BRITISH JUDO

# INTRODUCTION TO GENERAL DATA PROTECTION REGULATIONS (GDPR)

GUIDANCE FOR CLUBS - APRIL 2018

On the 25th May 2018, the new General Data Protection Regulation (GDPR) will come into force across the UK. This enhances and changes commitments to handling personal data set out in the Data Protection Act (1998), strengthening and unifying data protection for all individuals.

## HOW DOES THIS APPLY TO YOUR CLUB?

GDPR applies to organisations that take personal data from its customers or members, for example via manual or electronic based formats e.g. member forms, online platforms or club website. It relates to how the club not only obtains personal information but how it then stores and uses this data. All clubs need to ensure that when dealing with personal data:

- They process it securely,
- It is updated regularly and accurately,
- It is limited to what the club needs,
- It is used only for the purpose for which it is collected,
- It is only used for marketing purposes if the individual has given the club consent to do so.

The principles of data protection set out within the existing Data Protection Act still exists and therefore, if you are compliant with this, it is likely you will only have a few changes to make to fall in line with the new GDPR regulation.

## WHAT IS PERSONAL DATA?

Personal data can be defined as any information relating to:

- A natural person,
- The data subject, who can be directly or indirectly identified by the use of that data; for example, by their name, ID number, or online identifier such as an email address.

Sensitive personal data can be defined as:

- Any information consisting of racial or ethnic origin,
- Political opinions,
- Religious or philosophical beliefs,
- Trade union membership,
- Genetic data, biometric data,
- Data concerning health
- Data concerning a natural person's sex life or sexual orientation.

GDPR relates to members who are participants at your club, coaches, referees, volunteers, parents and any individual that you request personal data from, or hold data on.

## SUPPORT AND GUIDANCE

- The Information Commissioner's Office (ICO) website provides important information and further clarity on GDPR which we advise all clubs to read. Please click here or visit www.ICO.org.uk/for-organisations.
- ICO Helpline on 0303 123 1113, and select Option 4 under the list of options.
- British Judo Association GDPR support: GDPR@britishjudo.org.uk

# ICO STEPS TO PREPARE FOR GDPR

In preparation for GDPR implementation, the ICO recommend that organisations take the following steps. All text in bold is taken directly from the ICO's guidance on GDPR (Preparing for the General Data Protection Regulation, 12 steps to take now, 2018). Clubs should take time to read through this guidance, using the weblinks to gain further information, before taking the required steps to become GDPR compliant.

## Awareness 

**You should make sure that decision makers and key personnel in your organisation are aware that the law is changing to the GDPR. They need to appreciate the impact that this is likely to have and identify areas that could cause compliance problems.**

Who in your club will lead the process of GDPR awareness? How will you communicate to members and parents the impact that GDPR will have on your club and any specific changes/updates that need to take place? All members should be made aware of who in the club they should contact regarding GDPR issues (see Data Protection Officer section later).

## Information your club holds 

**GDPR requires you to maintain records of your processing activities. You should document what personal data you hold, where it came from and who you share it with.**

You need to understand clearly what information you are collecting from your members, why you are collecting it and how it is then used and stored. A data inventory/map will enable your club to document clearly the flow of personal data through your organisation. Clubs are advised to bring together key individuals (such as your Committee and Coaches) to carry out this task and ensure all aspects of your club's processes are accounted for. You should also consider Data Protection by design and Data Impact Assessment (information below) alongside this.

**Click here for ICO guidance on data protection principles.**

## Data Protection Officers 

**You should designate someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements.**

We would advise clubs to check whether they are required to appoint a Data Protection Officer via the ICO website. It is recommended that either way, clubs identify an individual to take responsibility for data protection compliance. This individual should be fully supported by your club's Committee to carry out their role effectively.

**Click here for ICO guidance on Data Protection Officers.**

# Communicating Privacy Information 

**When you collect personal data you must give people certain information, such as your identity and how you intend to use their information. This is usually done through a privacy notice. Under the GDPR there are some additional things you will have to tell people. As part of the regulations, you will need to explain your lawful basis for processing the data, your data retention periods and that individuals have a right to complain to the ICO if they think there is a problem with the way you have handled their data.**

If your club doesn't have a privacy notice (also known as privacy statement) then you must create one and consider how you will make this available to members? For example, you could upload your notice onto your club website and/or distribute this alongside your club membership form. If your club has junior members you will need to ensure you have a version of your privacy statement that is accessible and understandable to them.

**Click here for ICO guidance on Privacy statement.**

# Individual Rights 

**You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format. The GDPR includes the following rights for individuals:**

- **The right to be informed,**
- **The right of access,**
- **The right to rectification,**
- **The right to erasure,**
- **The right to restrict processing,**
- **The right to data portability,**
- **The right to object, and**
- **The right not to be subject to automated decision-making including profiling.**

GDPR aims to give individuals (your club members) more control over how you process their personal data. You need to be prepared to respond to anyone wishing to exercise any of their rights listed above. For example, how would you deal with a request from a member to delete their personal details from your records? A few exceptions do occur such as when individual's details are required for public health/safeguarding issues and/or making or defending a legal claim.

**Click here for ICO guidance on Individual Rights.**

# Subject Access Request (SAR)

**This refers to an individual's right to access information an organisation holds on them. You should update your procedures and plan how you will handle Subject Access Requests to take account of the new rules:**

- **In most cases you will not be able to charge for complying with a Subject Access Request.**
- **You will have 30 days to comply, rather than the current 40 days.**
- **You can refuse or charge for requests that are manifestly unfounded or excessive. If you refuse a Subject Access Request, you must tell the individual why and that they have the right to complain to the supervisory authority and to a judicial remedy. You must do this without undue delay and at the latest, within one month.**

Your club must be able to respond to a Subject Access Request from a member who wants to access copies of what personal data you hold on them, which includes both paper and digital forms. Consider how you will isolate data relating to an individual whilst ensuring the privacy of others when doing a SAR. Who will be responsible for collating this and are they aware of the 30 day deadline? Clubs should make sure that they have the processes and policies in place to deal with such requests.

**Click here for ICO guidance on Subject Access Requests.**

# Lawful basis for processing personal data

Many organisations will not have thought about their lawful basis for collecting and processing personal data. You will also have to explain your lawful basis for processing personal data in your privacy notice and when you answer a subject access request.

GDPR requires you to document what information you collect, use and why. Processing data is only lawful when at least one of the following conditions apply: consent, contractual, legal obligation, vital Interests, public tasks and/or legitimate Interests.

It is likely that consent will be the most commonly used lawful basis by your club along with possibly legitimate interest and/or contract. Decide careful which lawful basis is applicable to your club and document this clearly within your privacy notice (also known as privacy statement). Clubs should not use personal data in ways that could have an unjustified or adverse effect on the individual concerned.

**Click here for ICO guidance on Fair and Lawful Data Principles.**

# Consent 

**You should review how you seek, record and manage consent and whether you need to make any changes. Refresh existing consents now if they don't meet the GDPR standard. Consent must be freely given, specific, informed and unambiguous. There must be a positive opt-in – consent cannot be inferred from silence, preticked boxes or inactivity. It must also be separate from other terms and conditions, and you will need to have simple ways for people to withdraw consent.**

How does your club collect personal information from its members and does it have the appropriate consent to then use this in the way it does? Consent must be clear and reflect the lawful basis you have identified above.

To ensure your club is GDPR compliant, you should consider what information you already have on your members and whether anything needs to be done to ensure you have the right consent. Ignoring this will make you liable for a data breach. You must also have a clear process in place to allow members to withdraw their consent at any point.

**Click here for ICO guidance on Consent.**

# Children 

**You should start thinking now about whether you need to put systems in place to verify individuals' ages and to obtain parental or guardian consent for any data processing activity. For the first time, the GDPR will bring in special protection for children's personal data, particularly in the context of commercial internet services such as social networking. If your organisation offers online services ('information society services') to children and relies on consent to collect information about them, then you may need a parent or guardian's consent in order to process their personal data lawfully.**

Under GDPR the default age to which an individual is no longer considered a child is 16 and therefore, parental consent should be gained for any members under this age. Clubs should also carefully consider their online activity and any engagement with young people through this. It is advised that clubs develop a social media policy if they do not already have one.

**Click here for Sport England's guidance on developing a social media policy at your club.**

**Click here for ICO guidance on Children**

# Data Breaches 

**You should make sure you have the right procedures in place to detect, report and investigate a personal data breach. The GDPR introduces a duty on all organisations to report certain types of data breach to the ICO, and in some cases, to individuals. You only have to notify the ICO of a breach where it is likely to result in a risk to the rights and freedoms of individuals – if, for example, it could result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage. Where a breach is likely to result in a high risk to the rights and freedoms of individuals, you will also have to notify those concerned directly in most cases.**

Clubs need to ensure that they have in place data protection measures to safeguard members' personal information. Some examples of what could be derived from a GDPR breach are:

- Accidently sending someone's personal information to the wrong contact
- Losing a club file that contains all the member registration forms for members in your club
- A cyber-attack on the computer system that contains personal information

Clubs must have a process in place to investigate potential data breaches, react to this by informing the individuals concerned and then notifying the ICO. Failure to report a breach could result in a heavy fine, as well as one for the breach itself.

**Click here for ICO guidance on Data Breaches.**

# Data Protection by design and Data Protection Impact Assessment (DPIA) 

**You should familiarise yourself now with the ICO's code of practice on Privacy Impact Assessments as well as the latest guidance from the Article 29 Working Party, and work out how and when to implement.**

GDPR makes 'Privacy by Design' a legal requirement. It requires a club to carry out a Privacy Impact Assessments (PIA) to identify, assess and minimize privacy risks from within their data processing. For example, your club could be at risk if it keeps member information in a folder that is left unattended at a session or using a computer data system for this information but not having the correct encryptions or security safeguards in place.

**Click here for ICO guidance on Data Protection by design.**

# International 

**The GDPR imposes restrictions on the transfer of personal data outside the European Union, to third countries or international organisations. These restrictions are in place to ensure that the level of protection of individuals afforded by the GDPR is not undermined.**

It is unlikely that this will be relevant to your club unless it operates outside of the European Union.

**Click here for ICO guidance on International Transfers.**

# EXAMPLE DATA INVENTORY FOR CLUBS

1. Identify a group of key individuals at your club (committee or selected coaches/volunteers) to support the implementation of GDPR compliance and circulate this guidance for them to read. Organise a meeting to discuss and review existing club policies and procedures.

2. Create a Data Inventory/Map that includes what data your club holds, where it has come from and who it is shared with.

3. Carry out a Data Privacy Impact Assessment (DPIA) to identify where the safety of individuals personal data could be compromised and/or a data breach could happen.

4. Review your club membership form to ensure that the correct consent has been given by your members (Please refer back to Page 6 for more information)

5. Produce a club Privacy Statement (or revise your existing) and make this available to all members.

6. Produce a GDPR/Data Protection policy (or revise your existing data protection policy) to include the following:

- o The clubs process for responding to anyone wishing to exercise their individual rights. The clubs process for investigating and responding to a potential breach.
- o Approach for maintaining and reviewing its compliance.
- o The clubs process for dealing with a Subject Access Request. You may choose to implement a specific form for members to use to assist with this.

7. Train key individuals within your club (such as coaches and your club welfare officer) to ensure they understand fully any new procedures that are being implemented alongside any club policies that have been revised or developed.

8. Communicate with your members any changes that have occurred as a result of this process and provide them with contact information for your GDPR lead.

# FURTHER READING

- Step 12 - The Privacy and Electronic Communications Regulations (PECR) sits alongside the Data Protection Act. They give people specific privacy rights in relation to electronic communications.

**Click here for ICO guide on PECR**

- Sport & Recreation Alliance, www.sportandrecreation.org.uk


**FOR FURTHER ASSISTANCE, PLEASE CONTACT**

**GDPR@BRITISHJUDO.ORG.UK**