UNISON branch data protection handbook

Updated February 2018 for GDPR

Welcome to the UNISON Branch Data Protection Handbook

Data protection law in the UK and Europe is being strengthened. This makes it even more important, for UNISON and our members, that privacy is integrated into our day to day work. The increasing profile of the importance of protecting personal data means that the public at large, and so also our current and potential members, are more conscious of it. We cannot afford data protection to be an afterthought.

With this in mind, this handbook has been designed to give branches an appreciation of the legal requirements that UNISON must abide by to ensure that they comply with all UK and European Data Protection Regulations.

The appendices in this handbook contain further detailed information and example documentation which branches may find useful.

The content of this handbook is correct at the time that it was issued and will be updated from time to time as privacy legislation changes.

Contents

Introduction to Data Protection

Data Protection Regulation

There are several Data Protection laws that UNISON must comply with. At time of writing these are:

- Data Protection Act 1998 (DPA)
- General Data Protection Regulation 2016 (GDPR)
- Privacy and Electronic Communication Regulations 2003 (PECR)

This guide aims to take the key points from each law and put them into a UNISON context.

For clarity, in the following document, the terms “Data Protection” and “Data Protection Regulation” will be used. These terms should be taken to include all of the above regulation that is applicable.

Data Protection Basics

All organisations in the UK must comply with Data Protection Regulations.

Data protection is enforced in the UK by the Information Commissioner’s Office (ICO). The ICO has a number of powers, including the ability to fine organisations up to EUR 20,000,000 or 4% of annual turnover per data protection breach and the ability to publicise information about data protection breaches.

Data protection applies to the “processing” of “personal data” by “data controllers” and “data processors” about “data subjects”.

“Personal data” is any information about a living individual which enables them to be identified. If data is “obviously about” a person, then it is personal data. Examples of personal data potentially processed in UNISON branches are:

- Membership number
- Date of birth
- National insurance number
- Bank details
- Email address
- Home address
- Photographs
- Case files
- IP address

Records of opinions about an individual, or intentions towards them, are also classed as personal data.

Personal data can be held in any form. This could be on electronic media (such as USB sticks, CDs, computer drives and cloud computing) or hard copy files.

The majority of data UNISON branches hold on members is personal data.

Introduction to Data Protection

"Processing" includes:

- Obtaining and retrieving information.
- Holding and storing information, including in WARMS.
- Making information available to others, within or outside an organisation.
- Printing, sorting, matching, comparing, altering and destroying information.

Everything UNISON branches do with personal data is considered to be "processing".

A **"Data Controller"** determines how personal data will be used.

UNISON is the data controller for all personal data that branches have with one exception: branches are data controller for the employment records that they have about individuals they employ directly.

A **"Data Processor"** is a body which processes information on behalf of a data controller.

Mailing houses are data processors.

"Data subjects" are the individuals whose personal data we hold. They include:

- Members
- Lapsed members
- Prospective members
- Employees
- Previous employees
- Prospective employees
- Agency staff
- Contractors
- Suppliers

All of the membership related work which is carried out in UNISON's branches must be done in line with Data Protection Regulations.

Data Protection is about striking a balance between the rights of individuals to know about and control what's happening to their personal data and the sometimes competing interests of those with legitimate reasons for using their personal data.

The Six Principles of Data Protection

Data Protection Regulation focuses on six principles which stipulate that:

1. Personal data shall be processed fairly and lawfully and in a transparent manner.

2. Personal data shall be collected for a specific, explicit and legitimate purpose and not further processed in a manner that is incompatible with that purpose.

3. Personal data shall be adequate, relevant and not excessive for the purpose of the processing.

4. Personal data shall be accurate and where necessary, kept up to date.

5. Personal data shall not be kept for longer than is necessary for the purposes of the data processing.

6. Personal data shall be processed in a manner that ensures appropriate security of the personal data.

Principles of Data Protection

1. Personal data must be processed fairly and lawfully and in a transparent manner

There are six "fair processing" conditions for using individuals' personal data, and UNISON needs to comply with at least one of them to ensure that data is being fairly and lawfully processed. The key conditions which UNISON relies on are:

- The individual has given their consent for their personal data to be used by the organisation.
- The processing is necessary to pursue UNISON's legitimate interests as a trade union (in a way that will not cause unwarranted damage or distress to the individual).

To ensure transparency, UNISON must communicate to members how we will process their personal data. This involves:

- Publishing a privacy notice that explains how UNISON processes personal data. This is on the UNISON website: www.unison.org.uk/privacy-policy.
- Explaining to members of your branch what you will use their personal data for whenever you collect it. This could be explaining that you need to update their address details to send them a ballot paper, or explaining that the information they provide on a case form will be used to represent them.

The Six Principles of Data Protection

"Special categories" of personal data and further conditions for processing

Some personal data is classed as "special category" or "sensitive" under Data Protection Regulation. This data includes information relating to an individual's:

- Racial or ethnic origin
- Political opinions
- Religious beliefs
- Trade union membership
- Physical or mental health
- Sexual orientation

To be able to use special category personal data there are further conditions (additional to those highlighted above) which UNISON must meet. The most common are:

- The person involved has given explicit consent for the data to be used.
- Data is processed in the course of UNISON's legitimate activities, with appropriate safeguards, for trade union aims.
- The data is used to obtain legal advice or defend legal rights.
- Data on race, religion or health is used for equalities purposes.

The misuse of special category data, including information about trade union membership, can cause damage and distress for the individuals concerned. Extra care must therefore be taken when handling these categories of data.

2. Personal data shall be collected for a specific, explicit and legitimate purpose and not further processed in a manner that is incompatible with that purpose.

To legally process personal data, UNISON must be listed on the publicly available register which is maintained by the ICO. The process of registering is known as "notification".

Under Data Protection Regulation, branches are covered by UNISON's registration and so **do not need to notify separately**.

The only time when branches are considered to be a data controller is when they employ staff directly. Organisations do not need to notify if that is the only purpose for which they process the personal data as a data controller. If your branch notifies, please contact dataprotection@unison.co.uk before renewing – you may not need to do so.

Notifications identify several "purposes" for processing data, and these are the only activities that UNISON is legally allowed to collect and use data for. UNISON's registered purposes include:

- Processing membership data
- Processing potential membership data
- Processing staff data

The Six Principles of Data Protection

3. Personal data shall be adequate, relevant and not excessive for the purpose of the processing

This principle is about making sure that UNISON does not collect more information than we need to. For example, our application form used to ask potential members to state whether they were a Mason. The ICO ruled that this information was "not relevant" and instructed us to remove it from the form.

Never ask a member for information that UNISON does not need.

4. Personal data shall be accurate and where necessary, kept up to date

This principle requires UNISON to keep personal data up to date and accurate.

The key to accuracy is the use of one single membership system (WARMS/RMS) throughout all of UNISON. This is because membership data updates can be done from different parts of UNISON, for example:

- Member updates their own details via My UNISON.
- Member updates their details over the phone at UNISON Direct.
- Postal mailings to the member are returned to UNISON Centre.
- Member record is changed in a bulk update done by region, for example a group of members changing employer as a result of a TUPE transfer.

We therefore all need to use the same membership system.

Your branch should not keep membership data on any system other than WARMS.

5. Personal data shall not be kept for longer than is necessary for the purposes of the data processing

Data Protection Regulation stipulates that personal data should not be kept longer than is necessary for the purpose it was collected. The ICO expects organisations like UNISON to have a data retention schedule which identifies the different types of information in use and how long that information should be kept.

Data Protection Regulation does not set specific times for which data should be kept; organisations are expected to consider their own retention needs. However, there are some legal retention periods e.g. case files should be kept for at least 6 years. Other documents like membership forms only need to be kept for a year after all the relevant data has been entered onto WARMS.

An excerpt of UNISON's retention schedule is in Appendix 5 of this handbook.

6. Personal data shall be processed in a manner that ensures appropriate security of the personal data

Data Protection requires organisations to keep personal data (whether it be in hard copy or electronic form) secure against accidental loss, damage or destruction.

For **electronic data** e.g. that held on computers, cloud computing or removable media, (USB pens, CDs, etc) the ICO would expect to see:

- Password protection
- Encryption
- Virus protection
- Use of firewalls
- Data backup processes

For **hard copy data** examples of good data security practices are:

- Door security and restricted access to branch offices
- Lockable filing cabinets
- Secure storage areas
- Clear desk policies

Secure use of email

Some branches use their employer's email system, whereas some use email providers such as Hotmail and Gmail. Whatever email system you use, ensure it is as secure as possible by doing the following:

- Have a strong password.
- Lock your screen when away from your desk (Shortcut - Windows key +L).
- Always sign out of your email account when finished if you are using a shared device.
- Ensure that no one else has access to your emails. Never use a family or shared email account for UNISON business.
- If emailing more than one person, use the Bcc field rather than the To or Cc field (NB using WARMS bulk email does this automatically).

Secure archiving

Some branches use an offsite archive for the storage of old files. If your branch does this, you must make sure that the archive is sufficiently secure. You are still responsible for the security of any archived files. For advice on how to check your archive is secure, please contact dataprotection@unison.co.uk.

Rights of the Data Subject

Individuals have several rights under Data Protection Regulation. The following are most relevant to UNISON branches:

1. Right of access

Individuals have the right to be provided with a copy of their own personal data held by UNISON. These requests are called subject access requests (SARs). They cover information held in paper form and electronically.

Never write down anything about an individual that you would not want them to see.

UNISON can apply exemptions to withhold certain data. For example, legally privileged information between UNISON and its legal advisors does not need to be disclosed. Exemptions are applied on a case by case basis.

If an individual makes a subject access request, please contact dataprotection@unison.co.uk immediately. We must reply within one month, so time is of the essence!

2. Right to restrict processing

Anyone can request that a data controller, such as UNISON, stops processing their personal data. In practice, we may just stop doing whatever the person is specifically objecting to (e.g. sending mailings).

If a member asks UNISON to stop processing their personal data completely, that person would no longer be able to be a member, and if a potential member requests this, then they could not go on to become a member of UNISON.

If a member asks you to stop processing their personal data, please contact dataprotection@unison.co.uk immediately.

3. Right to erasure

An individual has the right to ask UNISON to delete their data, if there is no compelling reason for us to keep it. There are circumstances in which we can refuse to delete data (e.g. an ongoing legal case), but if possible the request should be complied with.

If a member asks you for their personal data to be deleted or destroyed, please contact dataprotection@unison.co.uk immediately. Do not start deleting anything until you have heard back from us.

4. Right to rectification

An individual can ask UNISON to rectify their data if it is inaccurate or incomplete.

If a member asks you to do this, you can update their details on WARMS or advise them to update their own details online via My UNISON.

Rights of the Data Subject

5. Right to data portability

Data Protection Regulation allows individuals to obtain and reuse their personal data for their own purposes across different services. For UNISON this is likely to take the form of a request for an individual's details to be passed to another union that they wish to join.

If a member asks you for this data, please contact dataprotection@unison.co.uk immediately.

6. Right to object to processing

a) Right to opt out of direct marketing

These requests must be acted upon immediately and no further direct marketing material sent to the individual. The ICO defines "direct marketing" broadly – it includes the promotion of an organisation's aims, values and policies. This presents some challenges when we want to contact members with regard to campaigning issues.

If a member asks to stop receiving marketing, you should update their communication preferences on WARMS.

b) Right to object to other types of processing

An individual can object to any processing where UNISON's lawful basis is legitimate interest (this covers most of our processing). If a member does this, please contact dataprotection@unison.co.uk immediately.

7. The right to complain to the regulator (the ICO)

If someone believes their personal data has not been processed in accordance with the Data Protection Regulation, they can ask the ICO to make an assessment.

If Data Protection Regulation is found to have been breached and the matter cannot be settled informally, the ICO could take action against UNISON which could be a fine up to EUR 20,000,000 or 4% of annual turnover.

8. The right to compensation

An individual can claim compensation from a data controller for damage and distress caused by a breach of Data Protection Regulation. Compensation for damage (i.e. financial loss) is regularly awarded by the courts. Compensation for distress only is less common, but has been awarded in certain circumstances.

International Data Transfers

Transferring data outside of the European Union

Data Protection Regulation states that data is not allowed to be transferred outside of the European Union ("EU") unless that country is designated as having "an adequate level of protection", or other safeguards are in place.

The following countries are currently considered to have an appropriate level of protection:

Any country in the European Economic Area
Jersey
Guernsey
Isle of Man
Switzerland
Andorra
Faroe Islands
New Zealand
Canada
Uruguay
Argentina
Israel

International transfers are not normally an issue for UNISON, but increasingly website hosting and online services are located in non-EU countries. It is important that this is borne in mind when using online services. If you are using an online service to process membership data, ask the provider where the service is hosted (sometimes you are able to request hosting in the EU) and ensure that appropriate safeguards are in place.

If you need support with this, please email: dataprotection@unison.co.uk.

Privacy and Electronic Communications Regulations 2003 (PECR)

The Privacy and Electronic Communications Regulations 2003 ("PECR") are specifically about electronic direct marketing communications.

Examples of "electronic communications" are: email, direct messages on social media, text message, fax and automated telephone calls.

"Direct marketing" is defined very broadly and includes the promotion of an organisation's aims, values and policies. A large proportion of UNISON's electronic communications are therefore direct marketing, even though they are not trying to sell a product.

The key requirement of the PECR is that individuals contacted electronically must have given their prior consent for this communication, other than in very limited circumstances.

PECR does not consider that contacting people as a default unless they have opted out is satisfactory. They look for evidence that individuals have given their explicit consent before any communications take place. This can make contacting potential members and members tricky when it comes to information which is about educational and campaigning matters.

Opt-out consent is only acceptable when **all** of the following three criteria are met:

1. The contact details were obtained from the individual during a sale of a product or service. For UNISON this will usually be when a person is becoming a member, or we are contacting an existing member; and

2. The communication relates to similar products or services. For UNISON this will usually be a communication about a campaign; and

3. The option to opt out (or "unsubscribe") was provided when the data was collected and is included on each and every subsequent communication. For UNISON this means always ensuring there is an unsubscribe option on all electronic communications.

The conditions are very specific and so cannot be relied upon in many situations.

Difficulties can arise when using a member's mobile or home telephone number to send campaigning messages if the number was not initially collected for the purpose of campaigning; instead, for example, during a case. It is therefore very important to know why the personal data that you have was collected in the first place.

> The PECR is due to be updated in the form of the ePrivacy regulation (ePR) in 2018. This handbook will be updated once full details of ePR become available.

Freedom of Information Act 2000

UNISON, although a trade union for public service workers, is not itself a public body. The Freedom of Information Act 2000 ("FOI Act") only applies to public bodies. Any FOI requests which come into the branch office should be forwarded to the regional office for review and response – the standard response is that the FOI Act does not apply to UNISON and therefore the information will not be provided.

Subject access requests (SARs) often incorrectly refer to the Freedom of Information Act. SARs must be responded to by UNISON within short deadlines or face large penalties. It is therefore important to recognise and respond to them quickly. Please see Appendix 3 – How to recognise a subject access request (SAR).

Although the FOI Act does not apply to UNISON, it does apply to the majority of our members' employers. Requestors do not always appreciate this and some organisations (such as the Tax Payers' Alliance) sometimes send identical FOI requests ("round robins") - often concerning facility time, DOCAS or similar subjects - to trade unions across the whole of the UK. Notwithstanding the fact that UNISON is not subject to the FOI Act, it is important that our responses to them are consistent across branches. To ensure this please forward any such requests to the regional office. They will respond appropriately.

Key Branch Activities and Data Protection

1. Recruiting and organising

1.1. Data processing in branch

All of the tasks below are data processing and must follow Data Protection Regulations:

- Receiving and inputting membership forms
- Amending or deleting membership details
- Running reports
- Sending bulk emails

When completing any of these activities:

- Do use WARMS for all of these tasks, as it is the easiest and most secure way.
- Do update member records as soon as possible.
- Do lock your computer screen when you are away from your desk.
- Do shred any membership information when it is no longer required.
- Do refer to WARMS e-learning and regional data protection contacts if in doubt.
- Don't let someone else use your WARMS login.
- Don't leave paper copies of membership details on your desk.

WARMS significantly reduces the risk of data protection breaches occurring and should be used whenever possible. It is a secure system, accessible only by authorised persons. It also records all changes made to membership data, maintaining the accuracy of the information.

1.2. Collecting potential member information

Potential members' personal data can be collected as long as the people are aware their data is being recorded and retained, and they must be allowed to opt out of this data collection exercise. It is imperative that the data collected about potential members is not excessive – avoid collecting more information than is needed – and that it is stored securely and not shared with anyone who has no need to see it.

A retention period should be set for this information and, once this time period has elapsed, the data should be disposed of securely i.e. deleted from a computer or shredded or placed in a confidential waste bin or bag if it is in paper form.

1.3. New starters

It is always a good idea to contact new starters and encourage them to join UNISON. Sometimes employers can use data protection as a barrier to passing this information on to unions. If possible, work with your employer to ensure that they make it clear - perhaps by adding into their induction materials – that, as long as the employees have been given the option to opt out, it is standard practice for new starters' names and contact details to be passed to trade union colleagues. Contact details that are obtained in this way have been collected within the confines of Data Protection Regulation.

1.4. Mapping and monitoring in the workplace

When collecting and recording mapping data, it is very likely that the information will include personal data i.e. the data could be used to identify individuals. As is highlighted in section 2 of this handbook, it is important to ensure that people are aware that their data is being collected, and that they are given the opportunity to opt out of their data being collected. If difficulties arise, and individuals decide to opt out of this exercise, the exercise should be carried out in a way to avoid collecting personal data by, for example, using anonymised data.

1.5. Data cleansing

This is a crucial branch activity, especially in the run up to a ballot. If a member requests that their personal details are updated, this should be done on WARMS as soon as possible.

It is important to ensure that in the process of collecting updated member data, this data is not inadvertently shared with others. This would breach Data Protection Regulation and could give cause for members to complain to the ICO. It is important to ensure that any method of data collection always maintains everyone's confidentiality. For example, do not openly circulate a spreadsheet which contains a line of information for each member; instead, send individual update sheets to individual members. Similarly, do not send out a blanket email to members without using the "blind carbon copy" (Bcc) field – some members wish to keep their membership confidential.

2. Storing data securely

2.1. Hard copies, file notes, incoming and outgoing letter correspondence

UNISON has a duty to ensure that data is held securely. Provisions the branch must consider putting in place include:

- Lockable filing cabinets
- Security keypad on the door of the branch office
- A file logging out and in procedure
- A clear desk policy
- Secure storage for archived files
- Secure destruction: using a shredder or confidential waste bin, for example.

2.2. Electronic data

The same requirement applies to electronically held data. Provisions the branch must consider putting in place include:

- A logging process for laptop removal from the branch office.
- Using storage on a network, rather than laptop or desktop computer, if possible
- Encryption of all removable media (USB pens, CDs etc). If your branch uses employer-provided computers it is likely that these will have some form of encryption installed. If your branch has bought its own computer equipment, it is highly recommended that some form of encryption is considered. A copy of the ICO's guide to encryption is available on their website: https://ico.org.uk/for-organisations/guide-to-data-protection/encryption/
- Password protection on all files containing member data.
- Use of WARMS for processing member data (encrypted and password protected).
- Up to date antivirus and malware systems.
- Adequate firewalls.
- Secure destruction.

It is important that when a computer is no longer required, that any data is removed in such a way that it is not recoverable. There are several organisations that will forensically clean a computer hard drive and provide a data destruction certificate to prove that it has been done.

2.3. Telephone and CCTV recordings

Telephone and CCTV monitoring and recording are not extensively used within UNISON, but if the branch is using these facilities, it is important to consider that these recordings contain personal data. It should be noted that the recordings would be subject to any request for

access by an individual, and should also be subject to a data retention policy and be deleted once the appropriate period has expired.

More information on CCTV and data protection is available on the ICO's website: https://ico.org.uk/for-organisations/guide-to-data-protection/cctv/.

3. Sharing information

Personal data can be shared with third parties but it has to be done with care.

3.1. Using an external print/processing house

When data is passed to third parties for processing, the ICO requires organisations to choose a third party which will provide sufficient security guarantees for both its use and storage. It doesn't matter whether the information is electronic or hard copy. Examples of third party processors are:

- Mailing houses
- Website hosting
- Payroll providers

It is essential that a formal agreement is in place with third party processing organisations. The agreement should ensure that there is a contractual obligation on the processor to:

- Implement specific security measures.
- Use the data only for the original purpose they received it.
- Have trained personnel.
- Disallow further subcontracting.
- Grant rights of access for audit and subject access purposes.
- Delete data within an agreed retention schedule or when a subject has requested UNISON delete their data.

A template Data Processor Agreement is in Appendix 2 of this handbook. A contract containing appropriate clauses is also sufficient.

3.2. Extracts from the membership system

Requests for extracts from the membership system should be treated with caution. Often you will receive requests from other, similar organisations for data which will enable them to contact our members directly and offer products or services or ask them to participate in a survey. These are what we call third parties.

Always refer these requests your region before responding. Each request needs to be carefully reviewed to determine whether to pass the data on to the third party.

If any data extracts have been taken, it is essential that the branch ensures that appropriate permissions and security are in place. The branch has to ensure that the information is:

- Passed to the receiver securely (for example using encryption, password protection or secure FTP which encrypts the file for you).
- Not circulated widely.
- Given only to those individuals who have a need to see the data.
- Only used for the specific purpose for which it was extracted.
- Held securely.

- Securely destroyed after use.

The importance of thinking before sending extracts from WARMS (or any other personal data to a third party) cannot be overstated. Consider what you are doing it for and check that doing it will not breach data protection law.

Below is a table of 'dos and don'ts' which you should bear in mind when extracting information from WARMS:

Do	Don't
Only extract the information that is needed to complete a task. This makes sure that the data is not excessive.	Extract more information than you need for a task. A lack of time is not a legitimate reason for not producing tailored reports.
Only use extracts for one task. A new list should be extracted for each task as the data may have changed.	Provide information to others not involved in the task for which the data was extracted.
Keep the information on systems and networks that are recognised as being acceptable for UNISON work. These may belong to an employer or to the union.	Email member data to a personal email address or save it onto a personal device for any reason. This includes lists of names, email addresses etc.
Take care when taking personal data out of the office. Only take the information if it is necessary, keep it safe and return it as soon as possible.	Keep the information that you have got to use for a very similar exercise that you know you're going to do in the future.
Update WARMS if a member's details are out of date.	Leave personal data that has been taken out of the office unattended.
Use WARMS for all membership data work.	Put information into a normal bin, use a secure disposal bin or bag instead. Someone else could find it and misuse it.
	Have a local member list or spreadsheet instead of using WARMS.

3.3. Releasing information to prevent or detect crime

The police or other crime prevention / law enforcement agencies (e.g. Benefit Fraud Office and Local Authority functions) sometimes contact data controllers or data processors and request that personal data is disclosed in order to help them prevent or detect a crime. UNISON does not have to comply with these requests, but Data Protection Regulation does allow organisations to release the information if they decide it is appropriate.

Before any decision is made about disclosure, the Information Commissioner asks that organisations carry out a review of the request. This includes considering:

- The impact on the privacy of the individual/s concerned.
- Any duty of confidentiality owed to the individual/s.
- Whether refusing disclosure would impact the requesting organisation's ability to detect, prevent or prosecute an offender.

If a decision is made to refuse, it is possible that a subsequent court order may be made by the requesting organisation for UNISON to release the information.

If such a request is received at a branch, please refer the requestor to UNISON's Data Protection Officer at the UNISON Centre on dataprotection@unison.co.uk .

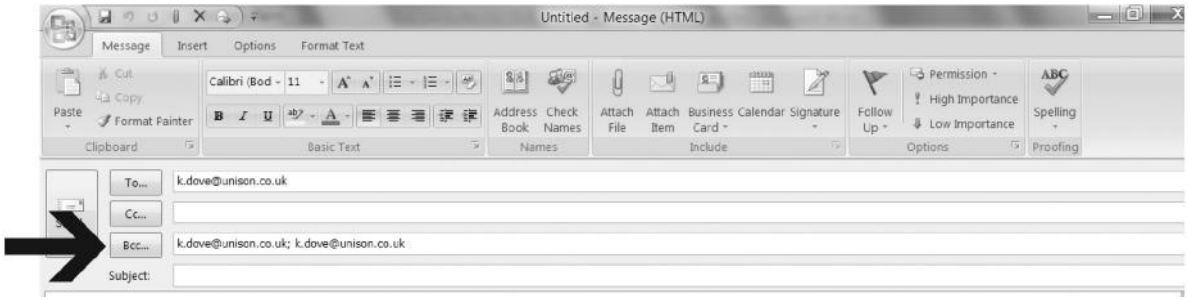
4. Communicating with members

As is explained in the PECR section this handbook, contacting members by email or text message requires opt-in consent.

4.1. Using email and text messaging

As well as the conditions relating to PECR, the ICO has stated that all email addresses are personal data, and as UNISON is a trade union, email addresses are sensitive personal data, requiring extra conditions to be met before the data can legally be used. It is therefore essential that when communicating with members using email and text distribution lists that the following provisions are made:

- Individuals who have opted out of mailings (apart from statutory information like ballots information) are not included in mailings or bulk text messages. WARMS bulk email will do this for you.
- The blind carbon copy (Bcc) field on the email address line – shown below – is used. WARMS bulk email will do this for you.
- An option to unsubscribe to similar communications is added to the bottom of the email or text message each time a message is sent out. WARMS bulk email will do this for you.



If a member informs the branch that they no longer wish to be contacted via email or text, their preferences should be updated on WARMS. They should also be removed from any distribution lists you have.

It is best to use WARMS to send bulk emails as the following security features are included within it:

- Lapsed members not emailed.
- Bulk emails are automatically sent using Bcc.
- Changes to member contact preferences are immediately reflected.
- An unsubscribe link / My UNISON link is automatically added.
- Communications are recorded to member's communications history.
- Avoids the need for membership extracts or lists.

4.2. Sending letters to members

Some members wish their trade union membership to be confidential and request that any union related mailings are sent to their home address, rather than their workplace address. The branch should ensure that these requests are complied with. Inadvertent disclosure of an individual's trade union membership would be a breach of Data Protection Regulation.

5. Representing members

5.1. Employment, welfare, and health & safety case files

Any information directly related to a potential or actual case is extremely sensitive and several of the Data Protection principles apply. Provisions that the branch need to make include:

- Secure storage for live and archived case files.
- Limited access to only those officials who need to see the data.
- Collection of data is limited to only that which is relevant to the case in hand.
- Information held in the file is accurate.
- A sign in/out process is in place, if the file needs to be taken out of the branch office.
- A file retention policy is in place.
- Secure disposal once the file is no longer needed.

It is much safer to keep any case files within the branch. If this is not possible, i.e. a file needs to be taken off the premises, considerable care should be taken to ensure that its whereabouts are known, and that it is always kept secure.

In order to preserve the legal privilege that exists between UNISON and its legal advisors - both our in-house legal team and external advice from Thompsons – for legal advice that is sought regarding a merits assessment for a particular case, the original documentation between UNISON and the legal advisors should not be copied in full to the member. This information should be summarised before passing it to the member – this serves to protect UNISON's interests in the longer term.

6. Requests for an individual's own personal data - a "subject access request"

An individual has a right to request access to all the personal data that an organisation holds about them. They also have a right to know the source of the data, the purposes that it is being held for and who it has been shared with. The individual can make the request in writing (by letter, email, social media etc.) or it can be made verbally.

UNISON receives several subject access requests (SARs) each month. Individuals requesting access do not need to provide a processing fee unless the request is "unfounded, excessive or repetitive" or the request is for further copies of information already provided. The individual must provide some form of identification so that we ensure we are providing data to the right person.

By law, UNISON must respond to subject access requests within one month.

Data we need to provide can include:

- Details held on WARMS, including notes.
- Case files including handwritten notes, emails, letters etc
- CCTV footage
- Photographs
- Telephone call recordings
- Records of any contact with UNISON Direct
- Complaint files

The scope of the search includes branches, regions, UNISON Centre, UNISON Direct and any other organisation which is processing data on UNISON's behalf.

It is important to note that email exchanges between branch officials, representatives and/or regional officers with reference to a member may have to be considered for disclosure in response to a SAR. So please:

- Keep any documented information factual.
- Carry out periodic housekeeping on email and other information sources.
- Keep a file note of the source of any incoming information (it helps when dealing with a subject access request to know if the requestor already has a copy of the document).
- Only copy into emails those people who "need to know".
- Do not use abusive or derogatory language in emails or other documents.
- Do not include any personal opinions in email or other documents.
- Do not use email when a telephone call will do.

What to do if a request for subject access arrives at the branch

If the branch receives a request it is important to immediately forward it to the Data Protection Officer at dataprotection@unison.co.uk otherwise time could be lost and so fewer days available to complete the response to the request. SARs must be responded to by UNISON within short deadlines or face large penalties. It is therefore important to recognise and respond to them quickly. Please see Appendix 3 – How to recognise a subject access request (SAR).

The branch should be prepared (but not begin) to gather all their relevant documents, including emails, as the UNISON Centre will soon be in contact asking for it. It is important to provide all the relevant documents, even if some are thought to be contentious.

UNISON Centre's SARs team will review all data before it is passed to the individual, and will either redact, withhold or provide the data in response to the SAR. Flag any documents which you consider to be contentious or sensitive in some way. Please explain why you are concerned about them being released. This will help inform the response to the SAR, but does not necessarily mean that the information will be withheld. Information can only be withheld in response to a SAR in very limited circumstances.

7. Breaches of data protection

Actions to take immediately

Whenever there is an actual or suspected breach of Data Protection Regulation, regardless of the level of impact, contact the Data Protection Officer at UNISON Centre: dataprotection@unison.co.uk .

Give the Data Protection Officer all the information that you can at that point about the breach. For example:

- The nature of the actual or suspected breach.
- The type of data involved and its sensitivity, including a copy of the information that has been compromised if possible.
- How the breach happened.
- When it happened.
- When you become aware of it.

There is a requirement under GDPR to report certain breaches to the ICO. Where necessary, this will be done by the Data Protection Officer. Please do not report anything to the ICO yourself – report it to the Data Protection Officer.

For examples of breaches please see Appendix 4 – What is a Data Protection breach and how to report it.

Once a breach has been managed, it is important that any lessons learned and security improvements are put in place as soon as possible, to avoid any recurrence of the same problem.

Key Branch Activities and Data Protection

8. Branch as employer

Under Data Protection Regulation, “data controllers” decide the purposes and means of processing personal data and “data processors” are responsible for processing personal data on behalf of a controller. For most forms of processing, UNISON is considered the data controller for the work that branches do.

An exception to this is where branches employ their staff directly. In that case, they are considered the data controller for their employees’ personal data.

Data controllers have legal obligations under Data Protection Regulation. If you fail to meet these the ICO can issue the branch with penalties of up to 4% of annual turnover.

Some important obligations to your data subjects (employees) include:

- Providing all personal data you hold on them for free within “1 month” of it being requests.
- Reporting breaches of their data to the ICO within 72 hours of becoming aware.
- Being lawful and transparent regarding how you process their personal data.
- Documenting your compliance with Data Protection Regulations.
- Deleting or removing their data where there is no compelling reason to keep it.
- Collecting their data for specific, clear and legitimate purposes.
- Collecting only data that is necessary in relation to the processing purpose.
- Securing their data against unlawful or unauthorised processing.
- Rectifying inaccurate or incomplete data you hold on them.
- Halting or restricting processing of their personal data where they object.
- Not transferring their data outside the EU without controls in place.

There are lots of resources provided by the ICO to help small organisations with meeting their Data Protection obligations. You can find these on their website: https://ico.org.uk/for-organisations/business.

Whilst UNISON is not responsible for your obligations as data controller, we can offer help and advice regarding ways to meet them effectively. You can obtain this from the data protection team on dataprotection@unison.co.uk.

Appendix 1 - Resources

Websites:

Information Commissioner's Office – https://ico.org.uk/for-organisations/

Data Protection Act (1998) guidance - https://ico.org.uk/for-organisations/guide-to-data-protection/

General Data Protection Regulation (2016) guidance - https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

Privacy and Electronic Communication (PECR) guidance - https://ico.org.uk/for-organisations/guide-to-pecr/

Encryption guidance - https://ico.org.uk/for-organisations/guide-to-data-protection/encryption/

UNISON Privacy Policy - www.unison.org.uk/privacy-policy

Alternatively, search online for:

Information Commissioner's Office

Data Protection Act ICO guidance

General Data Protection Regulation ICO guidance

Encryption ICO guidance

UNISON privacy policy

Appendix 2 – Data Processor Agreement for Branches

Please contact dataprotection@unison.co.uk to request this if you need it.

Template data processor agreement to follow.

Appendix 3 – How to recognise a subject access request (SAR)

Under Data Protection Regulation, individuals have the right to request the personal data that UNISON holds on them. This is known as a Subject Access Request (SAR). Personal data is any information that is about, or can identify, a living person.

Data Protection regulation requires UNISON to provide the personal data to the subject within 1 month of when a SAR is made, or risk receiving large penalties for not meeting our obligations. It is therefore important to be able to recognise them, as they will not all look the same.

The following are all examples of SARs that UNISON would be obliged to respond to:

- “I would like to see any emails you have regarding me....”
- “I want my Case file...”
- “I request all details of my membership...”
- “I want all information you have on me for the period from 2004 to 2017...”
- “I request the CCTV footage for Monday the 13th showing me...”
- “I request a SAR detailing all information you have regarding me...”
- “I am exercising my right under the above legislation to request a copy of all records held by UNISON on me, whether hard copy or electronically...”
- “Please accept this email as a formal subject access request for information held about me”;
- “Under the Freedom of Information Act I request the following data you have on me...”

N.B. a SAR may incorrectly refer to other regulations such as the Freedom of Information. If the subject is requesting personal data that UNISON holds concerning them, it is still a SAR and must be responded to.

The medium of the request does not matter, so you could receive it:

- in person.
- by letter.
- by email.
- by phone.
- by text.
- by social media.

On recognising a SAR as described above, please immediately forward it in an email to the UNISON Data Protection Officer at dataprotection@unison.co.uk, Cc’ing in your regional data protection contact. This will allow us to quickly determine what personal data will need to be provided to the subject by the 1 month deadline.

If you have any further questions regarding recognising SARs, do not hesitate to contact the data protection team on the email provided above.

Appendix 4 – What is a data protection breach and how to report it

In the course of its activities, UNISON accrues a large amount of personal data regarding members, staff and activists. Personal data is any information that is about, or can identify, a living person. This includes things such as their name, address, their image, phone number, email address, membership number and IP address.

Under Data Protection Regulation, a data breach is: “a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to personal data”. It therefore does not always refer solely to the loss of personal data.

Most breaches are a result of human error or procedures not being followed. They are rarely malicious.

Data protection regulation requires UNISON to report certain types of data breach to the ICO within 72 hours from when you discovered it, or risk incurring large penalties for not meeting our obligations. It is therefore important to **report suspected breaches or near misses to the UNISON Data Protection Officer on 0207 121 5237 or dataprotection@unison.co.uk as soon as they are discovered**. If in doubt, call anyway!

The following are examples of data breaches of varying severity:

- Leaving a case form on a bus which is either recovered later or lost.
- A UNISON laptop or mobile phone is stolen.
- Documents are left behind or mislaid during a branch move.
- Confidential waste is disposed of insecurely.
- Accidental deletion of a member’s case file.
- An employer informs you that a DOCAS file has been sent to a non-UNISON recipient.
- An RMS bulk update is applied to the wrong members in error.
- Saving a list of members in a publicly accessible location.
- Sending an email to lapsed members.
- Using the To or Cc field to send a bulk email instead of the Bcc field.
- Sending an email to the incorrect person with the same name as the intended recipient.
- Member data is accessed during a cyber attack.
- A significant disruption to access to MyUNISON.

If you have any further questions regarding data breaches, do not hesitate to contact the data protection team on the email provided above.

Appendix 5 – Retention Schedule for Branches

Data	Description	Examples	Start of retention period	Retention period	Action at end of retention period
Case files / documents	Documents generated during the course of representation of members from initial stages through to resolution.	• Completed CASE form • Meeting notes • Email exchanges • ACAS documents • Compromise agreements • Communication from/to member	Closure of case	6 years	Secure destruction
Membership information	Paper membership forms	• Membership forms • Direct Debit forms	Details input on RMS and membership started	1 year	Secure destruction