



## BRITISH MOTORSPORTS MARSHALS' CLUB LTD.

### Data Protection Policy

This policy applies to everyone involved in any way with the British Motorsports Marshals Club (BMMC), irrespective of role or capacity. The policy is effective from the Date of Issue shown at the bottom of this page.

## Statement of Intent

BMMC recognises its responsibility under the Data Protection Act 2018 (DPA) including the provisions made in the UK General Data Protection Regulations (UK GDPR), and believes that breaches are preventable. To operate effectively, and to meet our obligations, we process personal data relating to present, past and potential members. This may include data about children and their parents/guardians.

We will identify any potential data risks and put in place appropriate controls.

## Definition of Personal Data

Personal data refers to any information that could identify someone directly or indirectly. This includes things like name, address, email, birth date, bank details etc. The DPA also defines personal data to include elements such as location data or other online identifiers such as IP address.

The DPA also identifies so called "Special Category" data which is considered to be more sensitive, and so requires further protection. BMMC does not currently record this type of data.

## Policy Aims

To ensure effective implementation of this policy we will ensure data is:

- Processed lawfully, fairly and in a transparent manner.
- Collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which it is held.
- Accurate and up to date, ensuring that inaccurate data is rectified without delay.
- Kept in line with our Retention Guidance to ensure that personal data is only kept as long as it is required for the purpose it is held.
- 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.

BMMC will review this policy annually, as well as following a major regulatory change or in the event of any breach.

This policy will be communicated to all our member's and organisations working on our behalf, on our external website, and made available to third parties.

## Leadership Responsibilities

The Policy Owner, shown at the bottom of this page, is responsible for implementing this policy on behalf of the BMMC Directors who will monitor its effectiveness.

## Data Protection

The BMMC is a data controller and a data processor. We are not required to formally appoint a Data Protection Officer (DPO). The National Secretary is responsible for privacy and data.

|  |  |
|--|--|
| BMMC Policy Owner: John Edwards          | Policy Ref: BMMC/005                           |
| Date of Issue: 1 <sup>st</sup> July 2024 | Date of Next Review: 1 <sup>st</sup> June 2025 |

## **Holding Personal Data**

Ensuring personal data is collected and held in an appropriate manner is key to the successful operation of the BMMC.

In order to achieve this, the Club will:

- Undertake a Data Protection Impact Assessment for new software, databases or programmes of work that involve collecting, sharing or processing personal data, where this is likely to result in potential risks to the rights and freedoms of data subjects. This will also apply where existing systems are modified in such a way as to change existing ways of working.
- Identify a lawful basis in data protection legislation for collecting and sharing personal data.
- Collect, process and share the minimum amount of personal data required to achieve the objective(s), ensuring only that those who need access to such data have access.
- Use anonymised data where the identification of individuals is not required for the purpose of processing.
- Provide data subjects (individuals) with privacy notices and clear guidance on how to exercise their rights via the BMMC website.
- Ensure that a data sharing arrangement is in place where personal data is shared with external partners or there is a large-scale transfer of personal data. For the purposes of this policy, a large-scale transfer would involve more than 20 records. For the sake of clarity, sharing data with BMMC role holders is considered an internal matter.
- Ensure that data is not transferred to a country outside the UK or the European Economic Area, unless that organisation's security has been verified and the country has an "Adequate" level of protection for personal data as defined in law.

BMMC will only process personal data if it falls under one of the legal reasons set out by the Information Commissioner's Office: Consent; Contract; Legal obligation; Vital interests; Public task; Legitimate interests.

Children aged 12 and over e.g. (cadets) have the right to be informed and manage their own data. The same lawful bases as listed above also apply to children. (For children under 12, parental consent to process is required). The rights and freedoms of children are the same as for adults, including the requests covered later in this document.

## **Role Holders' Responsibilities**

All role holders are obliged to:

- Ensure that any information they provide to BMMC about themselves is accurate and up-to-date, and inform the club of any changes to their information, for example their address.
- Provide information in response to Data Protection audits and data breach investigations.
- In the event of a subject access request, provide all relevant information requested of them by a National Officer.
- Undertake training on Data Protection and Information Security when required to.
- Any personal data they hold is kept securely and that personal data is not disclosed accidentally or otherwise to any third party without authorisation.

All role holders should ensure that personal data is:

- when kept in hardcopy – including at home – is kept securely, such as in a locked drawer.
- not visible to anyone not authorised to see it, including on a computer screen,
- stored on BMMC systems only and if appropriate, password protected. not sent via e-mail without password protection or encryption if it contains, banking information, or data about children, and only sent to BMMC email addresses (@marshals.co.uk).

- not saved directly onto, flash drives, or other portable media.

Role holders should be aware that any information linked to an individual can be requested by that individual. Therefore, any remarks and annotations related to individuals should be appropriate, justified and relevant.

## **Subject Rights and Requests**

The DPA / GDPR provides 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.
- Rights in relation to automated decision making and profiling.

Requests should be made in writing to the National Secretary. BMMC will reply within one calendar month. Should there be a direct conflict of interest, the National Secretary may, by exception, request another Director's assistance.

## **Security and Retention of Data**

All records (including electronic, printed and handwritten) must be held securely to prevent unauthorised or unlawful processing or disclosure of data. Appropriate measures should be taken to minimise the possibility of accidental loss, destruction or damage to personal data. Role holders must not store Club data on, mobile phones or other personal storage equipment. Access to data must be limited to legitimate users only. Access to electronic records will be controlled through password protection and varying levels of access. Records should be kept only for as long as is necessary.

## **Reporting of Data Breaches**

A personal data breach is defined as: "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data."

The Club is responsible for ensuring appropriate and proportionate security for the personal data that we hold. The Club makes every effort to avoid personal data breaches, however, it is possible that data breaches will occur. Examples of personal data breaches include:

- Loss or theft of data or equipment.
- Inappropriate access controls allowing unauthorised use or access.
- Equipment or software failure.
- Unauthorised disclosure (e.g. email sent to the incorrect recipient).
- Human error.
- Hacking attack.

If a data protection breach occurs, the Club is required in most circumstances to report this as soon as possible to the Information Commissioner's Office, and not later than 72 hours after becoming aware of it. All breaches of this policy and data protection legislation must be reported immediately to the 3 National Officers, and role holders must take the action requested of them – such as complying with an investigation, contacting the IT Co-ordinator for support to secure an account, or informing others of virus or phishing attacks. A breach by a third party may result in a termination of contract.

## **Non-compliance with his Policy**

Data breaches are serious offences. Anyone found breaching this policy may face disciplinary actions or even criminal prosecution if they knowingly misuse personal information for their own purposes outside of legitimate BMMC purposes.

BMMC could also be fined for non-compliance with the Regulations.