Understanding the basic impact of General Data Protection Regulations (GDPR) and implications for our Club

Data Protection is regulated and enforced by the Information Commissioner's Office (ICO). The ICO is an independent authority set up to uphold information rights in the public interest and data privacy for individuals.

The ICO's powers include conducting audits, issuing warnings, serving enforcement notices and imposing fines for braches of data protection law.

Data protection law uses a lot of technical legal definitions. You need to be familiar with some of the key definitions to enable you to understand how data protection law works in practice.

Personal Data

What is Personal Data?
Personal data is basically any information which directly or indirectly identifies an individual. As well as information such as an your name, postal and email address, personal data also includes less obvious information such as opinions about individuals, location data, cookie addresses etc.

As well as the above, there is also Sensitive/special Category Personal Data, which include:

- Health
- Sexual Orientation
- Racial or Ethnic Origin
- Religious or Philosophical Beliefs
- Genetic data
- Political Opinions

Sensitive/special category personal data covers information that is likely to be of a private nature and which, if misused, could cause significant harm or discrimination to individuals. It therefore attracts a higher level of protection under the data protection law.

Processing sensitive/special category personal data is prohibited unless a specific legal condition or exemption applies;

- If we wish to process special/sensitive category personal data on the basis of the above, you would need to give your specific consent.
- A higher level of security is required if we handle sensitive/special category personal data.

Under this category we may hold Health information about you where this has an impact on your health and wellbeing whilst training and playing games. In this case we will have been given specific consent by you to hold this information.

What Forms of Personal Data are protected?
Generally speaking, in order to be protected by data protection law, personal data must either be held electronically, for example on computers or mobile phones, or form part of a paper filing system where personal data is stored using specific filing criteria.

Who has rights and obligations under the data protection law?

- Controller – This is Soham Rink Hockey Club as we are in charge of personal data and decide how to use it.
- Processor – (www.membermojo.co.uk) are our Data Processor. They process our data in accordance with their Privacy Policy (https://membermojo.co.uk/mm/privacy) and related terms and conditions.
- Data Subject –These are our club members (you) whose personal data is being processed.

Processing

Data Protection law regulates the "processing" of data. The definition of processing is extremely wide and it is difficult to think of anything we might do with personal data that would not fall within the definition of processing! For example any of the following would count as data processing: Collecting, Using, Disclosing, destroying, storing, erasing, disclosing, recording.

Data Protection Principles

We must process personal data in accordance with the data protection principles. These are a set of obligations imposed to ensure that personal data is processed properly. Under the GDPR there are seven data protection principles:

1. **Lawful, fairness**
   Personal data must be processed fairly and lawfully and in a transparent manner. This basically means that we must be open and honest about what we plan to do with personal data and only process it in a way you would expect. In addition, we must have a legal basis for processing personal data. These legal bases are set out in the data protection law and include the consent of the individual.

2. **Purpose Limitation**
   Personal data must be collected for specified, explicit and legitimate purposes. This means that when we collect your data for one reason (for example, to register you with the Club and competitions as outlined in the Privacy Policy), we should not use your personal data for any other purpose that you have not been told about, or would not expect.

3. **Data Minimisation**
   Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. This means that we should not hold more information than we actually need for legitimate purpose.

4. **Accuracy**
   Personal data must be accurate and kept up to date. This basically means that we must take reasonable steps to ensure that the personal data we process is accurate and updated as necessary.

5. **Storage Limitation**
   Personal data must be kept no longer than is necessary. Data protection law does not set out specific time periods relating to the storage of data. Instead it requires us to think about how long we need to keep personal data and why, after which it must be securely deleted. The time period for retaining personal data has been stated in our Privacy Policy.

6. **Integrity and confidentiality (security)**
   Personal data must be processes in a manner that ensures appropriate security. This means that we must take measures to prevent unauthorised or unlawful processing and accidental loss of or destruction or damage to personal data.

7. **Accountability**
   We must be able to demonstrate compliance with the data protection principles. This means that we are responsible for, and must take specific action to demonstrate data protection compliance.

The Main changes Introduced by GDPR

Demonstrating Compliance
The GDPR introduces the principle of "accountability", which essentially means that we are responsible for demonstrating our compliance with GDPR to the ICO.

The GDPR requires us to implement measures to insure that what we are doing with personal data complies with the GDPR and be able to demonstrate that compliance to the ICO. This means we must consider Data Protection impact on any actions we take as a club, such as arranging tournaments. We must also ensure that all our members are aware of our data protection principles.

Consent
One of the bases on which we can process personal data is that the individual concerned has consented to the processing of their personal data. Under GDPR this is defined as "any freely given, specific, informed and unambiguous indication of the data subject wishes by which he or she, by a statement or by clear affirmative action, signifies agreement to the processing of personal data relating to him or her."

The GDPR increases requirements for all valid consent. In particular:

- You must take a positive action (such as ticking a box) to give consent. Opt out boxes and pre-ticked boxes are not permitted
- You must have a genuine free choice when giving consent (eg an individual must not feel pressured into giving consent)
- Requests for consent must not be hidden within long legal docs or terms and conditions
- Separate consents should be given for different processing activities
- You have the right to withdraw consent at any time. You must be told about your right to do so and be given easy ways to withdraw consent. Consent must be as easy to withdraw as it was to give in the first place.
- We must keep clear records to demonstrate consent.

Privacy Notices

In order to process personal data fairly, lawfully and transparently (the first data protection principle) we must be clear and open about how we plan to use the data.
We are therefore required to provide certain information about data processing activities to you and we have done this through our Privacy Notice.

We must issue this to you as a current club member, and we must also provide this information at the point at which personal data is collected.

The GDPR increases the amount of information that we must be provided to you, for example, you must not only be told what personal data is being collected and why it is being processed, you must also be told on what legal basis it is being processed, who it will be shared with and how long it will be kept. The GDPR requires that the privacy notice is in an intelligible form and uses clear and plain language. We hope our Privacy Notice is clear, however please contact us if you have any queries on this.

Your Rights

Under GDPR, you have the following rights:

- Right to restriction – this is your right to block or suppress our processing of your personal data in certain circumstances. This right might arise where, for example, you have complained that personal data held us is inaccurate.
- Right of access – Under the GDPR, you have stronger rights to access information being processed about you and to obtain a copy of the information for free. This is known as a subject access request.
- Right to object – Under GDPR, you have increased rights to object to the processing of your personal data. If you object, we can only be able to continue with processing your data if we can demonstrate compelling grounds to do so.
    - In addition, you can still prevent the processing of your personal data for direct marketing purposes.
- Right to erasure - This is also known as the "right to be forgotten". The GDPR gives you wider rights to require that your personal data is deleted. This right will apply, for example, where our original purpose for which personal data was collected is no longer relevant. This could be if you leave the club and wish for your data to be removed before the timeline given in our Privacy Policy.
- Right to portability – where personal data is processed electronically, you will, in certain circumstances, be entitled to receive a copy of your personal data in a structured, electronic. format. You can even request that your personal data is transferred to another club.

- Right to rectification – This is the right to have inaccurate personal data rectified

Personal Data breach (PDB) Notification

One of the biggest changes introduced by GDPR is mandatory notification of certain PDB's.

- We are required to notify the ICO of any PDB's which could result in significant detrimental effect to you (eg financial loss, loss of confidentiality and discrimination).
- Notification must take place without undue delay and where feasible, within 72 hours of us becoming aware of the breach.
- We are also required, without undue delay, to notify you if you are affected by the PDB, where such a breach is likely to result in a high risk to you.
- We must also document all PDB's, even where the severity of the breach does not require notification to the ICO or you.

The levels of fines for breaches of Data Protection law are significantly increased under GDPR

How you can help us comply with the security and personal data breach reporting obligations.

What is a Personal Data Breach?
The GDPR defines a Personal Data Breach as - "breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed"

The definition of a PDB is wide and will include:-

- Destroyed data (unforeseen circumstances such as fire and flood), unauthorised access (someone accesses Personal Data or passes it on without proper authorisation).
- Human error (results in personal data being sent to the incorrect recipient), corrupt data (Personal Data is corrupted).
- Deception (by "blagging" an offence takes place where information is obtained by deception)
- Accidental loss (Personal Data is accidently lost or deleted)
- Cyber security (there is a network intrusion by third party eg a hacking incident or another type of cyber security attack)
- Password (inadequate security controls (such as weak passwords) result in an unauthorised person gaining access to our data base which holds personal data)
- Stolen data (data or equipment on which personal data is stored, is lost or stolen

A PDB therefore covers a wide range of incidents, including accidental breaches as well as situations where there has been deliberate or negligent action. Also, a PDB doesn't just cover data losses – a breach situation could arise, for example, if personal data is sent or accessed by unauthorised persons.

Steps you can take to help prevent a personal data breach

- Don't leave electronic devices containing Personal Data unsecured
- Keep your password for your computer secret
- Lock your computer if you are leaving it unattended
- Don't store Personal Data on unencrypted USB devices
- Store papers that contain Personal Data securely
- Don't send Personal Data be email unless it is passworded
- Dispose of Personal Data that is no longer required, confidentially
- Ensure your computer has the latest Anti-Virus
- Double check the email addresses is correct when sending any personal data by email
- Follow rules laid down by Soham Rink Hockey Club regarding data security

What to do if you identify a PDB
Don't delay, report the breach immediately to a committee member. This will give us the best opportunity of minimising the potential impact of a PDB and time to gather information to determine whether the breach needs to be reported to the ICO.