General Data Protection Regulation (GDPR) update Group Messaging Platforms (WhatsApp/Messenger/etc).

Information for Branch Officers and Area Representatives.

Use of messaging apps for union activities

Some Branches and Area Representatives are using platforms such as WhatsApp or Messenger to set up group messaging for the purpose of providing information and communications relating to union activities. These digital platforms provide an easy and accessible mechanism for personal communication and leisure purposes however, when used for union activities they are subject to GDPR legislation. It should be noted that WhatsApp and Messenger are not secure private communications platforms. The business model used by these platforms is based on the provision of free software in return for access to personal data for processing and commercial gain. The union does not promote the use of either platform although it is acknowledged these platforms are in common use. If using these platforms, the union advises only to circulate general union information. Sensitive personal data regarding union members and cases should not be communicated via these platforms. When using these platforms it is important to set the privacy and security to the highest levels and check for regular software updates. The Data Protection Commissioner's office has issued several notices and reports regarding such platforms see for example https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-statement-proposed-integration-facebook

Guidelines Branch Officer and Area Representatives

The following guidelines should be followed where a Branch Officer or Area Representative decide to use a messaging platform for union activities.

GDPR obligations comprehend all union related activities where the personal data of members is processed. Personal data includes name, mobile number, email address, image, voice, biometrics (any information which identifies an individual). When a member's personal data is used for the purpose of union activities by means of creating groups on platforms such as WhatsApp or Messenger (and other similar platforms) then the following GDPR guide applies.

The group convener has responsibility to:

- State the specific purpose of group (this could include sending out notice of union meetings, providing general information for branch or area representative, topic discussion etc.)
- Obtain consent from members who will be participating in the group (noting any individual has the right to remove their consent at any time and for whatever reason).

- Secure the personal data and do not share it with others (devices and accounts should be encrypted and password protected, the list of members names and numbers should not be circulated outside of the group however, they shall be provided upon request to the TUI Data Controller)
- Accurate record of contact details must be maintained (where a member leaves the group or changes union status or gets a new number the original number must be deleted from the group)
- Provide access to personal data stored relating to an individual upon receipt of a subject access request from the individual (the convener must provide the personal data requested within 29 days of the access request, note that stored personal data cannot be deleted after a request is submitted).
- Report any data breach to the Data Protection Officer as soon as possible, a risk assessment will be carried out and advice provided, there is a 72 hour deadline to complete this work starting from the time the convener became aware of the breach (data breach includes, loss of personal data, unauthorised access to personal data, third party access to personal data, sharing of personal data without consent etc.).
- Delete communications once the specific purpose of the communication is served (these platforms should not be used as storage facilities, used information should be erased on a regular basis).

Complaints can be lodged by an individual to the Data Protection Commissioner relating to the failure to provide personal data, failure to meet the timelines relating to access requests, unauthorised use or disclosure of personal data or failure to report a data breach. The Data Protection Commissioner can impose the fines to apply in successful complaints.

Both the group convener and group participants should be aware that communications relating to union activities should be respectful and professional. The union does not support nor will it accept liability for a member circulating illegal, abusive, or defamatory material on these platforms.

Things to do when setting up a messaging group	
Have a named convener	✓
Have a stated purpose	✓
Get consent	✓
Secure data	✓
Respond to subject access request	✓
Report data breach	✓
Update personal data	✓
Do not disclose personal data	✓
Allow respectful profession communication	✓
Delete used information	✓
Disband group when purpose is complete	✓

Things that you should not do in a messaging group	
Share others personal data	✗
Share illegal, abusive content	✗
Make defamatory statements	✗
Think the messages are private	✗
Store data for excessive periods	✗
Use unencrypted devise	✗
Access software without a password	✗
Send sensitive personal data	✗
Send private and confidential information	✗

Teachers' Union of Ireland.
73 Orwell Road, Rathgar, Dublin 6, D06 YP89, Ireland.
Email: dpo@tui.ie

Version 1, updated 30/9/2020