

Milton Keynes and District Referees' Association

Data Protection Policy

May 2021

Commented [J1]: To be inserted once approved

1 Scope

1.1 To carry out its purpose, Milton Keynes Referees' Association (MKRA) collects and uses certain types of information about its Members. There are safeguards to ensure this personal information is collected and dealt with securely within the Data Protection Act 1998 and EU-GDPR.

1.2 This policy applies to everyone holding office for Milton Keynes and District Referees' Association (MKRA), regardless of their role, who obtains, uses, accesses or stores personal data.

1.3 This policy covers the processing of all personal information required for the functioning of MKRA. The policy applies regardless of how (*i.e.* both hard and electronic copy) and where the personal data is held, including on personally owned equipment.

1.4 This policy shall be reviewed in the event of any change in regulation and at least annually.

1.5 Under the General Data Protection Regulation (GDPR), MKRA is the Data Controller, which means that it determines for what purposes the personal information it holds will be used.

2. Data protection principles

2.1 Article 5 of the GDPR requires that personal data shall be:

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

2.2 MKRA is committed to processing data in accordance with its responsibilities under the GDPR.

2.3 MKRA has undertaken a self-assessment using the online checklist provided by the Information Commissioner's Office (ICO) website and, as a not-for-profit membership organization run for its members, does not need to be registered with the ICO.

2.4 Following self-assessment using the ICO website, MKRA does not need to appoint a Data Protection Officer. Nevertheless, following good practice, MKRA will nominate one of its members, ideally a non-serving Officer, to have responsibility for data protection and one who will undertake an annual audit of all MKRA data handling and processing activity to ensure the Association is compliant with this policy.

Commented [rs2]: Must be checked and confirmed by an MKRA Officer

2.5 This Policy aims to:

- a. ensure MKRA adheres to the data protection principles of the GDPR in all processing of members' personal data;
- b. protect the rights of individual data subjects by applying the principles;
- c. outline the roles and responsibilities of all users of personal data;
- d. outline the potential consequences of non-compliance with this policy.

2.6 MKRA shall ensure that the collection and storing of personal data is adequate, relevant and limited to what is necessary in relation to the specified purposes for which they are processed.

2.7 MKRA shall take all reasonable steps to ensure personal data is up-to-date and accurate.

2.8 Personal data will be kept for no longer than is necessary for the functioning of the Association; standard practice will be to retain the current, and immediately preceding, annual membership. All data pertaining to membership prior to this will be deleted. The data will be reviewed annually.

2.9 Any individual member of MKRA has the right to access their personal data, and any such requests made to MKRA shall be responded to within one calendar month.

2.10 MKRA will ensure that every Officer of the Association processing personal information is appropriately trained to do so.

2.11 MKRA will regularly review and audit the ways it holds, manages and uses personal information.

3. Lawful purposes

3.1 All data processed by MKRA will be done according to the following lawful basis: *legitimate interests*.

The rationale for this basis is that the association shares data with other specified agencies in the course of providing services to members. These agencies are specified in the MKRA Privacy Notice.

3.2 MKRA will note the appropriate lawful basis in its Privacy Statement.

4. Data storage and security

- 4.1 Data may be stored in paper copy and/or electronic format(s).
- 4.2 Data will be held for a maximum of two years, the current membership year and the preceding year. Any data older than two years old will be securely destroyed/deleted.
- 4.3 Data in paper copy will be stored in a secure, locked environment. Documents will be securely destroyed by shredding, or by any other means at least equal to that achieved by shredding.
- 4.4 Personal data in electronic format(s) will be stored securely in a strong-password protected cloud storage area that is kept up to date. Electronic files will be securely deleted using an appropriate file shredder.
- 4.5 The cloud storage area may be located outside the UK.
- 4.6 No files will be stored locally on MKRA Officers' personal computing equipment (PCs, laptops, tablets, mobile phones and the like); where membership data files are updated on a local computer, once updated and uploaded to the cloud storage area the local file must be securely deleted. Any computer in which the data file(s) is/are stored temporarily in this fashion must be password protected.
- 4.7 Access to personal data will be limited to only those MKRA Officers who need access, and appropriate security should be in place to avoid unauthorised sharing of information.
- 4.8 All file and storage area passwords will be changed annually so that only current Officers have access to members' data.
- 4.9 All file and storage area passwords will be changed immediately whenever there is a change of Officers so that only current Officers have access to members' data.
- 4.10 All file and storage area passwords will be changed immediately should a suspected breach of access occur; should such a breach, or suspected breach, occur all members will be notified immediately.
- 4.11 Membership data files will never be transferred as attachments by email; should any third party, e.g. the National Referees' Association, require membership data then temporary access to the file in the cloud storage area will be given.
- 4.12 Personal data will be deleted in such a way that the data are irrecoverable.
- 4.13 Email communication with MKRA members will be carried out in such a way that individual members' email addresses will not be visible to other addressees (e.g. by using email lists and/or the bcc function).

5. Data sharing

5.1 MKRA may share data with other agencies in the course of providing services to members. Specifically, these agencies are:

- MKRA Committee Members in carrying out their roles
- Berks and Bucks Referees' Association (BBRA)
- The Referees' Association (RA)
- The Insurance provider selected by the RA
- Approved Football bodies where there is a benefit to a member or members

5.2 Members will be made aware of how, and with whom, their information will be shared as set out in the MKRA Privacy Notice.

6 Privacy statement

6.1 MKRA will have a Privacy Notice, a copy of which can be found on the MKRA website at <https://www.mkra.co.uk/> and will also be distributed to members upon joining or renewing membership. The Privacy Notice will outline the personal data to be collected, and shared and distributed to existing members at the AGM and to new members joining during the season.

6.2 Any queries or questions in relation to this policy should be directed to the Milton Keynes Referees' Association at jon_bradshaw@sky.com

7 Breach

7.1 In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, MKRA will promptly assess the risk to member's rights and freedoms, inform members of such a breach, and, if appropriate, report this breach to the ICO.

8 Policy update

8.1 This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the Data Protection Act 1998 and EU-GDPR.

END OF POLICY