



Data Protection Policy Reviewed 23rd April 2021

The Data Protection Act 1998

The information below contains an outline of the general law of data protection as it applies to all organisations in the UK.

The Data Protection Act 1998 (the “Act”), which came into force on 1 March 2000, overhauled data protection law in the UK. The Act implements an EU Directive on data protection (96/45/EC) and similar laws have been already or are being implemented across Europe. The Act imposes a significant regulatory burden on all organisations that process personal data about individuals and protects the rights of individuals regarding the use of personal data about them.

Summary of the Act

The Act applies to all organisations in the UK that process personal data about individuals. The Act covers personal data held electronically or in paper-based filing systems structured so that information relating to an individual can be accessed. “Personal data” means information that affects the individual’s privacy in his or her personal or professional life. It will include information kept on employee files such as personal details, medical records, etc. In summary, the main consequences for an organisation that processes personal data are as follows:

- The SKGB must make a notification with the UK Information Commissioner (the “Commissioner”) and inform individuals about processing concerning them;
- The SKGB must comply with the data protection principles set out in the Act; and individuals can ask to see their personal data and object to certain processing, such as use of their data for direct marketing purposes.

Notification

Before processing personal data, the SKGB must make a notification with the Commissioner at the data protection registry. It is a criminal offence for an SKGB to process personal data without having notified.

On notification, the SKGB must supply the Commissioner with certain details, including the purposes for which the data will be processed and persons to whom the data might be disclosed.

The Data Protection Principles

The SKGB must observe the data protection principles, which form the core of the Act, as part of their everyday operations. These principles broadly state that personal data must:

- Not be excessive for these purposes
- Be accurate and kept up to date;
- Not be kept for longer than necessary for the purposes;
- Be processed in accordance with the rights of individuals;
- Be adequately protected from loss, destruction or damage;
- Not be transferred to countries outside the EEA that do not have adequate protection for personal data;
- The information provided by the athlete in his or her application for funding under the WCP will be personal data, as will any further information about the athlete which the NGB obtains during the course of the WCP (such as, for example, his or her medical records).
- Be processed fairly and lawfully;
- Be only processed for one or more specified purposes;

Implications for the Scottish Karate Governing Body Ltd

The SKGB Ltd should ensure compliance through implementing a system of good business practice, including in particular:

- Notifying the Commissioner where required (failure to notify is an offence);
- Obtaining the members consent to the SKGB holding and processing personal data about them (especially in connection with "sensitive" data);
- Ensuring necessary information is provided to members, including information about the purposes for which the personal data will be used, informing them of their right to obtain access to any information held by the SKGB Ltd and their right to object to direct marketing;
- Implementing procedures to deal with requests from athletes to access their personal data held by the SKGB Ltd;
- implementing a formal policy of affirming the importance of good data protection practice and endorsing the data protection principles;
- Ensuring contractual security measures are in place where a third party processes data on their behalf.

Rights of Individuals

The Act gives individuals the following rights:

- To object to direct marketing
- To obtain access to personal data about the individual held by the SKGB Ltd;
- To receive information from the SKGB Ltd about the purposes for which the personal data will be used;
- To prevent use of the information that is likely to cause damage or distress;
- To object to purely automated decision-making in certain cases;
- To receive compensation for breach of the SKGB Ltd obligations;
- To require rectification or destruction of inaccurate information about the individual.

Enforcement

Under the Act, the Commissioner has the power to issue information notices and enforcement notices.

An information notice may require the SKGB Ltd to supply information to assess compliance with the data protection principles. An enforcement notice may require the SKGB Ltd stop processing or take particular steps if it fails to comply with the principles.

Failure to comply with an enforcement or information notice is a criminal offence, unless the SKGB Ltd can show that it exercised all due diligence to comply with the notice in question. In addition, the Commissioner has powers of entry and inspection in certain circumstances.

Individuals can complain to the Commissioner about activities of the SKGB Ltd which hold their personal data. Individuals also have rights under the Act to compensation for damage or distress caused by contravention of the Act.

Exemptions

There are some complex exemptions from some obligations contained in the Act. There are, for instance, certain cases where notification or disclosure of information to individuals is not required, such as where the public interest or national security requires otherwise.