



Toastmasters International offers the following guidance to club officers on how to comply with the General Data Protection Regulation (GDPR).

General Data Protection Regulation (GDPR)

GDPR will replace the Data Protection Act 1998 and will become enforceable in the European Economic Area on 25 May 2018.

Does this apply to our club?

The GDPR applies to any “data controllers” or “data processors.” Because your club collects personal data (e.g., name, email, address, phone number) to manage your club, the GDPR will apply. All clubs will receive a new privacy notice with a consent section to be presented to current members as soon as possible, and to guests when they visit your club.

My club has only a few members. Does GDPR still apply to my club?

If your club collects and stores any personal data, you must manage the data in accordance with strong data protection principles, or you could be fined.

What steps can I take to ensure that my club is GDPR-compliant?

- 1) Create a process/risk assessment:
 - Each club is responsible for ensuring GDPR compliance. A member of the club executive committee should take on the role of coordinating GDPR compliance activities. Toastmasters International recommends that it be the club secretary, but any officer can take on this role.
 - Create a document for members to easily visualize the club compliance activities. A best practice is to create a flowchart or list showing:
 - Where the data is
 - How it is accessed
 - Who has access
 - How it is used
- 2) Provide a privacy notice and consent form to each person for signature one time upon visiting your club. (Toastmasters International has included this template for you.)
- 3) Obtain Consent
 - New members, guests and current members should all be provided with the new club privacy notice and consent form. The consent section will allow the individual to opt in or out of having his or her data used, outside of what is needed to run the club. The club is to hold the form in its records as long as they hold any



data for that member or guest. It is important to note that you have the right to collect names as a function of managing your club, but to send out mail, email or phone messages to members and prospective members will require this signed consent on file.

4) Security

- Club information kept on a computer must be secure. Computers should have the latest software/security installed. Access to information should only be accessible by a secure password.
- If you use the Cloud, see the section below on third parties and Cloud services.
- If hard copies of information are stored, they must be kept in a lockbox, accessible by one officer, who keeps that box in their possession.
- Club officers should consider whether they can function using Club Central as their only information storage point. This limits the amount of liability the club has.

5) Outside Vendors

- If you are using any sort of Listserv (a software that helps to create an easy to use email recipient list) or website hosting in general (such as easy-Speak, FreeToastHost, or others); we highly recommend getting a statement from that service that they are GDPR-compliant. Most services will have this readily available.

6) Data Retention

- Data should be held only as long as it is being used. If someone requests their data be erased, your club must comply within a reasonable amount of time, within 72 hours is recommended.
 - It is important to advise that if a member requests complete erasure, they should be advised that the club will not be able to go back and retrieve those records, erasure will be permanent. This erasure may take place when a member switches clubs, or decides they no longer want to be a Toastmaster.

7) Subject Access Requests

- An individual may request a copy of their personal data the club retains at any time. Data should be provided without delay. We recommend logging these requests.

8) Breach

- If you discover your member data has been breached, you must report it to your country's supervisory authority within 72 hours.
- World Headquarters should also be notified immediately at **clubquality@toastmasters.org** or by calling in and asking for the club quality department.



What are the key things to consider for clubs?

The principles of data protection still exist. All clubs need to ensure that with regard to personal data:

- 1) They process it securely
- 2) It is updated regularly and accurately
- 3) It is limited to what the club needs
- 4) It is used only for the purpose for which it is collected and only used for communication purposes if the individual has given the club consent to do so

Who is responsible if we use a third-party website or Cloud services to manage our club data?

There will be direct obligations on data processors (third party) as well as on data controllers (the club). This may mean that if you use any third parties to process data, for example hosting your website, then you must have a written contract in place. Data security is key and when storing anything online you need to ensure that you protect the club by ensuring you keep passwords safe. Cloud services like Dropbox, OneDrive and Google Drive have built in security measures for the protection of files in storage or in the process of being shared. When using third-party software, you need to ask for assurances over the security of the system. For example, ask the provider for an explanation of how data security is managed or ask if a Data Privacy Impact Assessment has been undertaken. You also must consider how you might revoke access when individuals change roles or leave your club.

Could we be fined?

Under the GDPR, your country's supervisory authority will be able to issue fines up to 20 million euros or 4 percent of your global annual turnover (whichever is the higher) for serious breaches. The more members you have, the greater the risk.

The Toastmasters International legal team provides generic legal guidance for Toastmasters clubs. The information contained in this guidance represents Toastmasters International interpretation of the law as of the date of this communication. Toastmasters takes all reasonable care to ensure that the information contained in this guidance is accurate and that any opinions, interpretations and guidance expressed have been carefully considered in the context in which they are expressed. Readers are advised to confirm the up-to-date position and to take appropriate professional advice specific to their individual circumstances.