



DATA PROTECTION

WHAT IS IT ALL ABOUT

AND WHAT DO CLUBS NEED TO DO?

THE GENERAL DATA PROTECTION REGULATION (REGULATION (EU) 2016/679) (GDPR)

comes into force on **25th May 2018** (European-wide legislation) and will apply notwithstanding Brexit

UK legislation which includes the Data protection act 1998 will continue to run alongside the GDPR until that legislation is also updated, probably some time in 2019

practice and enforcement of data protection in the uk is overseen by the Information Commissioner's Office (the ICO) [WWW.ICO.ORG.UK](http://www.ICO.ORG.UK) where a great deal of guidance can be found

WHO DOES THE GDPR APPLY TO?

the GDPR applies to 'controllers' **and** 'processors'

a **controller** determines the purposes and means of processing personal data

a **processor** is responsible for processing personal data on behalf of a controller

the GDPR applies to processing by organisations operating within the EU and also applies to organisations outside the EU that offer goods or services to individuals in the EU

the GDPR does not apply to processing carried out by individuals purely for personal/household activities

WHAT IS PERSONAL DATA AND WHAT IS PROCESSING DATA?

PERSONAL DATA:

- Any information relating to an identified or identifiable (living) person 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 (living) person.

PROCESSING DATA means, whether electronically or on paper:

- Obtaining it;
- Recording it;
- Storing it;
- Updating it; or
- Sharing it.

WHAT IS “SPECIAL CATEGORY” OR SENSITIVE PERSONAL DATA?

SPECIAL CATEGORY or **SENSITIVE PERSONAL DATA** means personal data consisting of information as to:

- the racial or ethnic origin of a living individual,
- his political opinions,
- his religious beliefs or other beliefs of a similar nature,
- whether he is a member of a trade union,
- **his physical or mental health or condition,**
- his sexual life,
- the commission or alleged commission by him of any offence, or
- any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

WILL I HAVE TO REGISTER WITH THE ICO AS A DATA CONTROLLER?

The ICO has produced an online self-assessment (less than 5 minutes to complete) so that you can decide whether your club needs to register as a **Data Controller** with the ICO or not:

<https://ico.org.uk/for-organisations/register/self-assessment/>

Although it is a criminal offence not to register where an organisation is required to, typically, a Halliwick club is **UNLIKELY** to have to register as it is likely to be exempt from registration.

EXEMPTION FROM NEED TO REGISTER WITH ICO

The club will be exempt from the need to register as a Data Controller if, but only if:

- the club was established for not-for-profit making purposes;
- the club does not make a profit, or, if it does, it does so for its own purposes only; and
- any profit the club does make is not used to enrich others.

In addition, clubs must:

- only process information necessary to establish or maintain membership or support;
- only process information necessary to provide or administer activities for people who are members of the club or have regular contact with it;
- only share the information with people and organisations necessary to carry out the club's activities unless you have an individual's permission to share their information otherwise; and
- only keep the information while the individual is a member or supporter or as long as necessary for member/supporter administration.

DO I HAVE TO WORRY?

Being exempt from registration as a Data Controller with the ICO **DOES NOT** mean that you do not have to comply with data protection legislation. **YOU DO!**

- However, it isn't rocket science and you shouldn't panic!
- 'Common sense' will go a long way!
- When handling personal data of others, think about your personal data and how you would like it to be handled by others and you will be a long way along the road to handling data appropriately!

WHO IS RESPONSIBLE FOR DATA PROTECTION IN MY CLUB?

fundamentally,
everyone who
processes data
within the club for
club purposes should
act in accordance
with data protection
principles

- the GDPR says “the Controller shall be responsible for, and be able to demonstrate, compliance with the principles.”
- in practical terms in a club setting, the **Data Controller** is the club’s management committee (or where a registered charity, its trustees)
- others who process data within the club will likely be **Data Processors** so long as they are acting under the instructions of the data controller

personal
data
should
be:

KEY PRINCIPLES

- processed **lawfully, fairly** and in a **transparent** manner in relation to individuals;
- collected for **specified, explicit** and **legitimate purposes** and not further processed in a manner that is incompatible with those purposes;
- be **adequate, relevant** and limited to what is **necessary** in relation to the purposes for which they are processed;
- be **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;
- 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; and
- 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**.

LAWFUL BASES

To process data, you must have a **LAWFUL BASIS** for doing so. There are 6 lawful bases allowed:

- **(1) Consent:** the individual has given clear consent for you to process their personal data for a specific purpose.
- **(2) 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.
- **(3) Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations).
- **(4) Vital interests:** the processing is necessary to protect someone's life.
- **(5) 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.
- **(6) 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.

REMINDER!

WHAT IS 'SPECIAL CATEGORY' OR 'SENSITIVE PERSONAL DATA'?

SPECIAL CATEGORY or SENSITIVE PERSONAL DATA means personal data consisting of information as to:

- the racial or ethnic origin of a living individual,
- his political opinions,
- his religious beliefs or other beliefs of a similar nature,
- whether he is a member of a trade union,
- **his physical or mental health or condition,**
- his sexual life,
- the commission or alleged commission by him of any offence, or
- any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

LAWFUL BASES – SPECIAL CATEGORY DATA

if the data is of a **special category (sensitive)**, additionally, you **must** meet a condition (a further lawful basis) for processing that data

there are a total of 10 possible conditions available which allow the processing of special category data but only one will apply to Halliwick clubs

the data subject has given **explicit consent** to the processing of that data for one or more specified purposes

CONSENT

consent means any freely given, specific, informed and unambiguous indication of the individual's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her

- **Consent is valid if:**
- The controller can demonstrate that the individual has consented;
- Where consent is given in the context of a written declaration which concerns other matters, the request for consent is presented in a manner that is clearly distinguishable from the other matters, is intelligible, easily accessible and in plain language;
- The individual is informed that consent can be withdrawn at any time; and
- The performance of a contract, including the provision of a service must not be conditional on consent, except where this is necessary for the performance of the contact (or service).

RIGHTS OF INDIVIDUALS

the GDPR provides the following rights for individuals:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure (in certain circumstances)
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

THE RIGHT TO BE INFORMED

individuals have the right to be informed about the collection and use of their personal data

THIS IS A KEY TRANSPARENCY REQUIREMENT UNDER THE GDPR

- You must provide individuals with information including: your purposes for processing their personal data, your retention periods for that personal data, and who it will be shared with. This is '**privacy information**'.
- You must provide privacy information to individuals at the time you collect their personal data from them.
- If you obtain personal data from other sources, you must provide individuals with privacy information within a reasonable period of obtaining the data and no later than one month.
- There are a few circumstances when you do not need to provide people with privacy information, such as if an individual already has the information or if it would involve a disproportionate effort to provide it to them.
- The information you provide to people must be concise, transparent, intelligible, easily accessible, and it must use clear and plain language.

have a privacy policy which is given to all club members or anyone about whom you collect personal data and have it prominently accessible on your website

IN PRACTICE ...

it needs to set out:

- who you are
- why you collect and process personal data
- who you collect and process personal data from/about
- the personal data you might collect and process
- what you do with personal data
- who personal data might be shared with
- receiving marketing and further information from us
- the security of personal data
- how long personal data is kept
- the individual's rights concerning any personal data
- queries and complaints about personal data and who to go to



Search ...



Home



About



Swimmers



Courses & Training



Get Involved



Resources



News



Articles



Home

Home

A Special Halliwick Event...

Search ...

We are very excited to announce a special Halliwick event to be held in London on Saturday, 12 May 2018, especially aimed at our members who work with Halliwick within clubs ...

CLICK HERE FOR THE LATEST INFORMATION

Follow us for latest updates



Slideshow

THE RIGHT TO ACCESS INFORMATION

individuals
have the
right to
access their
personal
data

- You must provide a copy of the information **free of charge**. However, you can charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive.
- You may also charge a reasonable fee to comply with requests for further copies of the same information. This does not mean that you can charge for all subsequent access requests.
- The fee must be based on the administrative cost of providing the information.
- Information must be provided without delay and **at the latest within one month of receipt** of the request for the information.
- You will be able to extend the period of compliance by a further two months where requests are complex or numerous. If this is the case, you must inform the individual within one month of the receipt of the request and explain why the extension is necessary.
- You must verify the identity of the person making the request, using 'reasonable means'.

RIGHT TO RECTIFICATION

The GDPR includes a right for individuals to have inaccurate personal data rectified, or completed if it is incomplete.

- An individual can make a request for rectification (correct incorrect data) verbally or in writing.
- You have one calendar month to respond to a request.
- in most cases you cannot charge a fee to comply with a request for rectification.
- However, as noted earlier, if the request is manifestly unfounded or excessive you may charge a “reasonable fee” for the administrative costs of complying with the request.
- In certain circumstances you can refuse a request for rectification.

RIGHT TO ERASURE (AKA “RIGHT TO BE FORGOTTEN”)

individuals
have the
right to
have their
personal
data
erased if:

- the personal data is no longer necessary for the purpose which you originally collected or processed it for;
- you are relying on consent as your lawful basis for holding the data, and the individual withdraws their consent;
- you are relying on legitimate interests as your basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing;
- you are processing the personal data for direct marketing purposes and the individual objects to that processing;
- you have processed the personal data unlawfully (ie in breach of the lawfulness requirement of the 1st principle);
- you have processed the personal data unlawfully (ie in breach of the lawfulness requirement of the 1st principle);
- you have to do it to comply with a legal obligation; or
- you have processed the personal data to offer information society services to a child.

the GDPR specifies two circumstances where you should tell other organisations about the erasure of personal data:

- the personal data has been disclosed to others; or
- the personal data has been made public in an online environment (for example on social networks, forums or websites).

DO I ALWAYS HAVE TO COMPLY WITH AN ERASURE REQUEST?

the right to erasure does not apply if processing is necessary for one of the following reasons:

- to exercise the right of freedom of expression and information;
- to comply with a legal obligation;
- for the performance of a task carried out in the public interest or in the exercise of official authority;
- for archiving purposes in the public interest, scientific research historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing; or
- for the establishment, exercise or defence of legal claims.

You can refuse to comply with a request for erasure if it is manifestly unfounded or excessive

In that case, you can:

- request a "reasonable fee" to deal with the request; or
- refuse to deal with the request.

In either case, you will need to justify your decision.

DO WE HAVE TO APPOINT A DATA PROTECTION OFFICER?

clubs are not likely to have to appoint a Data Protection Officer (DPO) – only mandatory in specific circumstances – but it may be good practice to appoint one so that you have someone responsible for overseeing data protection policies and practice in your club

- The DPO isn't personally liable for data protection compliance. The club officers/trustees (as the Data Controller) and any other Processors remain responsible to comply with data protection obligations.
- Nevertheless, the DPO clearly plays a crucial role in helping you to fulfil your organisation's data protection obligations. The DPO should be your "go to" person and should be sufficiently familiar with data protection principles and requirements.

IN PRACTICE ...

in addition to your privacy policy, have a data management and retention policy

have a policy which sets out procedure in the event of a data access/rectification/erasure request and, should the worst happen, a breach

make sure everyone who deals with personal data in your club is familiar with these policies, understands them and knows what their obligations are

comply with data protection principles contained in the GDPR

be accountable – document who, what, where, why, when and how; if there is a breach, you will need to be able to show what happened, why it happened, what you had in place to prevent a breach, what you did to limit the damage that a breach caused or might have caused, why you made the decisions you did, etc.

IN PRACTICE ...

process data lawfully, fairly and in a transparent manner – know what your lawful basis is and, where consent is required, make sure you have it (remembering that there must be a lawful basis, and additionally for special categories of data, a condition met)

collect and process data for specified, explicit and legitimate purposes

make sure data is adequate, is relevant, is limited to what is necessary, is accurate, is kept up to date, and is not kept for longer than is necessary.

make sure data is 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**.

“APPROPRIATE TECHNICAL OR ORGANISATIONAL MEASURES”

What is appropriate for one organisation may not be appropriate for another – a local club will not be expected to take the same measures as, say would a multi-national company!

Use ‘common sense’ – if it were your data, how would you like it to be handled?

Think about risk – the more sensitive the data or the more likely a breach is to lead to significant consequences (for example, if the data relates to the disability of an individual or if the data covers several individuals), the more care needs to be taken.

IN PRACTICE ...

keep data secure, whether stored electronically or on paper and think about who should/could have access to it

do not share data inappropriately or inadvertently

be careful about destroying data and do it confidentially (shredding etc).

be careful about emails – don't inadvertently share email addresses (use BCC instead of CC where appropriate)

make sure that data on electronic devices is password protected using sufficiently strong passwords/codes and that malware/virus protection/firewalls are up to date

in general, data does not need to be encrypted, but if the data is particularly sensitive, there is a lot of it, or it is being kept on a portable device or disc which could get lost, this might well be an "appropriate measure"

use 'common sense' – how would you like your personal data to be handled and processed?



DATA PROTECTION

QUESTIONS!