GDPR guide for TUI; Area Representatives, Branch Officers and Workplace Reps

The General Data Protection Regulation (2018) requires organisations who process personal data to have appropriate measures in place regarding the seven key principles; gathering, use, access, storage, requests, accuracy and retention of such data. This short guide provides Branch Officers and Workplace Representatives with practical information regarding the processing of data for individual cases and a mechanism for secure shredding of data.

GDPR Guide Regarding Individual Case Data Processing and Deletion

PROCESSING DATA FOR INDIVIDUAL CASES	
Seven Principles	**Guide**
Gathering data	Personal data should only be gathered for a specific purpose relating to the activities and services provided by the union. In all circumstances, informed consent should be obtained from the member before accepting personal data for a case file.
Use of data	Personal data in a case file should only be used for the purpose it is provided and in pursuit of the agreed case objective, in accordance with union rule, policy and procedure.
Access to data	Access to personal data (case files) should be limited to a need-to-know basis and made available to the Area Rep., Branch Officer/Workplace Representatives who have been assigned to provide advice and representation.
Storage of data	All personal data (paper or electronic) should be stored in a secure place which is protected by lock and key, or password. ICT equipment (tablets, phones etc.) should be encrypted. Documents should be password protected.
Accuracy of data	Stored personal data case files should be reviewed for accuracy on a regular basis and updated where necessary.
Request for data	Personal data must be provided to a person within 30 days of receipt of a verified data access request. The identities of other persons should be protected by means of redaction.
Retention of data	Personal data should only be retained for a specific purpose relating to the work of the union or the services provided. On completion of a personal case the personal data should be returned to the member or securely deleted if they do not want it returned. The outcome of the case should be retained.

Secure confidential shredding
To assist areas and branches with the secure deletion of personal data (paper-based case files) Confidential Shredding Bags are available from Head Office. These bags can be circulated to current and previous Branch Officers for the secure disposal of paper records. Once the material is placed in the bag it should be sealed and returned to Head Office for shredding.

Further practical information regarding GDPR will be circulated to branches on a regular basis. If you become aware of a data breach, please immediately send the details to dpo@tui.ie.

GDPR Guide for Areas, Branches and Workplaces

The General Data Protection Regulation (GDPR) came into force on the 25th May 2018 in Europe and effects Irish legislation. GDPR provides a range of protections for an individual relating to their personal data. Personal data means all information stored in a system relating to a living individual, for example:

- Written/Text documents containing an individual's identity; name, address, email, phone number, membership number, employment number, social security number, bank account number, examination number, medical records.
- Visual formats, containing an individual's image; photographs, videos, CCTV footage, social media (Facebook, Snapchat, WhatsApp, Instagram etc.).
- Audio formats, containing an individual's voice; recording of phone call, recording of conversation, recording of interview.

The above list is only a guide only should not be taken as a comprehensive range of forms and formats of personal data.

GDPR strengthens an individual's right to; access their personal data stored, privacy of their personal data, protection against unauthorised use (including misuse) of their personal data, requires data processors to gain informed consent from the individual before using their personal data and have secure measures in place regarding; usage, storage, retention and deletion. In addition, GDPR contains significant financial sanctions that can be enforced in circumstance of non-compliance or breach of the regulation. The implementation of GDPR will increase confidence in the regulatory requirements and procedures needed to protect and secure individual personal data.

The Teachers' Union of Ireland (TUI) as a data processor, is obligated to fully comply with the terms of GDPR. This obligation applies to the whole organisation; structures, roles, functions and operations. The following short GDPR guide is provided to Area Reps, Branch Officers and Workplace Representatives for implementation when carrying out activities for the union.

Security of members' personal data

- All members' personal data (including case files) must be stored in a safe and secure place.
- Members' personal data should not be left unattended in areas where other members or individuals can have access to it e.g. home, car, meeting room.
- Personal data should not be visible in the workplace e.g. notice boards, desks, computer screen, printers and copiers.
- All devices which hold members' personal data should be encrypted or must be password protected at a minimum.
- Be aware that handwritten notes and correspondence may be subject to data access requests.

Email

- Always use the TUI email account for union business, this assures confidentiality and privacy.
- Remember the email account provided by an employer is their property and can be subject to both data access requests and Freedom of Information requests.
- When emailing notices to members always use the bcc option, members' email addresses should not be displayed.
- Request members to supply their personal private email address for union communication purposes.
- Lists of members email addresses should not be supplied to the employer or any other third party.
- Members' email list should only be used for TUI activities
- Do not send emails to members which contain information unrelated to TUI activities unless the member has given consent in advance.
- Do not circulate TUI information to non-members.
- Email attachments containing personal data should be password protected.
- Be cautious about opening email attachments or links from unknown sources, if in doubt delete.

Membership Listings

- Membership listings must be kept safe and secure and destroyed as soon as the list is used for the purpose it was requested.
- Membership listings or members' details should never be given to the employer or a third party.
- Access to local membership listings is granted to branch officers for union activities only.
- Hard copies of membership lists should never be left unattended in a workplace for others to see.

Retention of Personal Data

- When a personal case is complete, the outcome may be stored in a safe and secure place. All other personal data must be returned to the individual and deleted from the area reps, branch and workplace records.
- When a Branch Officer or Workplace Rep, leaves their union position all personal data relating to TUI activities must be returned to the branch and deleted from their personal devices.
- Area Reps, Branches and Workplaces can have their personal data files (paper based) securely shredded by the union, insert documents into the TUI Confidential Shredding Bags and return them to Head Office.

Data Breach

- A data breach is, "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed". If a Branch Officer is made aware of a potential data breach they must report the matter to the TUI Data Protection Officer as soon as possible. Thereafter the union (including the Branch) has 72 hours to;
  - Assess the nature and scope of the breach,
  - put measures in place to stop the breach,
  - provide notice of the breach to those affected and
  - report the matter to the Data Protection Commissioner.
- Failure to report and deal with a data breach can result in significant financial sanctions.

Access Requests

- Be aware, individuals have the right to request access to personal data relating to them stored by the union (including data stored by; Area Representatives, Branch Officers and Workplace Reps) subject to certain provisions.
- Data access requests must be responded to within 30 days from the date of the request.
- The procedure for processing a data access request is:
  - acknowledge receipt of the data access request and detail the 30-day timeframe,
  - circulate the access request to those that may have the personal data,
  - collate the data, redact all sections and other individual's names that are not related to the data access requester.
  - produce a log of the data to be supplied and using registered post send the hardcopy of the data to the requester's postal address.
- **Note:** documents which are clearly labelled private and confidential or were provided to the union in confidence or as legal advice may be withheld from an access request. However, the requester must be informed that the document exists and the reason for not providing it.

Use of Equipment

- The union supplied encrypted laptops to branch officers and area representatives to carry out union activities.
- The union resources area representatives to obtain smart phones for union activities.
- When union equipment is being decommissioned all personal data must be deleted and the hard drive wiped clear with deletion software.

Social Media

- The union supports branches use of social media to promote union activities and campaigns. However, members' personal data and privacy must be respected. The following is advised:
  - Do not publish a member's personal data (names etc.) unless the branch has received explicit consent from the member.
  - Seek the member's consent before taking pictures or video clips for use on social media.
  - Do not publish a list of membership on any form of social media.
  - If using an online petition, make sure a data protection statement is included and give the user the right to have their name displayed or hidden.
  - Do not circulate; pictures, videos or text that may cause offence, hurt or defame another person.
  - Be aware that a member has a right to have their details deleted from any social media forums which are administered by an; area rep, branch or workplace.
  - Note all social media forums used for TUI activities by an area rep, branch and/or workplace are subject to data access requests.
- Further information and updates on GDPR will be circulated to Branch Officers and Workplace Representatives on a regular basis. If you have a query on GDPR or want to report a data protection breach, please email the TUI Data Protection Officer at dpo@tui.ie

Teachers' Union of Ireland.

73 Orwell Road, Rathgar, Dublin 6, D06 YP89, Ireland.

Email: dpo@tui.ie

Version 1, updated 10/4/2020