University and College Union

Organising under GDPR

Table of contents

Introduction

This guidance is for UCU members and staff. It covers what you can and cannot do in your organising activities under UK data protection law, including the General Data Protection Regulation (GDPR).

There are general guides to GDPR in a trade union context but this one focuses on organising: how you can use data about UCU members and non-members in a given workplace to persuade them to join and/or become more active in UCU. It does not cover casework or other activities.

A section outlining principles of GDPR-compliant organising is followed by a section covering different types of organising activity, with specific examples. The guidance concludes with general advice about data security and respect for members' privacy.

Summary checklist

The key messages from this guidance are summarised in the following checklist:

1. **Purpose**: consider who needs to process data and for what purpose. Is the purpose in line with UCU's purposes as a union?
2. **Sharing members' data**: members' data can be shared within the union as long as this is in keeping with the union's stated purposes.
3. **Local agreements and employer policies**: before you start using non members' data, check what agreements and employer policies exist in your institution that may affect your ability to process that data.
4. **Consent**: you need non members' consent to process data that is not publicly available and in some cases you may need it for members, too.
5. **Contacting non members**: you can process non members' data for the purpose of contacting them but you will usually need their consent to do more.
6. **Anonymity**: if you need to keep data but do not have the right to process it, anonymise it.
7. **Conversations**: in person conversations are the best way to process members' and non members' data in a respectful, GDPR-compliant way.
8. **Security**: whether the data is in digital or physical form, process it securely.
9. **Length of time**: you can process data over the longer as well as the shorter term, as long as you have a clear purpose for doing so.
10. **Respect**: be transparent about your use of personal data, and respect people's boundaries. A certain method might be legal but that doesn't mean it is the best to use from the perspective of organising or privacy.

Agreements, policies and employer behaviour

This guidance presumes that the workplace where the reader is organising is not covered by any agreement relating to the use of employees' data. The approach which it sets out will normally be GDPR-compliant in any workplace UCU chooses to organise in. However, in many workplaces there are established practices, employer policies, and agreements between UCU and the employer that may affect how the union can use employees' data and it is important to be aware of these.

There may be a standalone data-sharing agreement between the branch and employer, or in some cases data-sharing may be covered by a section of the branch's recognition agreement (the vast majority of UCU branches are covered by a recognition agreement).

Some agreements permit UCU to do more than the bare minimum allowed under legislation: for instance, some employers have agreed to give the union a complete list of all employees each year, including their contact details, department, and job title, without requiring the union to seek the consent of each employee to process their data.

Before undertaking any of the activities in this guidance, you should find out whether your branch is covered by a recognition and/or a specific data sharing agreement and if so, what it says.

You should also be aware of any institutional privacy/data protection policies and what they say. In particular, look out for any language that explicitly prohibits use of employees' personal data by trade unions. This may be found at institutions with no data-sharing agreement with the union where the employer has refused to agree to any disclosure of information to UCU.

UCU's position is that communications by a recognised union with all employees on matters of legitimate concern to them could reasonably and objectively be described as a core trade union activity. Nevertheless, some employers will disagree with this position and will try to prohibit the union from collecting and using staff data. As well as refusing to share data, employers might also raise the prospect of a complaint to the Information Commissioner's Office, of other legal proceedings, or even of disciplinary action against organisers who are their employees. Cases of employers following through on threats against members are rare but when they do happen, UCU has a strong record of defending them.

Although UCU's position has been tested and defended in court in the past, the most efficient way to protect yourself against such risks is to follow the advice in this guide. Above all, work towards strength in numbers. Make sure you are not the only person undertaking organising activities in your workplace. The more members are taking part in organising and following this guidance, the safer you will all be.

If you are unsure about what you can do in your branch, or you would like to see copies of model or actual data sharing agreements, contact your regional or national UCU office via the UCU website's **Regions & Nations** section.

General principles

Personal data is any information that relates to an identified or identifiable living individual. This person is called a 'data subject'. Examples of personal data that could be relevant for organising purposes include:

- Job title and grade
- Salary
- Religious beliefs and political opinions
- Whether the subject is a trade union member or not

The last two bullet points in this list are 'special categories' of personal data which require extra protections when processing. For more information see the definitions of **personal data** and **special category data** on the Information Commissioner's Office (ICO) website.

It will be helpful to bear the following principles in mind when you are working out how to 'process' (collect, store, and use) personal data for organising purposes.

Transparency

If you are part of a UCU branch you should create a culture of transparency about your organising activities. This includes:

- Drawing attention wherever possible to UCU's **data policy**, e.g. including a link when you contact people on union business.
- Telling members and non members what information you gather about them, and why you gather it.
- Being open about the fact that you want to have information about the whole workforce and recruit more people to the union.
- Involving non members in as many of your activities as possible, including meetings, surveys, petitions, etc.

Consent

For much of the data you will need for organising purposes, especially data relating to non members of UCU, you will need the consent of the data subject to process it. When you seek the data subject's consent, you need to inform them what data you are processing and what purpose you are processing it for.

Purpose

You need to be clear with yourself, with colleagues in your branch and with your data subjects about exactly why you need the data you are processing. It needs to be no less and, crucially, no more than what you need to do your union work.

Imagine someone asking you for all the data you have about them and why you have that data. Could you explain to them why the union needs to process that data? If you can't, don't process it.

The data needs to be relevant to your organising activities. If you gain access to data which your branch may wish to use for a different, non-organising purpose, you may need to get specific consent to use it for that new purpose.

For example, if a non member discloses that they have an individual grievance to a member volunteer holding a recruitment conversation with them, the member volunteer should ask the non member if they mind it being reported to the branch casework coordinator so they can spot patterns in grievances. The volunteer should also follow up with the non member by email, or use some other mechanism to record the fact that the non member has consented to having that data shared for that purpose.

Time limits

You should not process data any longer than is necessary for the purpose(s) you collected it for. When you process data you should inform the data subjects how long you are going to process it for and when it will be destroyed or anonymised (on anonymising data, see the section headed 'Mapping the workforce and contacting non members').

Security

Steps should be taken to ensure that there are no data breaches, in which data is shared more widely than it needs to be, or for different purposes from those it was originally collected for (and which the data subject consented to, if they needed to consent). The Information Commissioner's Office can impose financial penalties on organisations that are responsible for data breaches, including trade unions.

A common example of a data breach is sending an email to a group of members that includes their email addresses in the 'cc' rather than the 'bcc' box, thereby disclosing each member's email address to every other member in the group. This not only discloses personal contact information, it may also (depending on the content of the email) disclose the recipients' trade union membership.

Another example of a data breach would be losing a document that contains personal data: for example, if you are talking to members in the workplace and you misplace a piece of paper containing information about them, including whether they have voted in an industrial action ballot.

If you become aware of a data breach you must report it immediately to UCU's Data Protection Officer by emailing DPO@ucu.org.uk.

Rights of the data subject

Data subjects need to be able to find out what data you have relating to them. You need to keep a record of any consent which data subjects have given you for data to be processed. Data subjects also need to be able to prevent you from processing data about them, and they need to be able to ask you to erase data or correct inaccurate data which you hold about them. For information about this see the section on 'Subject Access Requests'.

Types and examples of organising activities

Sharing data from the membership database

The question of access to the UCU membership database is often raised when branches are getting the vote out for ballots, or undertaking other organising or mobilising activities.

At the time of writing in May 2021, direct access to the UCU membership database is normally only granted to trained UCU staff and to two designated contacts per branch. That is principally because of the technical limitations of the membership system, which is currently being overhauled. This guidance will be revised as and when new opportunities for broadening branch-level access to the database become available.

However, the fact that direct access to the database is limited does not prevent branches from sharing members' data more widely. It is possible to download and securely store a branch's membership data (or parts of that data) in spreadsheet form, and the UCU **data policy** allows for data which members have given the union to be used in any way that is compatible with our legitimate purposes as a trade union.

For example: let us say that a branch wants to gather signatures for a petition. The branch might ask any departmental reps to gather signatures, department by department. The rep should already have a spreadsheet listing the members in their own department which is regularly updated from the central database, to ensure accuracy.

The role of a departmental rep includes acting as a point of contact between all members in that department and the branch committee. It is part of the union's legitimate purposes and in line with our **data policy** to let the rep have that information for as long as they have that role.

What about departments or work areas that do not have a rep? Or what if there is a rep, but the rep wants to engage other members to help them gather the signatures for the petition? In either case, the branch can let ordinary member volunteers who are not reps have some data relating to the members in that department. In doing so, the branch needs to take special care that the data is shared in a way that fits the purpose it is being shared for.

For example: if five member volunteers are being asked to gather signatures from a department with thirty members, each volunteer might be given whatever data is necessary to contact, say, five other members and persuade them to sign. The sharing of the data needs to be proportionate, so that each volunteer only has the contact details for a manageable number of people and does not hold data about lots of people whom they would otherwise be unlikely to have time to contact.

'Whatever data is necessary' can be broadly construed as long as it is in line with the purpose: for example, it could include information about whether the member in question has signed any other branch petitions in the past.

At the same time as the volunteers are provided with the members' data, they should also be told to:

- Avoid contacting the members in question or using their data for any other purpose than signing the petition.
- Store their copy of the data securely and destroy or anonymise it as soon as the campaign which the petition is part of has finished (except for data which the union needs to keep for the purpose of longer term recording of members' activities, as set out in the section on 'Tracking participation over the longer term').
- Get the member's consent to process any other data which they might share with the volunteer when the volunteer makes contact, if it relates to a purpose unrelated to the petition (for example, if the member says something about some casework which they are the subject of, as in the example given under 'Purpose' earlier in this document. While it may be part of the role of a departmental rep or caseworker to process data about members receiving casework support in their department, it is not part of the role of a member volunteer if they are only gathering signatures for a petition).

Mapping the workforce and contacting non members

Mapping the workforce (in particular, the part of the workforce eligible for UCU membership) is a fundamental part of organising which every branch should aim to undertake regularly as part of its campaigning and recruitment agenda. For a general guide, please read **this Workplace Mapping document**. In other unions this practice is sometimes known as 'charting' or 'wall charting'.

Some kinds of mapping may involve processing information about UCU members which cannot currently be recorded in the membership database: for instance, what issues a member is concerned about, or whether they have acted as a rep in a previous workplace. This is fine, as long as the information is stored securely and with a clear purpose. You need to be able to explain why the information needs to be processed as part of your mapping exercise, and why that mapping exercise is necessary. If the information is **special category data**, you may also need the member's explicit consent to process it, or you may need some other condition in place (e.g. that the member has made the information public).

Mapping will also involve processing data relating to non members. You may need their consent to do this. Mapping of non members is therefore more complicated, especially where non members have not (yet) been contacted by the union to seek their consent to have their data processed.

If the employer or the non member(s) in question have made their data publicly available, you can process that data and include it in your map without needing their consent – for example, if the employer has put the non member's name, job title and department on their public website. However, you still need the subject's consent to process any extra data that is not publicly available and add it to the map. You also need to bear in mind that any non-public data you process alongside the publicly available data (e.g. notes about the non member's attitudes towards the union) will be covered by any Subject Access Request made to the union (see further the section headed 'Subject Access Requests').

If the employer does not make staff data available publicly or to the union, you need to take even more care over how you process that data for union purposes – even if they make it available internally, e.g. via a staff-only section of their website.

The safest way to proceed in mapping non members whose data is not publicly available is to:

- Have a clear purpose which the mapping exercise is linked to: e.g. recruiting more members by holding an event or talking to them individually; surveying non members on an issue; involving non members in a specific branch campaign.
- The purpose should involve contacting the non members you have mapped. The contact needs to take place within a specific time frame and as soon as possible after the mapping exercise has been carried out.
- If you want to map non members without contacting them, leave any data that would make them identifiable out of your map. Anonymised data can still be useful for mapping purposes, e.g. seeing how many workers in a department or institution are on permanent as opposed to fixed term contracts.

- When you contact a non member, tell them what data you are processing and why, seek their consent to continue processing it, and do not continue processing it unless they give you their consent.
- If, after contacting a non member, you do not get their consent to continue processing the data, you must anonymise it: remove anything that could allow the person(s) processing the data to identify the data subject.

The best way to do this is by contacting non members individually, one-on-one. People are much more likely to give you a response (and a positive one) if they are contacted this way, especially if it is by someone they know and trust (e.g. a departmental colleague). If you send a blanket email to everyone in your map, a significant proportion of recipients will not read it and an even higher proportion will not respond.

For everyone who does not respond, you will no longer be able to process their personal data and you will need to anonymise it in a way which ensures their identity is unlikely to be guessed by someone who has access to the information and also the factual context.

For example, if a departmental rep uses a map to contact thirty non members in a seventy-person department and fifteen either do not consent or actively object to having their data processed, the rep should edit the map so that it only includes information that is too broad to make those colleagues identifiable.

If in any doubt, the rep should relinquish the information to someone else in the branch who has no knowledge of that department and therefore no chance of being able to identify individuals using an awareness of the factual context. This way, your branch can preserve useful information which your mapping exercise gives you about the workforce without violating GDPR.

Mapping the workforce more than once in a year can be problematic. For instance, if non members who are mapped and contacted by the union object to having their data processed as part of the map, we believe that a year is a reasonable amount of time to wait before you map the workforce again and contact those non members to see if their opinion has changed. If you map and contact non members more frequently than that, you risk committing a data breach. If a non member states when contacted that they must never be contacted again, then you must record that fact and comply with their request.

Ultimately, the best way to ensure you can process a non member’s data more freely, in a way that will benefit all your campaigns and ultimately all staff in the institution, is to recruit them into the union. Active recruitment should be integrated with all of your branch’s other activities. It should follow naturally from any mapping exercise and it should precede and be a part of any campaign which the branch undertakes.

Sharing maps with members

You may be interested in sharing data relating to members and non members via physical as well as digital maps, and you may wish to do so very widely within your branch's membership. A physical map might be located in a union office in your institution, if your branch has one.

One purpose of creating such a map is to impart a sense of collective ownership of the branch's activities to as many members as possible – including member volunteers as well as workplace/department reps and elected branch officers.

The data recorded in a physical map might include (for example):

- The fact of union membership or non membership.
- Name, department and job title.
- Participation in previous or ongoing union activities.

You can use physical maps as long as you continue to observe the principles set out in this guidance regarding secure storage and processing, and the purposes of sharing special category personal data with members. In particular:

- Don't let other members see a map if there is no purpose in letting them see it. If you are conducting a recruitment drive in a very large institution with many departments, it is reasonable to let members see a map covering their own department, so they can help each other and discuss how to go about recruiting colleagues they are familiar with. However, you should not let them see maps covering other departments unless they will also be involved in recruitment activities in those other departments.
- If you do need to partition physical maps so they can only be used by certain sections of your membership, don't leave them up on the wall of a union office when they are not in use. Instead, keep them locked somewhere which only the appropriate individuals will have access to.
- Avoid including contact details in a map, if the map might be seen by members who have no reason to contact the workers in question. Avoid including any other personal data that is not relevant to the union's purposes in creating the map and sharing it with members. (The exception to this is where the data is publicly available or the subject has consented to let the union process it in this way).
- Make sure that the map cannot be seen from outside the office or wherever it is kept, and that it can be stored securely.
- Follow the procedures for mapping non members in the section on 'Mapping the Workforce', including ensuring that you seek the appropriate consent to

continue processing their data. For example, don’t ask non members for their consent to let ‘UCU representatives’ process their data if you intend to let members who are not reps continue to see it; instead, refer to ‘UCU’ in general.

Conversations in person and by phone

The best and safest way to organise and to process data in a GDPR-compliant way is through one-on-one, in-person conversations. When done in the right way, an offer of a conversation can reach people who do not attend meetings and are not responsive to mass emails or other forms of communication.

If you are having a conversation in person with a non member, you do not need their prior consent to start the conversation. If you want to take notes or keep any record of the conversation that involves their personal data, you do need their consent and you can obtain it during the conversation (make sure that a written record of their consent is created).

If you are having a conversation with a UCU member, you do not need their consent to create a record as long as the purpose of the record aligns with the overall purposes of the union. However, it is always good practice to tell members what the purpose of the conversation is and what kind of record you will keep of it.

When holding conversations by phone, remember not to disclose a member or non member’s personal data to anyone else unless you know they are permitted to have it (either because they are covered by the union’s legitimate purposes or, in the case of a non member, because the data is publicly available or the data subject has explicitly consented to share the data with them). For instance, do not leave a voicemail message on a shared office telephone that discloses the fact that the intended target of your call is a union member.

Meetings

When you hold meetings of UCU members, it is good practice to keep an attendance register, if only for the purpose of tracking members’ participation in the branch’s activities. You do not need members’ consent to do this. However, you do need members’ consent to share information about meeting attendance beyond the branch. For example, if you want to take a photo of the meeting and post it on social media, tell everybody who will be in the photo what you are doing so they have the option to leave the area you are taking a photo of.

What if your meeting is open to non members as well as members? If you want to use such a meeting to process non members’ data (for instance by gathering their names and/or email addresses), you must seek their consent. When you seek their consent, you must tell them what data you are processing and why, and point them towards UCU's **data policy**.

Emails

You can of course email UCU members for union purposes. However, take care not to share or disclose a member's address more widely unless there is a clear purpose for doing so. For instance, if you are emailing a group of members in your branch to invite them to a meeting, make sure you BCC them so they cannot see each other's addresses. You should also make sure that there are mechanisms for allowing members to opt out of receiving emails and other forms of electronic communication – except for communications that are essential for allowing them to continue to be a member in good standing, e.g. communications about their subscription payments.

Emailing non members is more complicated. Emails, like other forms of electronic communication, can constitute 'direct marketing' and therefore be subject to the Privacy and Electronic Communications Regulations (PECR) 2003. This is one reason why approaching non members in person for a conversation is safer than contacting them remotely.

You can contact non members via email if you take the precautions outlined in the section on 'Mapping the workforce and contacting non members'. These precautions include not processing non members' data or contacting them too frequently (i.e. more than once a year) if they do not give you their consent to process their data and contact them.

The only other situation in which you can process non members' data and contact them is if you are undertaking market research. Market research is the only activity that is exempt from the conditions governing direct marketing in the Privacy and Electronic Communications.

What this means is that you can contact the non member for the purpose of research – for example, if your branch is conducting a survey of staff – as long as you do not promote the union in any way. This includes not promoting UCU's position on the issue(s) which the survey relates to or on any other issue. This is what differentiates market research from direct marketing.

However, if a non member has been contacted through some other means (e.g. as part of a regular mapping exercise) and explicitly asked you not to contact them or process their data, you should leave them out of your market research exercise.

Text messaging

The principles of GDPR-compliant text messaging are similar to emailing. The difference is that UCU does not process non members' mobile phone numbers for the purpose of texting them, so the guidance about contacting non members is not relevant here.

When texting members one-on-one, you should use the peer-to-peer messaging service, ThruText, to which UCU subscribes. ThruText allows organisers to conduct a very large number of one-on-one conversations via text with other members. For information about ThruText please contact your national or regional office. ThruText has a facility for allowing members to opt out of receiving any and all text messages from UCU. A record is kept of each member who has opted out. The opt-out will remain in place regardless of whether the member changes branch or leaves and then rejoins the union.

The other text messaging format that may be useful for organising purposes is a group chat, often hosted on WhatsApp (though other services are available; for example, Signal is popular because it offers a high level of security). If you are creating such a group:

- Do not simply create the group and then add members' phone numbers without their consent.
- Instead, create an empty group and then use the group's invitation link to invite people to join (you can find instructions on how to do this **at this link**).
- When inviting people to join, make clear that anyone joining the group will make their number and potentially their name and profile photograph (depending on their settings) visible to everyone else in the group.

Some members may prove more willing to join such groups if the groups are organised so as to be smaller (e.g., one group per department, instead of or in addition to a larger group for the entire branch).

Petitions, surveys, and other activities

Petitions and surveys may or may not be open to non members as well as members. The same principles apply. If you are asking a non member to put their name to a petition or complete a survey, you need to:

- Seek their consent to have their data processed.
- Tell them how long the data will be stored.
- Tell them what the purpose is.

For petitions it can be particularly important to tell signatories when and how widely their data will be shared. This includes cases where the list of signatories will only be published once a certain threshold of participation is reached, e.g. in the case of a 'majority petition', when 50% of people in a workplace or a branch have signed. You need to tell potential signatories what those conditions are when you are asking them to sign the petition.

Tracking participation in specific campaigns

Data from the activities covered here – mapping, conversations, emails and texts, petitions and surveys – can be recorded and stored both over the short term and the long term, but you need to take care over how and why you are keeping those records.

For example, imagine you are a branch officer coordinating a campaign that involves gathering signatures for a petition. You have mapped the entire workplace, department by department. You have contacted some members and non members via in person conversations, other members via email and text, and you have gathered several hundred signatures. Your workplace map is a spreadsheet that shows who has been contacted in which department, by what methods, and who has signed the petition.

You can share that spreadsheet with the rest of your branch committee, because they need to see how the campaign is developing across the entire workplace, which departments are participating enthusiastically in it and which ones are not, and make decisions about where to target the branch's efforts in the next phase of the campaign. However, you should consider carefully whether the committee needs to see information that personally identifies the individuals listed in the spreadsheet. You can almost certainly afford to remove the columns featuring names and email addresses, for instance.

This calculation may depend on the nature of your workplace and the division of labour between your committee and reps or volunteers who are not committee members. If the work of contacting and persuading individuals is being done outside the committee, the committee probably doesn't need to see much or any of those individuals' personal data. Instead, you may decide to restrict that data to yourself as campaign coordinator, and to the reps or volunteers doing the work of gathering signatures on the ground (although those reps/volunteers should only process personal data for the specific area where they are gathering signatures).

Tracking participation over the longer term

Going beyond specific campaign activities, you may wish to ensure that at least one person in your branch is keeping and analysing longer term records of individuals' participation in union activities: in other words, a spreadsheet like the one described in the previous section, but covering individuals' whole time as employees in your institution and tracking their participation in multiple campaigns rather than just one.

This is vital for effective organising and it can be done in a GDPR-compliant way. Think about who needs to do this and who doesn't:

- A membership secretary, or the chair of an organising committee, might be the best individual to designate as holder of this information.
- Departmental reps can be given the information for their department, but

not for other departments.

- Members who have volunteered to help with specific campaigns are unlikely to need the information, unless it is essential for the purpose of a specific campaign they are helping with, in which case they should be asked to destroy their copy of the information once that campaign has ended.

When you are seeking a non member's consent to process data about their participation in a union activity, you need to inform them about this longer term purpose as well as any shorter term purpose. For example, if they are filling in a survey, you need to tell them that their response will be kept throughout the campaign the survey is part of, but the fact they have responded will be recorded for as long as they work in your institution, to improve the union's understanding of the workplace.

Subject Access Requests

Data subjects, whether they are members or non members, can at any time ask the union to provide a copy of all personal data relating to them, and they also have rights to have data erased or to restrict or object to its processing. This means that it is essential to keep accurate records, especially when non members give you their consent to process their data.

It is also essential to bear the possibility of subject access requests in mind when considering the channels which you use to communicate about data subjects. Subject access requests are made to and handled by UCU's Data Protection Officer, but they can cover any personal data processed for the union's purposes by union members or staff. As well as observing all the other guidelines set out in this document, don't make records or process data which you wouldn't want the data subject to see or know about.

Security

Use as much security as possible when storing and sharing members' or non members' data:

- Use password protection when sharing information from the membership database or other files containing personal data.
- Use secure cloud storage services to back up and share large files.
- Protect any devices which you use to process personal data with a passcode or password.
- When storing data in physical form, keep it locked away.

Be mindful of any data that you may share with a third party (e.g. a commercial software service which you use to run surveys of members and/or non members):

- If you are sharing a member's data with a third party you should check the third party's privacy policy to ensure that it meets the standards set out in our **data policy.**
- If you are going to share a non member's data with a third party, as well as checking the third party's privacy policy, you also need the non member's consent.
- You must ensure that use of any such service does not involve selling members' or non members' personal data to a third party.

Privacy and members' understandings of GDPR

This guidance outlines what you can legally do, but that is not the same as what is best for people in your workplace or what is best from an organising perspective. Some workers may expect you to observe higher standards of privacy and respect for personal data than you are legally obliged to observe. Some will have a confused or inaccurate understanding of GDPR. Some will be put off by receiving mass emails to large numbers of non members, not because they believe those emails are unlawful but simply because they resent communications that do not have a personalised touch.

The first contact made with a non member or a relatively inactive member can be vital for determining how they feel about you and the union more generally. If you get it wrong, you may not get another chance to reach out to that person for a long time. You should prioritise more personalised, two-way forms of communication such as in-person conversations because they are usually the best way to hold a respectful dialogue that establishes a common understanding of the information that needs to be shared if workers are to advance their collective interests.

Further resources and queries

UCU data policy: **https://www.ucu.org.uk/privacy**

Information Commissioner's Office, including general guidance on GDPR in the UK: **https://ico.org.uk/**

Watch this TUC webinar recording on GDPR essentials for union reps: **https://www.youtube.com/watch?v=deDNsKcA_z4**

This guidance from UNISON is helpful regarding GDPR issues in a trade union context, although not always applicable to UCU: **https://www.unison.org.uk/get-help/knowledge/information-collection-management-privacy/gdpr-unison-branches/**

If you have questions about anything in this guidance please contact your regional or devolved national office.