PELICANS.H.C
Est.1920

General Data Protection Regulation (GDPR) Policy

This POLICY aims to help you understand the basics of the General Data Protection Regulation (GDPR) and how it will impact Pelicans Hockey Club.

The new regulation will have an impact on all sport and recreation organisations and it will change the way that we handle, use and store data about the people we engage with. The regulation is designed to strengthen existing data protection laws for all individuals who reside in the EU. Please be aware that even if the UK leave the EU it is most likely that it will adopt this Regulation into UK Legislation.
We have identified 10 questions that will help you to get to grips with GDPR. These are:

What is 'personal data'?

Personal data is defined as any piece of personal information that can be used to identify an individual, either directly or indirectly. This includes information such as an individual's:

- Name
- Telephone Number
- Email address
- Date of birth
- Health information
- Location data
- Online identifier e.g. IP addresses or cookies

What is 'sensitive data'?

The GDPR defines 'sensitive personal data' as data which reveals an individual's:

- Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Trade Union membership;
- Genetic or biometric details, where processed to uniquely identify an individual;
- Health details.

Under unless specific cases the GDPR regulations, organisations are banned from processing sensitive data, the individual gives the data holder his or her permission or processing is allowed in

What are the six privacy principles?

To comply with GDPR, Pelicans Hockey Club will have to meet six privacy principles· These are:

- Personal data must be processed lawfully, fairly and in a transparent manner;
- Personal data must only be collected for "specified, explicit and legitimate purposes"
- Data collected must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- Personal data must be accurate and where necessary kept up to date;
- Personal data that is no longer required should be deleted;

Processors should ensure all personal data they hold is secure.

What are the lawful bases an organisation can process data?

Under the GDPR, an organisation can lawfully process data only if at least one of the following conditions are met:

- The data subject has given their consent;
- If the processing is necessary for the performance of a contract;
- For compliance with a legal obligation;
- If the processing is necessary to protect the vital interests of the data subject;
- Public interest purposes;
- If there is a legitimate interest pursued by the data holder or a third party.

What rights does an individual have?

The GDPR reforms create some new rights for individuals when their personal data is being processed, as well as strengthen some of the rights that currently exist under the Data Protection Act. These rights are:

The right to be informed:

An individual has the right to be informed whenever their personal data is being processed. Any information an organisation supplies about the processing of an individual's personal data must be;

- Concise, transparent, intelligible and easily accessible;
- Written in a clear and plain language, particularly if addressed to a child;
- Free of charge.

The information an organisation must supply to an individual is determined by whether or not the organisation obtained that individual's personal data directly from them. More information on this can be found in the briefing produced by the Information Commissioners Office (ICO).

The right to access:

Under the GDPR reforms, an individual will have the right to obtain access to their personal data and confirmation that their data is being processed. This is similar to existing rights to access data that exist under the Data Protection Act.

Any information requested by an individual must be provided without delay and at the latest within one month of receipt. The information must also be provided free of charge, although the organisation who holds the data can charge a 'reasonable fee' if a request is repetitive or excessive. The data holder could also refuse to respond if they feel the request is manifestly unfounded or excessive, provided they explain why they have chosen to do so to the individual who made the request and inform them of their right to complain.

The right to rectification:

An individual has the right to ask for any wrong or incomplete information an organisation holds about them to be rectified. Any third parties who have had access to the personal data in question must also be informed about any changes. Any request for rectification must be answered within one month.

The right to erasure:

Also known as the 'right to be forgotten', this right allows an individual to request the deletion or removal of personal data that is held about them. However, this right can only be applied by an individual for a specific set of reasons, including:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally intended;
- When the individual withdraws their consent;
- When the individual objects to an organisation processing their data and there is no overriding legitimate interest to continue the processing;
- If the organisation holding the data is in breach of GDPR;
- The personal data must be erased in order to comply with a legal obligation;
- The personal data is processed in relation to the offer of online services to a child (which requires parental permission).

A data holder can refuse a request from an individual to erase their data for the following reasons:

- If it compromises freedom of expression and information;
- To comply with a legal obligation for the performance of a public interest task or exercise of official authority;
- For public health purposes;
- For research purposes that are in the public, scientific or historical interest;
- The exercise or defence of legal claims.

If the erased personal data has been shared with third parties, the data holder must inform those third parties that the data needs to be erased·

The right to restrict processing:

An individual has the right to ask the data holder to restrict the processing of their data if they have legitimate grounds to do so, though the data holder can still store the personal data.

The data holder is required to restrict the processing of an individual's data on the following grounds:

- If an individual contests the accuracy of their data;
- If an individual has objected to the processing, and the data holder is considering whether its legitimate interests over ride those of the individual;
- When processing is unlawful and the individual requests restriction instead of erasure of their data;
- If the data holder no longer needs to store the personal data but the individual requires the data for a legal claim.
- If a data holder has had to restrict the processing of personal data, it must inform any third parties with whom they have shared that data of the processing restriction.

The right to data portability:

An individual has the right to obtain and reuse their personal data for their own purposes across different services. This new right allows individuals to move, copy or transfer personal data easily from one IT environment to another in a safe and secure manner. An individual's right to move their data only applies to:

- Personal data that an individual has provided to a controller;
- Where the processing is based on the individual's consent or for the performance of a contract;
- When processing is carried out by automated means.

This data must be provided in a structured, commonly used and a machine-readable format, so that other organisations can use the data. The personal data must also be provided free of charge and must be handed over within one month.

The right to object:

An individual has the right to object to the processing (in particular for scientific/historical research purposes) or direct marketing of their personal data, although an individual can only raise an objection based on "grounds relating to his or her particular situation". The data holder must stop processing the personal data unless:

- They can demonstrate legitimate reasons for the continuation of processing the personal data which over-rides the interests, rights and freedoms of the individual; or
- The processing is related to legal claims.
- The data holder must also inform individuals of their right to object "at the first point of communication" and in a privacy notice.

Rights relating to automated decision making and profiling:

An individual has the right not to be subject to an automated decision intended to evaluate certain personal aspects relating to them, such as their performance at work, reliability, conduct etc. An automated decision is one in which technology is used to automatically make decisions, e.g. profiling someone to predict their performance or health. Fully automated decisions are rare, as most decisions do still have an element of human intervention. But they are becoming more commonplace, hence why this has been included.

This right applies if:

- The decision is based on automated processing; or
- The decision has a legal or similar effect. However, this right does not apply if the decision:
    - Is necessary for entering into a performance of a contract between the data processor and the individual;
    - Is authorised by law;
    - Based on explicit consent.

Where necessary, the data holder must ensure that an individual is able to:

- Obtain human intervention;
- Express their point of view;
- Obtain an explanation of the decision and challenge it.

What are a sport and recreation organisation's obligations as a data holder?

The 'accountancy principle' requires you as data holders to demonstrate that you comply with the principles.

To be able to demonstrate that you comply, we must:

- Create and implement appropriate internal data protection policies such as staff training, internal audits of processing activities and reviews of internal HR policies;
- Record data processing activities;
- If you have less than 250 employees you are only required to record high-risk data processing e.g. data that is related to criminal convictions/offences;
- Check if you need to appoint a Data Protection Officer (The ICO has more information on whether you will need one);
- Run impact assessments to anticipate any issues around data protection, particularly for high risk processing;
- Protect any personal data that you hold using appropriate security e.g. data about participants, volunteers, staff etc;
- Protect the rights of people who give you their data (see above) by ensuring your organisation has the right systems in place to be able to observe those rights;
- Ensure the data you are processing is secure and is kept confidential;
- Ensure that data is only collected in your organisation for specified, explicit and legitimate purposes and is kept accurate and up to date;
- Review how you get consent to use personal data and ensure the criteria for making data processing legitimate is observed;
- Build data protection safeguards into services from the earliest stages of development;

What happens when there is a data breach?

Under the GDPR, organisations holding data will be required to report certain types of data breach to the Data Protection Authority and, in some cases, to the individuals affected by the data breach. The GDPR defines a personal data breach as a "breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data".

The Data Protection Authority, which for the UK is the ICO, must be notified of any data breach that will result in a risk to the rights and freedoms of individuals e.g. it will result in discrimination, damage to reputation, loss of confidentiality etc. If this risk is particularly high, then the individuals who are affected must be notified.

Any data breach must be reported to the ICO within 72 hours of the organisation being made aware of it. Failure to notify a breach when required to do so can result in a fine of up to €10 million Euros.

What happens if I break the rules?

The ICO will be monitoring whether organisations are complying with the GDPR regulations. Any failure to do so will result in the ICO issuing anything from a warning to a fine of up to €20 million Euros.

Pelicans Hockey Club Data Policy:

Why do we collect your data?

Pelicans Hockey Club will collect data from you by means of the Subscription & Membership Form and through our 'private members area' within our website.

The lawful basis for collecting your data is that pelicans Hockey Club has a legitimate reason to collect and hold your data to ensure that it can operate as a Club and ensure its members and associates are able to fully utilise the membership. You have also provided your consent for us to hold your data in accordance with this policy.

The information collected from your membership form allows the treasurer to ensure that all members are identified and subscription fees are paid. It also provides a central database of all members contacts details and identifies any data protection restrictions such as 'no photography', medical or emergency contact details.

The information collected through the 'private members area' of our website is used to collate teams for the purpose of match selections and player profiles. Any personal information is protected by password and only accessible by members with passwords and permission eg. administrators. We will also be able to send you emails relating to general hockey and club related events and information.

Personal information such as addresses and telephone contact details will also be held by coaches who will also be subject to the same GDPR and data protection rules.

What data do we collect?

- Name
- Telephone Number
- Email address
- Date of birth
- Health information

- Location data
- Online identifier e.g. IP addresses or cookies

What about data of Minors (under 16years old) – parental consent

We have a legitimate reason to collect data of junior club members so that we can ensure their safety and to provide them with coaching and club membership requirements. Specific consent will be sought from their parent or guardian and any children under the age of 16 years of age who wish to be registered as a member on the website require parental/guardian permission and details to be entered into their profile allowing parental/guardian monitoring.

Sensitive Personal Data

The lawful basis for collecting sensitive personal data is under a legitimate interest to ensure the safety of our members. We will collect the following sensitive data where relevant;

- Medical information including allergies and injuries

Such data will only be collected with your express consent and will be held securely by the relevant coaching staff or team manager and by the data processor and data controller.

What data do we not collect?

We will not collect data which is irrelevant or discriminatory

We will not pass your details onto any third party for marketing purposes.

We may occasionally send you information about upcoming Pelicans or general hockey related events and offers. This will only be sent to you via the club facebook page or by email through the club website. Your express consent will be obtained before sending out any marketing information to you. You have the right to withdraw such consent at any time.

How we will store your data?

The Club Treasurer will maintain and have access to a current list of all members and associates on his personal data file and backup. These files are password protected and securely and appropriately stored. All written application forms and any written personal data are securely stored by the treasurer.

The data held on our website is managed and held by the website host Clubbuzz. Pelicans Hockey Club is not responsible for any data held by third parties but will however ensure that any data is only passed to third parties with your express consent and that any such third parties are also compliant with the GDPR.

We will not display any personal data in the clubhouse unless you have given your express consent.

Disclosure

Any information you provide to us will only be used by us and possibly passed to our partners for the purpose of dealing with payments and using communications portals. It may also be disclosed to your committee. You should also be aware that your information may be disclosed where we are obliged or permitted by law to do so.

Cookies

A 'cookie' is a small amount of information that is placed on your computer's hard drive when you visit a website. It collects details of visitor behaviour, which can be used to improve the service delivered to you on a website.

Your computer can be set to accept or reject cookies if you visit the "help" menu on your web browser. However, by rejecting cookies, you will not be able to use the "members' area" of the website and you will not be able to complete the registration process.

When you visit our website, your Personal Information may be collected using 'cookies'. Such information is subject to data protection laws and is dealt with in accordance with this Policy. For more information please visit : http://www.aboutcookies.org.

This site uses Google Analytics to collect usage data and Google also uses cookies for this purpose. Google has its own Privacy Policy which can be viewed at http://www.google.com/intl/en/privacy/privacy-policy.html. Where the site links to other websites and services these may also involve cookies. You are advised to check the privacy policy of each of these sites before using them.

Who is your data processor?

Currently Matt Bower and Nicola Pluck are your data processors

Who is your data controller?

Currently Sean Kerry is your data controller

How do we keep your data safe?

The Club subscribes to 'ClubBuzz' who host the Pelicans Website. All security of data within the website is managed by them and is contained within their own data policy. Access to personal data on the website is restricted to senior committee members. All members are able to send emails to other Club members through the website email system.

Any computers used to carry out club business are password protected.

All complete membership forms are stored securely by the Club Treasurer. Such records are kept for 24month after which they are destroyed.

How long will we keep your data?

All data and information held is reviewed every 6 months. All old, non-allocated or non-subscribed members will be removed from the database and website When you cease to be a member all personal data will be deleted within 6 weeks of the date of your resignation.

How/when can you remove your data? – "Right to be forgotten"

You can apply to the data processor or data controller either by email telephone, in writing or in person. We will remove your data NO LATER THAN 14 days of receipt unless specified as critical.

If you no longer wish to subscribe to our website you can unsubscribe at any time by following the link at the bottom of the homepage.

How often will we check we need your data and how will we do this?

Data will only be accessed in accordance with the reasons stated above. As stated we will review our database and website every 6 months and when required.

How can you complain if you are not happy?

You can complain to any member of your Pelicans Club Committee.

This policy will be reviewed annually and in accordance with any advice, update or recommendation from England Hockey and/or ClubBuzz. We will notify our members of all changes and updates.