



Instructions to Holders of Personal Information on MGF Members

The way that MGF holds and uses the personal information which it has on its members is subject to the EU General Data Protection Regulation (GDPR). This places strict conditions on how personal information is to be handled.

As an MGF administrator or organiser of an MGF event, you may need to have access to some of this information: for example, contact details of members in your area or of participants in a particular event.

You must ensure that your own handling of this information complies with MGF's policy on the protection of personal information. The full text of this can be found here:

[MGF Policy on Personal Information](#)

The purpose of these instructions is to provide a quick checklist of what may and may not be done when dealing with personal information.¹ They apply to all MGF administrators, whether elected committee members or those fulfilling a specific role with the association. They also apply to any non-administrator who is participating in the organisation of an MGF event.

1. Only collect the information that you really need for your task. Normally, this will be limited to contact information: name, email address and telephone number. Do not pass this information to third parties (including other participants in an event) without getting the permission of those concerned.
2. When getting permission, you should tell people what pieces of their personal information you will be passing on, to whom it will be passed, and why. This particularly applies when you ask people to supply additional information about themselves. When requesting such information, you must clearly state that it will be shared with others and that they may decline to provide it.
3. When passing on personal information to others, you should tell the recipients that they should treat it as confidential and not pass it on to others.
4. Do not post any personal information on social media such as Facebook or Instagram.
5. When sending emails to a group of recipients, the addressees should be placed in the blind copy field (BCC), so that the other participants do not see the others' email addresses. This also reduces the risk that the addresses are exploited by malicious software.²
6. At the end of an event, destroy permanently all copies of the information concerned in your possession (a simple list of the names of participants may be retained). Computer files should be deleted and the recycle bin (Windows) or the trash bin (Mac) emptied. Shred or burn paper copies. Do not forget to remove any mailing lists from web-based email systems such as Google group.

¹ In the event of any discrepancy between the full policy and these instructions, the full policy has precedence.

² Many viruses and spam programs are now able to sift through mail files and address books for email addresses. Using the BCC field acts as an anti-spam precaution because it reduces the likelihood that recipients will receive a spam message or a virus from another recipient's infected computer.



Consignes pour les détenteurs des informations à caractère personnel des membres de MGF

La méthode utilisée par MGF pour détenir et se servir des informations à caractère personnel de ces membres est assujettie au Règlement général de la protection des données (RGPD) de l'Union Européenne. Ceci soumet à des conditions strictes le traitement de ces informations.

Comme administrateur MGF ou organisateur d'un évènement MGF, il est possible qu'il vous sera nécessaire d'avoir accès à une partie de ces informations : par exemple, les coordonnées des membres dans votre région ou celles des participants à un évènement spécifique.

Vous devez tout faire pour que la manière dont vous traitez ces informations conforme à la politique de MGF sur la protection des informations personnelles. Le texte intégral de cette politique est ici :

[Politique MGF sur les informations à caractère personnel](#)

L'objet de ces consignes est de fournir une simple liste de vérification de ce qu'il est permis de faire et ce qui ne l'est pas concernant le traitement des informations à caractère personnel.¹ Elles s'appliquent à tout administrateur MGF, soit un élu du Conseil d'Administration, soit une personne qui remplit un rôle spécifique dans l'Association. Elles s'appliquent aussi à toute autre personne qui participe à l'organisation d'un évènement MGF.

1. Recueillez uniquement les informations strictement nécessaires pour accomplir votre tâche. En principe, celles-ci seront limitées aux coordonnées des membres : nom, adresse mail, numéro de téléphone. Ne les transmettez pas à autrui (y compris d'autres participants à un évènement) sans la permission préalable des personnes concernées.
2. En demandant cette permission, vous devez informer les personnes de quelles informations vous allez transmettre, à qui vous allez les transmettre et pourquoi. Ceci est particulièrement important si vous demandez aux personnes de fournir des informations supplémentaires leur concernant. Dans ce cas, vous devez informer les gens qu'elles seront transmises d'autres personnes et ils ont le droit de refuser de vous les donner.
3. Si vous transmettez des informations personnelles d'autres personnes, vous devez insister auprès de celles-ci qu'elles doivent traiter ces informations en confiance et ne pas les transmettre à autrui.
4. Ne postez jamais des informations personnelles sur les réseaux sociaux comme Facebook ou Instagram.
5. Si vous envoyez des mails à plusieurs récipiends, les adresses de ceux-ci doivent être placées dans la zone 'Bcc/cci', afin que les destinataires ne voient que leur propre adresse mail. En plus, cette procédure réduit la possibilité que les adresses soient exploitées par un logiciel malveillant².
6. Après un évènement quelconque, détruisez de façon permanente toute copie des informations en votre possession (il vous est permis de garder une simple liste des noms des participants). Effacez tout fichier informatique et videz la corbeille. Déchiquez ou brûlez des copies papier. N'oubliez pas d'enlever toute liste de diffusion stockée dans des messageries en ligne comme Google Group.

¹ En cas de divergence entre le texte intégral et ces consignes, c'est le texte intégral qui prime.

² Beaucoup de virus et de programmes spam sont capable de chercher les adresses mail dans les fichiers mail et les carnets d'adresses. L'utilisation du champ 'Bcc/cci' agit comme protection anti-spam parce qu'il réduit la possibilité pour un destinataire de recevoir un mail spam ou un virus de l'ordinateur infecté d'un autre destinataire.