

IMMAF DATA PROTECTION POLICY

1 Introduction

This policy applies to IMMAF and all staff and volunteers working on behalf of IMMAF.

The policy has been updated to enable compliance with the General Data Protection Regulation (GDPR).

IMMAF is fully committed to protecting the privacy of all individuals including staff, contractors, service users and others, by ensuring lawful use of their personal information in accordance with GDPR.

IMMAF shall take all necessary steps to implement this policy and to ensure that all staff and volunteers are fully aware of it and abide by it.

2 What is personal information?

This policy applies to all information collected and held by IMMAF relating to identifiable individuals. Data protection law regulates information about identified or identifiable individuals known as personal information. It is a concept broadly interpreted by regulators and the courts so that even if in some instances we don't know a person's name we still have to treat information about them as personal information. The GDPR applies to both automated personal data and to manual filing systems.

3 Why is Personal Information Collected?

In order to operate efficiently, IMMAF collects and uses information about people with whom they work. These may include members of the public, current, past and prospective staff members, clients, service users and suppliers. In addition, IMMAF may be required by law to collect and use information in order to comply with the requirements of Government.

4 Principles

IMMAF regard the lawful and responsible treatment of personal information as very important for successful operation and for maintaining confidence between IMMAF and those with whom it carries out business.

IMMAF will comply with data protection law by complying with certain principles. Through appropriate management controls, IMMAF will ensure that data:

- is processed lawfully, fairly and in a transparent manner in relation to individuals;
- will be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- will be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that which is inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- be kept in a form which permits identification of data subjects for no longer than is necessary for purposes for which the personal data is processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
- will be processed in a manner that ensure 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.

5 Approach to compliance

In respect of personal information IMMAF will:

- Comply with both the law and good practice
- Respect the rights of individuals
- Be open and honest with individuals whose personal information is held
- Insofar as is practical, provide training and support for staff and volunteers who handle personal information, so they can act confidently and consistently

IMMAF recognise that their first priority under data protection rules is to use information in a way that avoids causing harm to individuals. In the main this means:

- Keeping personal information securely in the right hands; and
- Holding good quality personal information

Secondly, data protection rules aim to ensure that the legitimate concerns of individuals about the ways in which their personal information may be used are taken into account. In addition to being open and transparent, IMMAF will seek to give individuals as much choice as possible and reasonable, over what personal information is held and how it is used.

6 Risks

IMMAF have identified the following potential key risks, which this policy is designed to address:

- Breach of confidentiality (personal information being given out inappropriately)
- Failure to offer choice about personal information use when appropriate
- Breach of security by allowing unauthorised access
- Failure to establish efficient systems of managing changes to volunteers, leading to personal information being out of date
- Harm to individuals if personal information is not up to date
- Failure to offer choices about use of contact details for staff and volunteers
- The misuse of information used by Data Controllers external to IMMAF

7 Roles and Responsibilities

Overall responsibility for ensuring compliance with the policy and with the legal requirements of data protection lies with the Board of Directors of IMMAF. They have delegated operational management of the policy to the CEO, who has responsibility for:

- Briefing the Board on its data protection responsibilities
- Reviewing data protection and related policies
- Advising staff on data protection issues
- Ensuring that data protection induction and training takes place
- Handling subject access requests
- Approving unusual or controversial disclosures of personal information
- Approving contracts with data processors/service providers

Staff are key to ensuring that IMMAF comply with this policy. IMMAF will ensure that:

- There is a Manager with specific responsibility for data protection.
- Everyone managing and handling personal information understands they are contractually responsible for following good data protection practice.
- Everyone managing and handling personal information is appropriately trained to do so.
- Everyone managing and handling personal information is appropriately supervised.
- Anyone wanting to access their personal information knows what to do.
- Queries about handling personal information are promptly and courteously dealt with.

- Methods of handling personal information are regularly assessed and evaluated.
- Data sharing is carried out under a written agreement, setting out the scope and limits of the sharing. Any disclosure of personal information will be in compliance with approved procedures.

Staff and volunteers will accept responsibility for compliance with these policies and procedures within the area which they manage. Significant breaches of these policies and procedures will be considered a disciplinary matter, to be handled in accordance with IMMAF disciplinary procedures.

8 Contractors and Third Parties

All contractors, consultants, partners or agents of IMMAF who are users of personal information supplied by IMMAF will be required to confirm that they will abide by the requirements of this policy. IMMAF will require that they enter into a data sharing agreement which will oblige them to:

- Ensure that they and all of their staff who have access to personal information held or processed on the behalf of IMMAF, are aware of this policy and are fully trained in and are aware of their duties and responsibilities under this policy. Any breach of any provision of the Act will be deemed as being a breach of any contract between IMMAF and that individual, company, partner or firm.
- Ensure that they only act on our instructions with regard to the processing of personal information we supply to them.
- Ensure that they have adequate security around personal information supplied to them and, in particular, will take appropriate organisational and technical steps to ensure that there is no loss, damage or destruction of such information.
- Indemnify IMMAF against any prosecutions, claims, proceedings, actions or payments of compensation or damages, with limitation arising out of any breach of the Act by them.

9 Data Recording and Storage

IMMAF will regularly review its procedures to ensure that its records remain accurate and consistent and, in particular

- ICT systems will be designed, where possible, to encourage and facilitate the entry of accurate personal information;
- Personal information on any individual will be held in as few places as necessary, and all staff and volunteers will be discouraged from establishing unnecessary data sets;
- Effective procedures will be in place so that all relevant systems are updated when personal information about any individual changes.

IMMAF will establish retention periods for at least the following categories of data and this shall be set out in our Retention and Disposal Schedule:

- Staff
- Directors/Committee Members
- Volunteers
- Participants
- Member Federations
- Information Service Beneficiaries

10 Rights of Individuals

Under data protection rules, individuals have rights to control how their personal information is used. This includes the right to access personal information, right to rectification, right to erasure, right to restriction of processing, right to data portability, right to object and right not be subjected to automated decision-making including profiling.

If IMMAF receive a request from an individual relating to the use of their personal information, such requests must be directed to and handled by the CEO or a person delegated that task by the CEO. All staff and volunteers are required to pass on anything which might be a subject access request without delay.

Where the individual making a request is not personally known to the CEO and IMMAF have reasonable doubts concerning their identity, we must verify their identity before handing over any personal information.

IMMAF will provide a response to a request within one month of the written request from the individual and we may extend the time period by a further two months where necessary due to the complexity and number of requests. Any required personal information will be provided in

permanent form unless the applicant makes a specific request to be given supervised access in person.

Any subsequent request which is made to correct personal information in the event that it is faulty will be addressed immediately, or at any rate as soon as is practicable.

11 Transparency

IMMAF are committed to ensuring as far as is reasonable and practicable that in principle individuals are aware that their personal information is being processed and:

- For what purpose it is being processed;
- What types of disclosures are likely; and
- How to exercise their rights in relation to their personal information.

Individuals will generally be informed in the following ways:

- Staff
- Directors/Committee Members
- Volunteers
- Participants
- Member Federations
- Information Service Beneficiaries

Via privacy notices

Whenever personal information is collected, the number of mandatory fields will be kept to a minimum and individuals will be informed which fields are mandatory and why.

12 Privacy Notices

A privacy notice is a statement that discloses some or all of the ways a party gathers, uses, discloses and manages an individual's personal data. It fulfils a legal requirement to protect an individual's privacy.

What should be included in a 'Privacy Notice'?

IMMAF privacy notices will tell people:

- who we are;
- what information we hold;

- what we are going to do with their information; and
- who we will share the information with.

However, they can also tell people more than this and should do so where you think that not telling people will make your processing of that information unfair.

13 Consent

Consent is one of the conditions that can be relied upon in order for use of personal information to be lawful. The GDPR sets a high standard for consent. Consent is not always required. If consent is difficult, look for a different lawful basis.

Consent means offering individuals real choice and control. Genuine consent should put individuals in charge, build trust and engagement, and enhance your reputation.

IMMAF will:

- regularly review their consent practices and any consent that does not meet the GDPR standard will be updated;
- include a positive opt-in for consent (pre-ticked boxes or any other method of default consent will not be used);
- ensure that consent is very clear and specific;
- keep consent requests separate from other terms and conditions;
- require that consent is given for different areas of the organisation's activities;
- provide details of any third party controllers who rely on the consent;
- make it easy for people to withdraw consent and tell them how;
- will keep evidence of consent – who, when, how, and what;
- try to avoid making consent to processing a precondition of a service; and
- take extra care to show that consent has been freely given from staff, and should avoid over-reliance on consent.

Consent will normally not be sought for most processing of personal information about staff and casual coaches, with the following exceptions:

- Staff details will only be disclosed to third parties (e.g. financial references) with their consent;

Personal information about members and participants will only be made public with their consent (this includes photographs).

Certain personal information will be classified as sensitive personal information. This 'Sensitive' personal information about members and participants (including health information) will be held only with the knowledge and consent of the individual.

For all of the above, any consent which is provided may be withdrawn, so long as this is done in writing – but not retrospectively, as there may be occasions when IMMAF have no choice but to retain data for a certain length of time, even though consent for using it has been withdrawn.

14 What are the lawful bases for processing?

The GDPR requires that IMMAF process all personal data lawfully, fairly and in a transparent manner. IMMAF will only process data to which it can demonstrate that a lawful basis applies.

The lawful bases for processing are set out below. At least one of these must apply whenever you process personal data:

(a) Consent: the individual has given clear consent for IMMAF to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract which IMMAF has with the individual, or because they have asked IMMAF to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for IMMAF to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for IMMAF to perform a task in the public interest or for IMMAF official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for IMMAF legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

15 Marketing

The law considers communications to be marketing in a very broad sense. In other words, most of the communication IMMAF sends to our members, participants and supporters will be marketing.

IMMAF will treat the following unsolicited direct communications with individuals as marketing:

- Promoting any IMMAF services or products; and
- Promoting active recreation sessions and other community events.

Whenever personal information is first collected which might be used for any marketing purpose, this purpose must be made clear to the individual, and we must collect consent for the use of their personal information for marketing purposes unless the law allows us to rely on opt out. For e-marketing we will obtain prior consent from individuals but must ensure that the consent is freely given, specific and informed and provided by a clear affirmative action, e.g. ticking a box which is not pre-ticked. Individuals always have the right to opt-out of marketing.

16 Confidentiality

IMMAF staff and volunteers will often have access to confidential information which may include, for example:

- Personal information about individuals who are members or otherwise involved in the activities organised by IMMAF;
- Information about the internal business of IMMAF;
- Personal information about colleagues working for IMMAF;

IMMAF is committed to keeping this personal information confidential. ‘Confidential’ means that all access to personal information must be on a need-to-know and properly authorised basis. Staff and volunteers must use only the personal information they have been authorised to use, and for purposes that have been authorised. They should also be aware that under data protection rules, unauthorised access to data about individuals can be a criminal offence.

Staff and volunteers must assume that personal information is confidential unless they know that it is intended by IMMAF to be made public. Disclosing personal information to a third party such as a mailing house, or vice versa does not count as making it public, but IMMAF must put in place a contract or receive other reassurances (as required by law) from the third party that the personal information will be adequately protected.

IMMAF must ensure that any disclosures to third parties of personal information are to third parties who have a legitimate right to receive the personal information eg WADA or other international organisations.

Staff and volunteers must also be particularly careful not to disclose confidential information to unauthorised people or cause a breach of security. In particular, you must:



IMMAF
INTERNATIONAL MIXED MARTIAL ARTS FEDERATION

- Not compromise or seek to evade security measures (including computer passwords);
- Not gossip about confidential information, either with colleagues or people outside of IMMAF; and
- Not disclose personal information – especially over the telephone – unless you are sure that you know who you are disclosing it to and that they are authorised to have it.

If in doubt about whether to disclose personal information or not, staff and volunteers should not guess, but instead should withhold the personal information while they check with an appropriate person whether the disclosure is appropriate.

These confidentiality obligations continue to apply indefinitely to staff and volunteers after they have stopped working for IMMAF.

Please note that if you suspect or know that personal information has been subject to a data security breach you must inform the CEO immediately since we may be required to notify relevant authorities or the affected individuals about any data security breach.