The GDPR
Unite Activist Briefing

1. **What is the GDPR?**

   The **General Data Protection Regulation**, known as the GDPR, sets out new rules on data protection and information security.

2. **Why is it in the news now?**

   Our current data protection laws date back to 1998 and haven't kept pace with advances in technology and the way we use data now. So new rules are coming in and they are in force from **25 May 2018**.

3. **Why is the GDPR important?**

   You handle personal information all the time when you are performing your role as a Unite rep, especially information about members. By following the rules in the GDPR **you can make sure you are protecting members' information** as best as you can, and avoid any complaints or sanctions.

4. **What is personal data?**

   The data protection rules apply to any information about a living individual from which the individual can be identified. That includes obvious things like name, date of birth, address, as well as less obvious things like IP or email address.

   The GDPR refers to all of this as **'personal data'** and to the individual as the 'data subject'. If an individual can be identified, for example from their membership number, the information still counts as personal data, even if their name is not included.

5. **I have heard the phrase "special category data". What is that?**

Stricter rules apply for some kinds of particularly sensitive personal information, and the GDPR calls these kinds of information **special categories of data** or special category data. It includes information about a person's race, religion, politics, health, sex life or sexual orientation.

Importantly for you in your role, it also includes personal information about **trade union membership (or non-membership).** That means that a lot of the personal information you handle as a Unite rep is likely to be special category data, because it reveals trade union membership, and so you need to follow stricter rules to ensure extra protection of this sensitive personal information.

6. What is processing?

The GDPR applies to the "processing" of personal data electronically and "processing" personal data manually (i.e. paper records) where this forms part of a structured filing system (or it is intended to form part of a structured filing system – i.e. documents that are waiting to be put on file).

The term "processing" is very wide under the GDPR. It essentially means anything that is done to, or with, personal data (including collecting, recording, storing, changing, deleting, using or sharing the data).

So accessing a membership database on your computer will be covered and, so will, printing, using, amending or sending a copy of the database or individual details from it.

7. What do I have to do to comply with the GDPR?

The GDPR says you must only handle personal information lawfully and fairly. It sets out some key principles which you have to follow and in particular it requires that you only process data when you have a **lawful basis,** i.e. a lawful reason for doing so.

You should make sure that you only handle data in line with the guidance given in this document, and in line with Unite's privacy policy and other data protection and information security procedures.

8. Where can I find Unite's privacy policy and other procedures?

You can access a copy of Unite's **privacy policy** at www.unitetheunion.org/legal-information/privacypolicy. You should read this carefully and make sure that the way you work is in line with the guidance in these documents.

Unite is in the process of reviewing all existing data processing activities carried out by the Union. The existing privacy policy will be updated before 25th May 2018 and will continue to be reviewed and updated as necessary. Further guidance will be provided once internal audits are complete.

9. Do I need to have consent from the member or individual for every use of personal data?

No. Consent is one lawful basis for processing data, but there are others. If another lawful basis applies, you do not need consent. This means you need to consider carefully which lawful basis or reason applies whenever you use personal data, especially member data.

For 'ordinary' personal data, the GDPR gives six lawful basis for processing, including consent. One of these reasons must apply to every use of personal data.

For special categories of data, which includes any information about an individual's trade union membership or non-membership, an extra condition must also apply.

However, for some information and some uses of information, it is best to get consent every time, in particular

- For **any use of medical records or reports**, you should always have consent from the individual concerned and you should keep a record of this.
- For **any disclosure of personal information outside the union** (which includes disclosure to the employer) you should always have consent from the individual and you should keep a record of this.

10. What are the six lawful basis for processing personal data?

You must have at least **one lawful basis or justification for processing** whenever you handle or use personal data. The six possible lawful basis are:

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

11. What are the conditions for processing special categories of data?

When you are handling special categories of data, which includes any information revealing trade union membership or non-membership, you need to have a lawful basis for processing (as set out above) **and in addition**, one of the **conditions for processing special data** must also apply.

There are 10 possible conditions for lawful processing of special categories of data, one of which must apply in addition to one of the lawful basis. The most important condition for you as a Unite rep is the condition relating to the **legitimate activities of a trade union**.

There are also separate conditions regarding legal claims and legal obligations in the field of employment law.

12. What is the legitimate activities' condition for processing special categories of data?

The **legitimate activities condition** allows you to process special category data, including membership information, where:

- the processing is carried out in the course of a trade union's legitimate activities and
- the processing relates only to members or to former members of the union and
- the personal data are not disclosed outside Unite without the consent of the data subjects.

In other words, you can use the personal data of members and former members in the course of Unite's legitimate activities, provided you are not disclosing any personal information outside Unite.

If your use of data falls within this, you do not need to obtain consent. However, for some information and some uses of information, it is best to get consent every time, see above.

13. What does GDPR mean for me as a Unite rep?

As a Unite rep, the GDPR means you can use the personal data of members and former members for any of the union's legitimate activities, provided that you are not disclosing any personal information outside Unite.

You should still think carefully about your use of personal information though. If you are using particularly sensitive information such as medical reports or records, you should always obtain consent from the member. Similarly, you should always obtain consent for any disclosure of personal information outside the union.

You should also make sure you protect member information and handle and store it safely and securely. There is more information about this below.

14. What should I do if a member sends me a letter from their GP that would help defend them in a capability hearing, but they ask me not to share this with the employer?

You should tell the member why you think it would help their case to share the letter, but do not disclose this to the employer unless the member agrees. If the member changes their mind, it is always best to keep a written record of this – this could be an email from the member or a note of a pre-meeting where you discussed this with them.

15. Does the GDPR mean I cannot obtain details of the members in the workplace I represent?

You can obtain details of members from your Regional Officer or Branch Secretary for your union work, but that information should not be passed on, should be held securely and kept up-to-date.

It is also OK for your employer to provide you with details of new joiners in your workplace, as long as they provide you with details of all new joiners, not just non-members.

16. I send my members information on issues like pay negotiations and health and safety issues. Can I still do that?

Yes, keeping members updated on the work the union is doing is part of the legitimate activities of the union so you can still do this. You don't need to obtain consent to do this, provided you do not disclose any personal information outside the union.

17. How should I store personal data of members?

If you keep hard copies of any member information such as membership lists or personal case files, you should store these in a locked draw or cabinet. Do not leave any papers out at home or at work when you are not there and when they could be seen by others.

For emails and documents which you hold electronically, make sure you keep them on a computer or an individual user account to which only you have access, and which is password protected. You can password protect individual documents as well. If you hold the only copy, make sure you have arrangements in place to back up your data.

If you need advice on how to password protect a computer or an individual document (like a membership list), you should contact your Unite Regional IT Co-ordinator.

18. Can I use a work email address to correspond with members?

In some workplaces, there may be facilities agreements permitting use of work emails, in others reps won't use the work email system for communications with members. If you're unsure about the practice in your workplace, check with your Officer whether it's OK to use your work email, and if you are using it, include the words Private and Confidential in the subject line.

It is better to use a Unite email address when dealing with union issues, if you can, or a private email address that only you can access. You should not use a shared family email address for union matters, to make sure members' data is kept confidential. If you don't have a union email address, you can request one by contacting your Regional IT Co-ordinator. If you are concerned, think about password protection, particularly of sensitive documents

19. Can I keep personal data (e.g. membership lists)?

Yes, you can keep any personal data which you need to carry out the legitimate activities of your role as a Unite rep. You should ensure any membership list you are using is kept up-to-date.

If you are asking an individual member to provide you with their personal information, for example for you to help them with a personal case or for an industrial action ballot, then tell them why you need it.

The data protection rules require that you only keep personal data for as long as you need it. So as soon as you have carried out the work you are doing with the information and reached a satisfactory conclusion, dispose of it securely. Your Regional Office can assist with secure hard copy data disposal.

Also, the data protection rules say that you should only collect and keep personal information that you need. Don't take copies of anything you don't actually need for the work that you are doing for the member. This is referred to as 'data minimisation'.

20. What are the good practices I should adopt to ensure I am protecting members' personal data in accordance with the GDPR?

You should make sure you keep papers in a locked cabinet, and do not leave them out where others could see them.

You should use a password protected computer or individual user account for work in your role as a Unite rep. Also make sure mobile devices are password protected as well. 25% of complaints about loss of data are because of loss of mobile devices.

You should take extra care if you have membership information with you while travelling. You should never leave papers, bags or a laptop unattended on a train. You should not discuss member information on the phone or when others can hear you.

You should never leave member files or information in a car.

You should never provide member information to third parties outside the union without the member's explicit consent.

You should dispose of member information (e.g. membership lists) securely when you no longer require them.

21. What do I do if I have a query about GDPR?

As a first step, raise it with your Officer. They will be able to advise you and point you in the right direction to relevant policies and procedures.

22. What do I do if I discover a loss of member information or other personal data breach has happened?

You must report this **immediately** to your Regional Legal Officer and Regional Officer. There are very strict rules about time limits for reporting data breaches to the regulator, the Information Commissioner, so Unite needs to know about the problem as soon as you discover it. Don't be worried about bothering someone unnecessarily, you must report all possible issues, even if it's not a serious problem or if you find the information later.

23. What rights do members have to see their data?

Members have the right to see the personal data that Unite holds about them electronically or in a highly structured hard copy filing system. This is called the right to make a subject access request. The GDPR provides for stronger subject access rights than before. Under the GDPR, individuals have the right to be given access to their personal information, generally without paying a fee, and in standard cases, information must be provided without undue delay and within a month.

You should have this in mind when you write emails or notes about members.

If you receive a request from a member for a copy of their data, you should pass this immediately to your Regional Officer.

24. My employer provides me with information relating to Unite members. Is it possible that they may ask me to sign a GDPR Agreement?

Yes it's possible, any organisation that shares information with a third party may look to put agreements in place to ensure that the data that is being provided to others is only used for the purpose it is provided and is kept securely. This is **not** a requirement under the GDPR and, if your employer asks you to sign a data agreement, please speak to your Officer to ensure that any agreement is appropriate and proportionate.

Unite Legal Services
4 May 2018