# GDPR

The General Data Protection Regulation (GDPR) (EU) 2016/679 is a regulation in EU law on data protection and privacy for all individuals within the EU. It also addresses the export of personal data outside the EU.

**Terms**
Data controller: organisation holding the data and their appointed manager
Data processor: person using the data eg secretary, paddler development officer, treasurer
Data subject: person the data is about

**Comes into force 25th May 2018.**
**Scope:** Organisations that collect personal data whether it relates to personal, professional or public life. Type of information includes address, date of birth, a photo, a name or computer's ip address, coaching qualifications.

The principle is "privacy by design and by default" by the data controller. The organisation's data controller is responsible for third party data handling services so if we use external services, we must make checks that they are GDPR compliant. Our products and services have to ensure privacy by design.

The default status of all personal data is privacy. So, for updates and any marketing, users must opt in to specific types of information and choose communication method. The default is no communication.

**Data may not be processed (stored or used) unless there is at least one lawful basis to do so:**
The data subject has given consent to the processing of personal data for one or more specific purposes or:

1. processing is necessary for the performance of a contract to which the data subject is party or to take steps at the request of the data subject prior to entering into a contract – eg sales transactions, receipting etc;
2. processing is necessary for compliance with a legal obligation to which the controller is subject;
3. processing is necessary to protect the vital interests of the data subject or of another natural person (eg child protection);
4. processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (eg searching for a missing paddler);
5. processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party unless such interests are overridden by the interests or fundamental rights and freedoms of the data subject, which require protection of personal data, in particular if the data subject is a child.

Risk assessment and mitigation are required. We need to do a Data Risk Assessment. Are we high risk? I think not, but we do need to keep our house in order and ensure privacy. We do hold member data (see points 1 and 2), incident reports, child protection records, CPD records and email addresses. Also data on trustees. We use third party controllers (eg websites with forms, banks, Doodle Poll etc) and we need to consider use of these.

**Consent**
If consent is used as the lawful basis for processing, consent must be explicit for data collected and the purposes data is used for. Consent for children (u18) must be given by the child's parent or custodian. Data controllers must be able to prove "consent" (opt-in) and consent may be withdrawn. Opt-in measures (eg caption for a box tick) must be clearly understandable.

**Data protection officer/controller**

Public authorities and large organisations need to appoint a Data Protection Officer. I think it would be good practice to appoint a person responsible and first step is to risk assess what data we hold and our handling processes. B&BCC isn't a public authority or large organisation.

**Pseudonymisation and encryption**
Data can be encrypted or pseudonyms assigned. The data still has to be protected. http:// (hyper text transfer protocol) websites are not secure. https:// ('s' = secure) websites encrypt data transfer between browser and website. BBCC's website is a secure https:// type.

Secure wifi encrypts data transfer. 'Open' networks (eg Mackie D's) don't. Password protected data storage eg Dropbox and Google Drive, encrypt data. Dropbox encryption uses 256-bit AES keys to protect files at rest and encrypts data in motion with 128-bit AES SSL/TLS encryption or better. USB sticks in your trouser pocket aren't, generally speaking, considered secure.

**Data breaches**
Under the GDPR, the data controller is under a legal obligation to notify the supervisory authority without undue delay unless the breach is unlikely to result in a risk to the rights and freedoms of the individuals. There is a maximum of 72 hours after becoming aware of the data breach to make the report. Individuals have to be notified if adverse impact is possible. In addition, the data processor will have to notify the controller without undue delay after becoming aware of a personal data breach.

However, the notice to data subjects is not required if the data controller has implemented appropriate technical and organisational protection measures that render the personal data unintelligible to any person who is not authorised to access it, such as encryption.

**Right of access**
The right of access gives citizens the right to get access to their personal data and information about how this personal data is being processed. A data controller must provide, upon request, an overview of the categories of data that are being processed as well as a copy of the actual data. Furthermore, the data controller has to inform the data subject on details about the processing such as the purposes of the processing, with whom the data is shared, and how it acquired the data.

**Right to erasure**
A right to be forgotten is replaced by a more limited right to erasure in the latest version of the GDPR. The data subject has the right to request erasure of personal data related to them on any one of a number of grounds, including noncompliance with lawfulness. The legitimate interests of the controller are overridden by the interests or fundamental rights and freedoms of the data subject.

**Data portability**
A person is to be able to transfer their data from one electronic system into another without the controller preventing them (eg when transferring custom from one club to another). This excludes sufficiently anonymised data. Data provided by the subject and data observed by the controller eg behaviour, are included.

**Data protection by design and by default**
Data protection by design and by default requires data protection to be designed into the development of business processes for products and services. Privacy settings must therefore be set at a high level by default and that technical and procedural measures should be taken by the controller to make sure that the processing, throughout the whole processing lifecycle, complies with the regulation. Controllers should also implement mechanisms to ensure that personal data is not processed unless necessary for each specific purpose.

Encryption and decryption operations must be carried out locally, not by remote service, because both keys and data must remain in the power of the data owner if any privacy is to be achieved.

Outsourced data storage on remote clouds is practical and relatively safe if only the data owner, not the cloud service, holds the decryption keys, eg passwords.

**Records of processing activities**
Records of processing activities must be maintained that include purposes of the processing, categories involved and envisaged time limits. The records must be made available to the supervisory authority on request.