

Frederiksberg Toastmasters GDPR Handbook

General Data Protection Regulation (GDPR) applies to Frederiksberg Toastmasters (hereafter “the Club”) when *personal data* is processed.

What is “personal data”?

Personal data is *any information relating to an identified or identifiable person* (“data subject”).

- Examples of personal data are: name, e-mail, telephone number, birth date, address, shoe size, CPR-number, job title, EasySpeak username, Toastmasters member number.
- As is seen, the definition of personal data is very broad. A general rule of thumb is that if information even vaguely relates to a person, it should be regarded as personal data.

What is “processing”?

Processing of personal data is any operation which is performed on personal data, such as collection, recording, organization, structuring, storage, and more. Simply storing data is regarded as processing. Therefore, when a Toastmasters club or when Toastmasters International keeps records of members contact details, they must be in compliance with GDPR.

Why does the club need to process personal data?

The purpose of the club’s processing of personal data is the proper administration and overview of the members of the club, and the processing of bi-yearly dues.

What kind of personal data is processed?

The Club processes information about:

- Its members
- Guests who attended club meetings and consented to be contacted
- Potential guests/members who contact the club

The information that is processed is only information that is required to maintain and administrate the club, such as contact information and information needed to process dues. The club never processes personal data that can be regarded as article-9 data in the GDPR.

The Club transfers information about all members to Toastmasters International Headquarters, which is located in the United States of America. Toastmasters International is the worldwide company which governs all of the individual Toastmasters clubs around the world.

When can the Club process personal data about its members or guests?

The only reason for lawful processing of personal data a Toastmasters club can have is *the data subject’s consent*

- The consent must be specific and the request for consent must be presented in a manner which is clearly distinguishable, using clear and plain language.
- A data subject can always recall their consent.
- When a person has consented to the processing of data with one purpose, the data can only be used for this purpose. If the club wants to use the information in another way than what the person has consented to, another consent must be gotten.

In practice:

- **All members must sign a privacy notice to be members of the Club.** If they do not, we cannot process their data, and therefore they cannot be registered as members of Toastmasters.
- If the club wants to collect signatures of guests to contact them and send information about the club, the guests must give their oral consent for this. It is required that guests write their contact information on singular sheets of paper. A list, where many guests put their contact information in the same sheet *cannot be used* since it enables guests to see other guests’ personal data, which would be considered a breach of personal data.
- It is included in the Club’ privacy notice that the club may use photos taken at meetings as promotional material on relevant social media or in print. This only applies to pictures of the audience, or a

significant part of the audience. If the picture focuses primarily on a specific person(s), e.g. a photo of contest winners, the image may only be used for promotional material *with specific consent from the subject*.

- If the Club wants to make a post on social media which contains personal data, the Club must receive specific consent first.
 - Example: Person X gave a speech and the VPPR wants to make a post about this speech, writing something like “at the meeting yesterday, X gave a wonderful speech about...” The VPPR will need a consent. In practice, such a post will also include a picture of the speaker on stage, which also requires a consent.

General procedures regarding deletion and correction of personal data

- Any e-mails, Facebook messages, etc. that the club receives from (potential) guests must be deleted **30 days after the correspondence has ended**.
- All members and guests can at any time recall their consent for the processing of personal data. In this event, *all* information about this person must be deleted.
 - If a member/guest wants to quit the club or have their data deleted, they must request this to a member of the board. If this is done, the board must delete *all* club records and accounts connected to this member. A note that all information about “X person” has been deleted is also personal data and can therefore not be made. **The request must be fulfilled within 72 hours**. If they wish to be deleted from the entirety of Toastmasters’ systems, see directly below.
 - Members who wish to recall their consent for all processing in Toastmasters in general should be referred to Toastmasters International where they can request total deletion of data - they should be informed that this will result in all traces of their previous achievements, e.g. progress in the pathways system, will be completely gone and that they will have to start from scratch if they choose to join again.
- All members and guests can at any time recall their consent for the processing of some of the personal data that the club processes.
- Everyone has the right to have their data corrected if the data is incorrect. If there is reasonable doubt whether the information which the data subject wants corrected is correct, the data subject’s argument must be duly noted.
 - *Example:* If the club roster states that a member is not in good standing because they have not paid their dues, the member has a right to have this corrected if he/she have actually paid the dues. If the treasurer does not agree that the member has paid their dues, this should be explained to the member. If the member insists that this information is wrong, the treasurer is required to note down that the member believes Toastmaster’s information to be incorrect, and the treasurer must strive to uncover the truth as quickly as possible.
- Everyone has the right to be informed about the personal data which the club processes about him/her. If the data subject requests this right executed, they must receive an overview of the personal data in written format.

Procedure in the event of a personal data breach

A breach of personal data include: computers storing personal data being hacked or otherwise compromised, the contents club’s internal Dropbox folder being hacked or otherwise compromised, the club’s Locker at the venue being broken into, board members who keep physical papers with personal data of other members in their homes having their homes broken into, the wrong person being CC’ed into an e-mail that contains personal data, etc.

In the event of a breach of personal data, the club president must **within 72 hours after becoming aware of the breach** make contact to the Danish governmental administration Datatilsynet (www.datatilsynet.dk) and inform them of the breach. The notice *must* include:

- Describe the nature of the personal data breach including the categories and approximate number of data subjects concerned.
- Communicate the name and contact details of the club president.
- Describe the likely consequences of the personal data breach
- Describe the measures taken or proposed to be taken to address the personal data breach.

A copy/translation of the notice to Datatilsynet should also *immediately* be sent to Toastmasters International Headquarters. Potentially compromised members should always be notified of breaches.

General code of behavior for the Board members and other members who rightfully gain access to personal data

- All personal data about all people who come in contact with the Club shall be treated with respect for the data subject's privacy and personal rights.
- Only relevant personal data shall be processed. For example, information about a member's race, sexual orientation, religion, etc. is *never* relevant.
- Only those for whom it is relevant shall have access to personal data. In the Club, this means that only members of the board or members of committees in charge of organizing events can process personal data.
- Personal data should only be stored digitally in e-mail clients or in the club's Dropbox/Google Drive folder that only the current board can have access to. Duplicates of documents should not be stored. If members of the board have physical papers that contain the personal data of members or guests stored in their homes, these papers must be stored out of general view, preferably locked up.

Joint liability of the board

Violations of the GDPR can result in big fines to the Club. The rules will be enforced by the Danish governmental administration, Datatilsynet.

In Denmark, board members of associations are jointly and severally liable for severely irresponsible and inadvertent actions that any member of the board makes. *In the absolute worst case scenario*, this means that if any member of the board, for example the VPM, violates the GDPR and the club receives a fine that it is not able to pay, *every member of the board can be held liable* for the remainder of the fine. This provides a strong incentive for all members of the board to understand what they can and cannot do regarding GDPR, and it requires board members to ensure that other members follow the rules.

Therefore, it is decided that every member of the board must sign a declaration of compliance (separate document).

This is a working document. Any suggestions for improvements is greatly appreciated.