

GDPR and BMC Volunteers

Key Steps to be compliant with GDPR

What is GDPR?

The General Data Protection Regulation came in to force on 25th May 2018 replacing the Data Protection Act 1998. The regulation is updating the law to reflect the changes that have happened in the past 30 years in the way that we use data, particularly with technological advances. The regulation will give us, as citizens, much more control over the way that our data is used.

GDPR relates to the protection of 'personal data' by organisations and entities [such as clubs and the BMC] that process such data. 'Personal data' is any information relating to a natural (living) person that can be used to identify them such as a name, date of birth, postal address, email address, telephone number etc.

What does this mean for me as a volunteer?

The BMC holds personal data centrally about volunteers in a similar way to how it holds personal data on members. The way that we process that data is detailed within the BMC Privacy Policy.

However, any personal data that BMC volunteers hold (contact lists, attendee lists etc.) also need to be processed in a way that complies with GDPR.

There will be steps that volunteers will need to take to ensure compliance with GDPR. Some of these will involve a new way of working to ensure that we are all keeping the data that we have access to as safe and secure as we can.

Ideally volunteers should not hold or store data on BMC members or other interested parties¹ who we work with. Ideally all data should be held on the central BMC database. However, we don't live in an ideal world and there will be occasions when BMC volunteers will need to handle personal data and ensure its security, such as for an event.

The BMC Privacy Policy contains lots of detail but the following points are the key things that volunteers will need to do.

If at any time you are unsure what to do please contact your BMC Officer, the BMC Office or the BMC data protection leads. [Kate Anwyl & Alan Brown]

[¹ Does not include business contacts. Does include non-members]

Storing and Using Personal Data

It is advised that...

- All data processed (about members, participants, other volunteers etc.) is done to BMC standards.
- Personal data held on spreadsheets, emails, email lists, paper lists or similar is deleted or anonymised
- If old data needs to be kept it is sent to the BMC Office for storage and then deleted from personal records.
- If new personal data is acquired it is sent to your BMC Officer / BMC Office
- A Privacy Impact Assessment is to be produced for any event or activity where personal data is to be used (PIA's can be completed in conjunction with your BMC Officer).
- Those volunteers who need to use personal data to undertake their role will use 'MSO' to access it

- Only up to date personal data is to be used (hence why MSO is the one place where data will be held)
- Personal data that has been provided to a volunteer is to be held securely and deleted/destroyed once the event/activity has taken place.
- Personal data is only to be used for the purposes for which it was collected, and is not passed on to anyone else.
- Ensure any volunteers you work with who are involved in data handling are aware of their responsibilities

Emails

- Mass emails will all be co-ordinated from the office. The key volunteer (e.g. Area Secretary, Event Organiser) would send the content of the email to Jon Chittenden (jonc@thebmc.co.uk) who will then send out to the complete mailing list as required.
- Committee emails – committees are asked to consider alternative systems, such as Teamwork, to help to reduce the number of emails that volunteers receive directly in to their inbox.
- Later in 2018 there will be an option for key volunteers to have an *@thebmc.co.uk* email address to reduce the need for personal email addresses to be in the public domain.

There are several principles that the BMC (and every other organisation) needs to abide by to be compliant with GDPR. A few are listed below with the actions that the BMC will be taking to ensure compliance.

[The full list of principles is in the Glossary]

We need to keep personal data up to date and hold it securely	– we will hold all data on the BMC Database where members will be able to log-in and update their details and preferences
We need to ensure that we don't collect or retain excessive amounts of personal data	– we will only collect the data that we need and we will delete data that is old / out-of-date / no longer needed (see the BMC Retention Policy)
We have to identify a 'lawful basis' for processing personal data	– this is identified in the BMC Privacy Policy and is why mass mailings need to go from the office as it allows recipients the option to opt-out and to manage their mailing preferences

Glossary

Anonymising Data / Partial deletion

For the purposes of this document, 'anonymising data' can be used when you need to keep some records (such as the number of people who attended an event and the town that they travelled from) but you don't need to keep personal data to be able to identify those who attended. Basically you will delete the personal data that is not required so that everything that remains is anonymous.

Deleting Data

For the purposes of this document, the term 'deleting data' also requires deleted documents to be deleted from the 'recycle bin', the 'deleted items' folder or any other similar location. It also requires paper to be shredded or otherwise destroyed. If you hold a significant amount of personal data and you are looking for support in destroying it please contact the BMC Office for advice.

MSO – Membership Services Online

MSO is the portal for members to be able to access their personal data, make changes (such as changing their address) and update their communication preferences. It will be where volunteers will be able to access personal data relating to their role, i.e. competitor lists.

PIA – Privacy Impact Assessment

A 'PIA' needs to be completed prior to undertaking an event or activity where personal data will be used. It will identify whether there are any risks to data. In most instances this will be completed by or in conjunction with the BMC Officer.

Privacy Principles

To comply with GDPR, clubs (and all other organisations) will have to meet six privacy principles. These are:

1. Personal data must be processed lawfully, fairly and in a transparent manner;
2. Personal data must only be collected for "specified, explicit and legitimate purposes";
3. Data collected must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
4. Personal data must be accurate and where necessary kept up to date;
5. Personal data that is no longer required should be deleted;
6. [Processors](#) should ensure all personal data they hold is secure.

Processing data

'Processing' data is any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaption, alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, restriction, deletion or destruction.

This document has been written for BMC Volunteers to use to ensure compliance with GDPR. It is based on information available at the time of writing. There are several topics where the Information Commissioners Office still has to provide full guidance, therefore additional information may be made available in the future.

This guidance is provided by the BMC to assist volunteers and does not constitute legal advice.

Top Tips for BMC Volunteers

DON'T

- Store personal data on your computer, on email, on a memory/USB stick or in a web storage location
- Store personal data in a folder, or in a filing cabinet
- Share or pass on personal details to any other person
- Take paperwork to an event with personal data on it, unless you are able to keep it secure
- Leave personal data in a place where others may be able to read it or take it

DO

- Destroy personal data once you have finished with it or the event has completed
- Keep any personal data in your care as secure as you can
- Ensure that any Subject Access Requests you receive are passed to the BMC Data Protection Officer immediately
- Contact the BMC data protection leads if you believe that personal data in your care has been lost or stolen
- Contact the BMC Office / BMC data protection leads if you have any questions