

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

The new GDPR comes into force on 25th May 2018, replacing the Data Protection Act 1998 (DPA). It 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 little background information
- an outline of the 6 GDPR principles
- actions to be taken now (and an outline of development phases II and 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.

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'.
- If you are a processor, the GDPR places specific legal obligations on you; for example, you are required to maintain records of personal data and processing activities. You will have legal liability if you are responsible for a breach.
- However, if you are a controller, you are not relieved of your obligations where a processor is involved – the GDPR places further obligations on you to ensure your contracts with processors comply with the GDPR.
- The GDPR applies to processing carried out by organisations operating within the EU. It also applies to organisations outside the EU that offer goods or services to individuals in 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](#)

Firstly, what is the legal basis for collecting, processing and holding data?

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](#)):

At least one of these must apply whenever you process personal data:

- (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).
- (d) **Vital interests:** the processing is necessary to protect someone's life.
- (e) **Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
- (f) **Legitimate interests:** the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

In regard to gliding clubs, taking out membership is a form of contract; clubs are legally obliged to keep flight logs and so on, so these bases already exist and additional consent is not required in these instances.

As part of our ongoing work to support clubs, we will check a number of scenarios to see if we can identify areas within normal club activities that may require additional consent and let you know in good time.

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.

Does your club need to register with the ICO?

Most gliding clubs probably won't need to register with the ICO as organisations or individuals who only process personal data for judicial functions, to maintain a public register or **for** domestic or **recreational reasons** are exempt. However, if your club uses CCTV for crime prevention purposes then you will need to register.

Action point: carry out the [quick self-assessment process](#) on the [ICO website](#).

Please note that regardless of the need to register with the ICO, your club will need to comply with the GDPR.

The 6 GDPR principles

Down from eight under DPA and broadly equivalent, but with a couple of critical new features:

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

Article 5 of the GDPR requires that personal data shall be:

- a) processed lawfully, fairly and in a transparent manner in relation to individuals;
- b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- e) 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
- f) 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.

Article 5(2) requires that: the controller shall be responsible for, and be able to demonstrate, compliance with the principles.

This translates to more paperwork, but with a logical approach GDPR compliance shouldn't be insurmountable.

The BGA will either be creating gliding specific starter (rather than template) documents and/or signposting clubs to relevant generic examples.

It is likely that your club will need to put the following in place:

- New policies: data protection policy; information protection policy
- A data protection notice, together with admin systems to ensure DPNs are issued at the point where personal data is collected
- Admin systems that will enable: erasure of personal data; issuing of an electronic copy of the personal data held for an individual
- Role description for the data protection lead (or job description if the role is held by an employee)
- Updated membership forms: full; temporary; junior

Actions to be taken now

Working towards GDPR compliance is an iterative process, so there are steps that you can take now, in readiness for when the more detailed, practical compliance information becomes available.

Various sport organisations are working together to create sport specific compliance information and starter documents.

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

Map existing personal data held by the club

- Why is it held?
- Who holds it?
- How do they use it?
- Who do they share it with?
- What format is it held in e.g. Excel spreadsheet; Sage etc

Look at existing data handling processes

- How is personal data added to the current database(s)?
- How does data flow through the organisation?
- How is it used and who handles it?
- How easily can data be removed or transferred to the legacy database?
- Do you have systems for contacting temporary members e.g. glider pilots from other clubs or people who have taken a trial lesson that you want to encourage to come back?

Check existing data safeguards

- 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?

Go through existing databases and sort into 'current' & 'legacy'

- As soon as possible, i.e. before May, contact people on the legacy database (tactfully) to explain you are carrying out a review and ask if they wish to continue to receive news from the club
- Remove any data that is no longer required
- Be considerate e.g. do not automate contact with the family of deceased club members

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	Now	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	During February	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	March / April	Dependant on sport version availability – probably end of March

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