect your system from cyber criminals targeting software vulnerabilities and zero-day attacks

Risk Intelligence: Identify sensitive data held on your devices and quantify the potential financial liability of this being breached

- Many of you will be using these already so it will just be a case of making sure you are making use of the features available to you.
- Those that are not should seriously consider making use of these technologies as running systems on-premise increases the burden on you to have the necessary documentation and ensure continued compliance.
- Microsoft offers substantial discounts to registered charities/non-profit organisations for the majority of their cloud services.

Meeting GDPR with Microsoft:

Microsoft have 4 areas of focus:

- Discover
- Manage
- Protect
- Report

Table to right illustrates where their products have features for each area.

		Discover	Manage	Protect	Report
Azure:	Data Catalog	●	●		●
	Key Vault		●		
Office 365:	Advance Data Governance		●		●
	Advance Threat Protection	●	●	●	●
	Data Loss Prevention	●	●	●	●
	eDiscovery	●		●	●
	Threat Intelligence	●	●	●	●
Enterprise Mobility + Security:	Active Directory Premium		●	●	●
	Cloud App Security	●	●		●
	Information Protection		●	●	●
	Microsoft Intune		●	●	●
Windows:	Bitlocker			●	
	Data Classification Toolkit	●	●		●
	Defender Advance Threat Protection	●	●	●	●
	Hello			●	
All:	Audit Logs	●			●
	Alerts		●		●