



COMMUNICATION WORKERS UNION

GDPR Policy and Guidance for Branches

Contents

	Page
Introduction	1
Section 1 Principles	3
Section 2 What information does the GDPR apply to?	4
- Personal Data	4
- Sensitive Personal Data	4
- Processing Personal Data	5
- Security	6
- Email	6
- BCC or CC	7
- Opting Out	7
- Laptops and other devices	7
- Hardcopy files and records	7
- Working from home and working on public transport or other public areas	8
- Personal Case Work	8
- Contacting Members	8
- Organising and Recruitment	9
Section 3 Subject Access Request (SARS)	10
Section 4 Data Breach	11
Appendix LTB 227/18	12

Introduction

Dear Colleague,

GDPR POLICY AND GUIDANCE FOR CWU BRANCHES

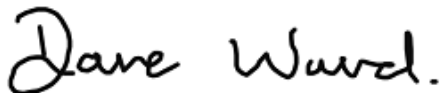
This policy is published on the CWU website and is also available on request from the CWU's Data Protection Officer.

We may change our privacy policies from time to time in order to reflect changes to our practices or for other operational, legal or regulatory reasons.

We will also keep such policies under regular review to consider any improvements.

When we do, we will give you notice of any material changes by posting the revised privacy policy on our website and by other means.

Denis Lenihan
CWU Data Protection Officer
Communication Workers Union
150 The Broadway
Wimbledon
SW19 1RX
020 8971 7279
dlenihan@cwu.org



Dave Ward
General Secretary



Tony Kearns
Senior Deputy General Secretary

Introduction

The government has confirmed that the General Data Protection Regulation (GDPR), which will harmonise data protection procedures across the EU from 25 May 2018, will have direct effect in the UK on that date.

The CWU is obliged to abide by the GDPR, and this includes all CWU Branches.

The GDPR will supersede the 1988 Data Protection Act.

The key changes will be:

- Wider definitions of personal data
- Enhanced rights for individuals
- More stringent requirements for consent
- Stricter requirements for reporting breaches.

In relation to personal information processing, it also requires:

- Increased fairness
- Increased accuracy
- Increased transparency
- Increased security.

1 Principles

Under GDPR, the data protection principles set out the main responsibilities for organisations when collecting and storing data.

Article 5 of the GDPR requires that personal data shall be:

- a) Processed lawfully, fairly and in a transparent manner in relation to individuals;
- b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- d) Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- e) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
- f) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Article 5(2) requires that:

The controller shall be responsible for, and be able to demonstrate, compliance with the principles.

2 What information does the GDPR apply to?

Personal Data

The GDPR applies to ‘personal data’ meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

This definition provides for a wide range of personal identifiers to constitute personal data. These include: name, identification number, and location data, and reflects changes in technology and the way organisations collect information.

The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

Personal data that has been pseudonymised – e.g. key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

So unless anonymised, personal data can be anything that identifies an individual, including:

- Name
- Address
- Date of Birth
- Email
- Telephone
- Photograph
- Membership Number

[The above listed criteria is not exclusive]

Sensitive Personal Data

The GDPR refers to sensitive personal data as “special categories of personal data”, and these would include:

- Race
- Sex
- Political
- Religion
- Trade Union membership

[The above listed criteria is not exclusive]

2 What information does the GDPR apply to?

Processing Personal Data

'Processing' refers to the collection, storage or any other use of information about individuals or groups of individuals.

In the case of a trade union, this will mainly apply to membership data.

CWU membership records are stored at CWU Headquarters and that is the central point for the processing of such information.

Members' personal data should not be stored in other locations (e.g. a Branch Office). This includes Membership lists, email contact details and paper records.

This does not mean that Branches cannot use Members' personal data. However, it necessitates that they do this via the CWU Membership Department.

For example, if a Branch wishes to carry out an organising activity in relation to the Branch members. The Branch (i.e. the Branch Secretary and Designated OLS Users) will have online access to their records and can produce their own CSV files as and when needed. This ensures they are working to current membership records and will avoid ex-members being messaged.

Branches will have personal data in other contexts also, personal case files for example. Whether it is in situations as in the above example, or any other where there is personal data being used, we all need to be extremely careful about how we handle said data.

After all, we all value our privacy and none of us would be happy to find out our data had been misused. Furthermore, the risk to CWU, both reputationally and financially, is very significant.

Much of the good practice in relation to protecting personal data is common sense and there are a number of practical steps we can take to minimise any risk, i.e.:

- All personal data must be kept secure at all times and must not be provided to any third parties whatsoever.
- If there is no good reason to retain personal data it should be disposed of in a safe and secure manner.

The maximum period to retain records such as case-files is six years. This refers to six from the time the member left the union or six years from the relevant issue (a personal case for example) being resolved. The six year period is standard time period in case of litigation or similar.

2 What information does the GDPR apply to?

Security

We need to have secure systems in place both in terms of technical and organisational measures to help ensure that personal data is not processed unlawfully (e.g., by disclosing it to someone who is not authorised to receive it), lost, destroyed or damaged.

What is appropriate depends on the type of information held, how sensitive it is and what damage could result in its improper use.

The Information Commissioner has produced some useful guidance on security.

For organisations / Guide to data protection / IT security top tips:

<https://ico.org.uk/for-organisations/guide-to-data-protection/it-security-top-tips/>

And further reading:

- **A practical guide to IT security**
- **Protecting data in online services: learning from the mistakes of others**

<https://ico.org.uk/for-organisations/guide-to-data-protection/it-security-top-tips/>

Email

Are the Branch and Representatives using the employer's email system? Or is it part of the CWU email system? Or using Hotmail or Yahoo? None of these are wrong per se, but do be aware of how secure the system is, who has access and so forth. It is worth considering the following:

- Employers may have the right to access email accounts at their discretion, possibly without having to inform the user. This, of course, will depend on the policies and procedure in operation at the place of work.
- If operating under a Branch domain and using an email system from it consider who has access to those accounts and where is it being hosted? Is it being hosted by a reputable company? What security is in place and is it updated regularly?
- There have been high profile cases of Yahoo, Hotmail etc. being accessed illegally. The CWU wants to inspire confidence in our Members that the best care is being taken of their data.
- Any sensitive data should be password protected whichever platform is being used.

Put simply: the general rule of thumb should be to treat the data as if it were your own. Always password protect sensitive data when emailing it.

The CWU IT Department will be able to advise on possible security measures.

2 What information does the GDPR apply to?

BCC or CC

When you send emails to members (or non-members) remember that you must not disclose someone's union membership to anyone else, so always use the BCC option in an email to list recipients' email addresses and send it to yourself, thereby allowing recipients to only see your email address.

Opting Out

If a member contacts you and asks that they be excluded from receiving further communication from the CWU (either locally or from HQ) they must be allowed to do so but ***do let the CWU Data Protection Officer know.***

Laptops and other devices

If a Branch or Representative's laptop or other device was lost or stolen, would the information on it be safe? The use of encryption/passwords will go some way to making them safer. Better still would be ensuring that the device can be disabled remotely.

You can also encrypt individual documents. You should do this with documents containing special data such as union membership.

Also lock any laptops or other devices away when they are not in use and remember to regularly update software and anti-virus software to maintain security.

Again the CWU IT Department will be able to advise you on this.

Hard-copy files and records

We need to ensure that all paper records are locked away in a filing cabinet or other secure location, when not in use, and especially overnight, as a safety precaution.

- Think about who has access to any paper records or could gain access – and if they do have access, should they? Do they need to have access and if so could we explain why?
- Remember to regularly identify outdated records and dispose of them in a secure manner such as shredding.

2 What information does the GDPR apply to?

Working from home and working on public transport or other public areas

When working at home we still need to consider security. For example, shared accommodation, service or maintenance workers and burglary can all pose potential risks.

We also need to be very careful when working away from our usual workplace. Documents and electronic devices can be easily lost or stolen in such circumstances.

Again, locking your computer and the use of passwords/encryption will help.

We should also consider the confidentiality of members' issues. For example when discussing a personal case on a train, there is the risk of being overheard or even recorded.

Personal Case Work

There may be particular issues over security because of the portable nature of case files so you may need special care that files are kept safe when they are not in the office. They should be returned to safe keeping in the office immediately once the case is completed.

The identity of the member should only be shared with those who need to know and any generalised discussion (verbally or by email for example) of the case should be anonymised.

Contacting Members

While it is legitimate for trade unions (and therefore Branches) to retain information about our members (including contact details) CWU Policy is that Branches, Representatives, Officers etc. should not be maintaining their own membership contacts lists. This is because under the GDPR there are much more stringent regulations about security, accuracy, transparency, etc. (e.g. what we wish to avoid might be where a Branch uses an out-of-date contacts list to email people who are no longer CWU members, who could then complain to the Information Commissioners Office because we have kept their details!)

We ask that Branches (and Officers, Representatives, etc) not to keep membership lists, but rather, to work from the central membership database at CWU Headquarters.

Going forward, it will be possible for all CWU Members to use the 'My Union' facility on the website to decide what communications they receive. It is also a requirement of the GDPR that individuals have control over the information they receive and by using this system, it means the CWU will be a long way along to being GDPR compliant.

Please see LTB 227/18 which is attached as an appendix to this document.

2 What information does the GDPR apply to?

Organising and Recruitment

You will need to be mindful of the GDPR when carrying organising and recruitment activities in the Branch.

You may want to collect information such as lists of employees attending a meeting so that you can identify non-members and contact them with a view to becoming a member. You may also wish to identify members who are interested in becoming more active in the union and note anyone who has expressed an interest in taking on certain types of union activities. In doing any of these, you will be creating a filing system of personal data.

For the employees who are already CWU members we will process their information to carry out our legitimate trade union activities - on the strict conditions that there are appropriate safeguards in place and the data will not be disclosed outside the CWU without the individuals' consent.

It is a little less clear for non-members. Ideally we would obtain consent to record their personal data for organising purposes at a meeting by providing a form for the individuals to sign. You should specify on the form what information you are asking for, and why, and what you intend to do with it. When compiling a list of potential members though, it will not always be possible to obtain everyone's consent in advance. However it is likely this sort of processing will be permissible on the basis that it is part of the union's legitimate activities. Once you have the list though, you should give individuals the opportunity of taking their name off it.

You must only collect as much information as you need for your purposes, and you must keep it up to date. You must also keep it securely, and for no longer than is necessary for those purposes, after which time you must destroy it securely.

3 Subject Access Request (SARS)

Be aware that individuals for whom we retain information now have enhanced rights to access their information. It is important that information is accurate, objective and up to date, relevant for the purpose we have kept it.

The 'subject' in our case would most likely to be a CWU member (or ex-member).

The information we are compelled to provide might include:

- The reasons why their data is being processed;
- The description of the personal data concerning them;
- Anyone who has received or will receive their personal data.

Of course the best way to avoid any problems related to this, is to not hold personal information at all unless strictly necessary.

It is very important that if you are made aware of a member (or ex-member or other individuals) who has asked to see the information the CWU holds about them, that you immediately let the Data Protection Officer know. This is because under the GDPR, we must respond to SARs within one month of receipt so we will need to begin the process of assembling the relevant information immediately. [Contact details below].

Denis Lenihan
CWU Data Protection Officer
Communication Workers Union
150 The Broadway
Wimbledon
SW19 1RX
020 8971 7279
dlenihan@cwu.org

4 Data Breach

It is also vitally important that in the event of something going wrong with our handling of personal data (or 'breach' in the technical jargon) that you inform the CWU Data Protection Officer at CWU HQ immediately. [Contact details below].

This could mean the loss or theft of data – in an email, spreadsheet, paper file, etc. It also refers to records being accidentally or unlawfully destroyed, altered, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

We need to act to rectify or ameliorate the breach, as we and may have to report it to the Information Commissioners Office, and if so, we only have 72 hours to do it.

Denis Lenihan
CWU Data Protection Officer
Communication Workers Union
150 The Broadway
Wimbledon
SW19 1RX
020 8971 7279
dlenihan@cwu.org

Appendix

LTB No. 227/18

17th April 2018

Dear Colleague,

General Data Protection Regulations (GDPR)

The purpose of this LTB is to inform all Branches of changes we will be making on the issue of Data Protection. These arise from the need for us to comply with new regulations known as “General Data Protection Regulations” (GDPR) that will come into force on the 25th May 2018.

The new GDPR regulations mean that from the above date information on members is no longer owned by the CWU but is owned by the member. As such the regulations place greater emphasis on the documentation we must keep to demonstrate our compliance with these new requirements. As stated above individuals will now have total control of their personal data as it is their data not ours. The member, known as the data subject will have the right to obtain from the Data Controller (the CWU) confirmation as to where, how and for what purpose their personal data is being held and processed.

To ensure we are compliant we are currently in the process of drafting a number of notices that will cover privacy information, individual rights and data consent.

As the issue progresses we will continue to keep Branches informed of developments to any new strategy that we are required to implement to alleviate any potential fines that the Information Commissioner’s Office (ICO) could impose if we are in breach of GDPR. This point is made because it will only be in the light of working experience will any areas of dubiety be cleared up.

What is important for us to understand is that breaches of the new regulations can result in organisations being fined up to 4% of turnover. To put this in perspective, unless we take action to show we are compliant we risk a fine that could total up £1.1 million for breaches. Clearly our job is to mitigate against such risk and as such there will be number of actions we have to take.

The first of these and the purpose of this LTB is to ensure that the organisation has in place a secure system that contains only data we are entitled to hold, that a member knows where this data is held and is able to access and change their own personal data at any time.

This means we must work to one main database that being the database held by CWU Headquarters in our Membership Records Dept. It is essential that the only data held within Branches is that from the central Integra Online Service (OLS). It is only through such central control can we show the member and the Information Commissioners Office that we are protecting membership information, can inform members where their information is stored and allow them direct access to it. It is not possible to do this if such information is held across multiple platforms in different locations.

Appendix

As a result **any Branch who holds their own data should cease using and maintaining these files with immediate effect.** Failure to adhere to this instruction will place the union into conflict with legislation and risks punishment by way of a fine or fines in line with the parameters set out above.

We have already received a small number of queries on this matter from Branches wishing to ensure they don't do anything that falls foul of the new regulations. Our advice on this is fairly straightforward, as a rule of thumb, do not use any locally held databases for contacting members and contact CWU Headquarters (details below) if you are unsure about the content contained within any message to members.

These new regulations place restrictions on what issues we can communicate with our members on and we will write separately to Branches on this nearer to the 25th May 2018. We are committed to continued communication with our members both at Branch and National level but we have no choice under these regulations but to focus in the immediate future on maintaining data privacy and that is the reason for this particular LTB. We are also assessing a number of options available to us including the development of a Member Case Management Online Service for Branches to utilise.

We will need write to Branches separately to receive written confirmation that no other membership data is being held by them in order that, if necessary, we can show to the relevant authority, that we have acted to ensure compliance with these new regulations.

We also have in place a temporary Data Protection Officer at CWU Headquarters, Denis Lenihan who can be contacted for further information on dlenihan@cwu.org

Any enquiries regarding this Letter to Branches should be addressed to the Senior Deputy General Secretary's Department on telephone number 020 8971 7237, or email address sdgs@cwu.org.

Yours sincerely,



Tony Kearns
Senior Deputy General Secretary