GDPR: How to Make It Work for Unions

Toolbox for Trade Unionists from industriAll European Trade Union

industriAll EUROPEAN TRADE UNION

FRIEDRICH EBERT STIFTUNG
Competence Centre Future of Work

Why this toolbox?

GDPR stands for the General Data Protection Regulation. It came into force in 2018 to update and unify EU data protection rules. There is sometimes confusion about what GDPR means for trade unions. This short toolbox from industriAll European Trade Union summarises the key information trade unionists need to know about GDPR, including the law's main provisions, the ways it impacts on trade union work and union strategies to defend their members' rights as pertains to personal data.

Throughout this toolbox, notes in the margin will indicate the relevant articles of the GDPR to the topic being discussed. You can find a link to the full text at the end of this publication. Don't hesitate to consult the text directly for more information. If an employer references a specific article, you can use the notes in the margin to quickly find relevant information in this toolbox.

What is GDPR?

The General Data Protection Regulation is a type of EU legislation called a regulation. A regulation applies directly to all EU member states. This differs from a directive, the instrument often utilised to implement EU standards of most interest to unions, like the Working Time Directive or rules on occupational health and safety. While directives set out principles which are then applied through national legislation, regulations, like GDPR, lay down a single legal text that applies to all EU member states. This means that the text of the regulation, as published, directly applies to workers' data anywhere in the EU.

GDPR applies to any personal data that is processed

GDPR protects people's personal data, defined as any information that identifies, or could be used to identify, a physical person. The law regulates data processing by any organisation for any purpose other than purely personal use. Data processing refers to anything you might do with data, such as collecting, filing, storing, indexing, consulting or otherwise using data.

GDPR puts obligations on both unions and employers

GDPR applies to unions as organisations that process data. This means that any information you hold about members, for example membership lists, case files or social security information, must be handled in line with GDPR.

GDPR also covers data collection by employers. Unions should have enough knowledge of the legislation to ensure that employers follow the rules and respect workers' data protection rights.

GDPR sets out a series of principles for how personal data is to be processed and clear reasons that act as lawful justifications for processing data. More information about the details of GDPR, as well as a glossary of essential terms, can be found towards the end of this toolbox in the 'GDPR Key Facts' section.

Why should unions care about GDPR?

Trade unions need to know about GDPR in order to:

- Keep the union within the law when processing data, particularly because trade union membership is a special category which requires specific protections (see below)
- Ensure workers' data is being protected and employers are behaving as the law requires
- Push back against employers who erroneously use GDPR to undermine union activities

Keeping your union compliant

GDPR has now been in force for several years and your organisation should be compliant. It is important to keep its provisions in mind when dealing with personal data. This means:

- Identifying the purpose and legal basis for processing data before doing so. Remember, you do not necessarily need a data subject's consent if there is a reasonable legitimate interest or contractual basis for processing. For example, someone may reasonably expect their membership details to be accessed in order to assist with a dispute or case work. However, the data processed should be kept to the minimum to achieve the purpose and not be shared outside the organisation without consent.

- Checking your union has a data protection officer and knowing who this is. Make sure they have the skills and resources they need.

- Ensuring clear arrangements in writing when data is processed outside the union, for example by lawyers, researchers, consultants etc. The data protection officer should be able to ensure compliance with GDPR.

- Being aware of special categories of data, including trade union membership status, and ensuring the special protections are met (see below).

Understanding Special categories

Article 9

GDPR prohibits the processing of these special categories except in certain, specified circumstances. Also note that national law may place extra restrictions on processing data on some or all of these categories (for example, ethnic origin in France). These special categories are:

- racial or ethnic origin
- political opinions, religious or philosophical beliefs
- **trade union membership**
- genetic data, biometric data for the purpose of uniquely identifying someone
- data concerning health
- data concerning a person's sex life or sexual orientation

However, there are important exceptions to this prohibition. These specifically allow trade unions to carry out their legitimate activities, whilst protecting against the misuse of such data by employers. These most relevant exceptions for unions are:

- When the data subject has given explicit consent for processing the specific data for one or more specified purposes

- When the data controller must process the data to meet obligations under employment or social security law (as authorised by national legislation or collective agreement)
- When **a union or association is carrying out its legitimate activities** as long as the data only relates to members and former members or people who are in regular contact with the organisation (for example a non-member who is in contact with the union). This data must not be shared outside the organisation.
- If the data has already been made public by the person concerned
- If necessary as part of a legal claim
- For reasons of substantial public interest whilst safeguarding the rights of the data subject

Importantly, article 9 affords specific protections to workers against being blacklisted or discriminated against because of their trade union affiliation, whilst allowing unions to carry out their normal activities and representing their members. Article 9 means that employers cannot collect information about a worker's trade union affiliation without their specific consent.

Fighting blacklisting and the right to access

Article 15

If you believe that a worker's union membership has been illegitimately recorded by an employer, you can support the worker to make a subject access request under article 15 of GDPR. This is the same procedure for requesting any personal data an employer may hold about a worker. The worker can then request rectification or deletion of the information.

You can also lodge a complaint with your national data protection supervisory authority. See the end of this publication for how to get their contact details.

Article 77

How can unions use GDPR?

Unions should not see GDPR as a threat or a danger. Instead, because of its legally binding character, and the specific rights it affords to unions, it can be an important tool for the labour movement. When employers cite GDPR as an excuse for obstructing legitimate trade union work, unions can and should push back. The best way to do this is by understanding the legislation, and knowing where to go to get further advice and help.

Your trade union's lawyer may be the first port of call for more information. Your national centre may also have useful information. IndustriAll European Trade Union can also point you to specific resources developed at European level. You can also find more resources and links at the end of this publication.

Demand to be consulted about data protection

Articles 37-39

If you are not already talking to employers about data protection, there as a few simple steps to begin a dialogue. There are several ways you can get more information about an employer's policies and begin the discussion:

- Ask to speak to the employer's data protection officer. This person can be your ally. Engage with them in a friendly manner to understand the organisation's data protection policies and how your members' data is being used. GDPR makes provisions for representatives of data subjects (i.e., the employees) to be consulted on data protection matters.
- If the employer does not have a data protection officer, ask them to justify why (see page 9 for details of when required and art. 37-39 of GDPR).
- Propose that the topic be included in the workplace's information and consultation procedures, for example at a works council.
- Ask the management to provide you with a complete mapping of technologies that process workers' data, and to provide you with the complete documentation, i.e. how these systems work, and how workers' personal data is processed. This should include any data protection impact assessments relevant to workers' data.

Article 40

- Ask if the employer is signed up to any sectoral codes of conduct under GDPR.

Asking the right questions

When an employer seeks to inform or consult the union about some aspect of data protection, it is important to understand the basics of GDPR and know the right questions to ask. The information in this publication will give you an understanding of the key terminology and principles, as well as how they are applied to the workplace. Some employers may try to hide behind jargon or assumed ignorance to circumvent consultation with unions. Do not worry if you do not understand every detail of data protection policy. When an employer informs the union about a data protection issue, start by asking some basic questions. This will show the employer you know what you're talking about and get you important information with which to begin a discussion.

In case of new technology that processes workers' data, or a change to the firm's data protection policy, ask:

- What data will be collected, where will it be stored, for how long and how will it be used?

Article 4

- Will personal data be collected? If the employer claims it won't, ask what steps are being taken to pseudonymise (anonymise) the data so it cannot be used to indirectly identify individuals. Refer to article 4 of GDPR.

Article 5

- What is the legal basis for processing of any personal data?
- How will workers' rights under GDPR be guaranteed?

Articles 12-13

- Will a data protection impact assessment be done? If not, why not? For data processes that affect people's rights and freedoms, this is a legal obligation. See page 9. Article 35 section 9 of GDPR provides for consultation with data subjects or their representatives as part of this impact assessment. This should include the trade union.

What to do if…

…an employer introduces a new data protection policy

- Demand to be consulted and ask the right questions (see above) .
- Liaise with the data protection officer.
- Ask how workers' data subject rights will be guaranteed.

…an employer introduces a system for monitoring and/or geo-tracking workers

- Employers must inform employees and provide information about what data in being collected.
- They must prove that the measure is appropriate and protects employees' fundamental rights and freedoms.
- Demand a data protection impact assessment (DPIA) and ensure the union is involved (see page 9). The employer must carry out a DPIA where workers' location is being monitored (geo-tracking).

…an employer wants to use artificial intelligence and/or automatic processing of workers' data

- Workers have a right not to be subject to decisions based solely on automatic processing which would have a significant effect on them, including profiling (see page 9 on profiling). **Articles 13-15**
- Since this kind of processes implies a high risk, employers should carry out a data impact assessment (DPIA).
- Demand to know how workers (or job applicants) can exercise their right to contest any decision.

…union members raise concerns about how their data is being used

- Approach the data protection officer.
- Ask to see the data protection impact assessment. If there isn't one, ask why not and request written justification from the time the decision was made.
- Support workers to exercise their rights to be told what is done with their data (articles 13-14) and request a copy of their data (article 15). **Articles 13-15**
- Inform workers about their right to rectify incorrect data (article 16) and restrict data processing (article 18) if they believe the data is incorrect, or to object to processing (article 21) if performed with the justification of legitimate or public interest (see page 10). **Articles 16, 18 & 21**
- Workers also have the right to request erasure of their data (article 17) if the information is no longer needed for the purpose for which it was collected. **Article 17**
- Raise data protection concerns with management in the usual consultation forums.
- Propose joint guidelines or an agreement on data protection or that it is included in collective bargaining negotiations.

Remember! Don't take the employers word for granted on data protection matters. Ask questions and speak to your union's lawyers with specific legal concerns.

GDPR – Key Facts

GDPR applies to anyone processing data about EU residents

GDPR safeguards the data of anyone resident in the EU and applies to organisations throughout the bloc. If a company, for example, collects data about EU residents or offers services in the EU but then processes it elsewhere, it is still bound by GDPR rules. This means that if an employer uses a third-party HR platform or software to monitor employees based outside the EU, they must still follow GDPR.

The rules are based on broad principles

Article 5

GDPR's rules are based on seven principles, set out in Article 5 of the regulation. Because these need to be taken under consideration when making decisions about data processing, it is worth knowing them. Employers should also follow these principles in how they deal with data. Unions can reference them when consulted about a firm's data protection policies or when asking questions of employers about their data protection practices.

These principles are:

- **Lawfulness, fairness and transparency**
  The reason for collecting data must follow one of the regulation's lawful bases (see pages 9-10). Fairness means treating people reasonably and not deceiving them in order to collect their data. Transparency pertains to what data is collected, why and by whom.
- **Purpose limitation**
  Data must be collected for an explicit and legitimate reason and should only be processed as is needed to fulfill that purpose.
- **Data minimisation**
  The collection of personal data should be kept to the minimum of what is needed to achieve the stated purpose.
- **Accuracy**
  Information should be kept up to date. It is the responsibility of the organisation holding data to proactively ensure this and to rectify any errors quickly.
- **Storage limitation**
  Data should only be stored for as long as needed.
- **Integrity and confidentiality**
  Information must be held securely and everything done to ensure that no unauthorised person can gain access.
- **Accountability**
  The organisation collecting the data is ultimately responsible (and liable) for following the rules set out by GDPR.

GDPR Jargon: a little knowledge goes a long way

As in any area where a union negotiates with an employer, it is helpful to know key terms around GDPR. The list below sets out definitions for the most common terms used in the legislation. Understanding them helps trade unionists to ensure GDPR compliance within the union and, importantly, to ask the right questions when employers use this jargon to talk about data protection.

- **Personal data** – Any data about an individual or that may reasonably be used to identify an individual.
- **Data processing** – Anything you may do with data, including collecting, storing, analysing and transmitting.
- **Data controller** – An individual or organisation that determines what, why and how data is processed. The data controller is responsible for defining the purpose of data processing and gaining consent, if that is the relevant legal basis. Unions and employers are both data controllers. Both may also be data processors, see below.
- **Data processor** – An individual or organisation that deals with personal data, for example managing a membership database or administering employment records. This may be done in-house or contracted to a third party. Where this is the case, for example when an employer uses an external HR firm, there must be a contract with clear data protection provisions in place. Data processors must keep records and enumerate their responsibilities under GDPR.
- **Data subject** – An individual to whom personal data relates.
- **Data protection officer (DPO)** – The person responsible for data protection in an organisation who ensures compliance with GDPR. Certain organisations must have a DPO, for example public authorities. Specific rules are set out in national legislation, however DPOs are mandatory if an organisation's core activities include the systematic monitoring of data subjects or the processing of special categories of data (see below). **Articles 37-39**
- **Data protection impact assessment (DPIA)** – An analysis of the grounds for collecting personal data and the effect that it would have on individual's rights. A DPIA should be conducted when people's rights and freedoms may be at risk, for example when someone could suffer economically, like losing their job. National data protection authorities provide lists of when a DPIA is necessary. **Article 35**
- **Special categories** – Certain types of personal data are afforded special protection by GDPR. These include racial or ethnic origin, political opinions, religious or philosophical beliefs, and sexual orientation. Importantly, **trade union membership status is considered a special category** (more information on page 4). **Article 9**
- **Codes of conduct** – Voluntary agreements covering how GDPR obligations are implemented in a certain sector. These can be drafted by trade associations or other bodies representing groups of data controllers. They must be approved by national or European data protection authorities, at which point they become binding on the signatories. **Article 40**
- **Profiling** – automatic processing of personal data in order to evaluate a physical person. HR software to evaluate employees' performance would be one example. Workers have the right not to be subject to decisions based solely on automatic processing. **Article 22**

Six reasons for legally processing data

Anyone processing personal data must have one of the six reasons set out in GDPR, set out in article 6. These are sometimes called lawful bases. For data processing to be legal, it must be covered by one of these. Special provisions apply to sensitive categories of personal data (see page 6). **Article 6**

- **Consent of the individual** – The person whose data is being processed has agreed to it. Sometimes people think this is the only lawful way of processing data under GDPR. However, this is not true.
- **Performance of a contract** – In order to carry out provisions of a contract. You do not need to get consent on top of the contractual agreement. For example, processing

personal data about a member may be necessary to fulfill a union's contractual obligation to represent them.

- **Compliance with a legal obligation** – When the law requires data to be processed. For example, an employer might collect data on his employees on behalf of the national tax authority
- **Vital interests of a person** - When someone's life is at stake. For example, emergency workers may need to access an unconscious person's medical records. Although if a person can consent, this should be sought before doing so.
- **Public interest** – This generally covers the activities of the justice system, government and parliaments, as well as historical and scientific research.
- **Legitimate interests** – Where an organisation has a reasonable and legitimate interest in processing the data. The interest must be clearly identified, its importance assessed and weighed against less intrusive ways of achieving the same result. GDPR mentions employee and client data as cases where legitimate interest can be invoked. However, the reasons and decision-making process for this should be well documented and justified.

More information and useful links

You can access the text of GDPR in all EU languages on the European Union's website. Don't hesitate to check the articles referenced in this toolbox. It will help you become more familiar with the legislation.

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504

All EU national supervisory authorities are listed, with their contact information, on the website of the European Data Protection Board.

https://edpb.europa.eu/about-edpb/about-edpb/members_en

Access Now, a digital rights organisation, has published a short introductory guide to GDPR rights and how to exercise them. It contains practical information about requesting personal data being held on you and how to launch a complaint.

https://www.accessnow.org/cms/assets/uploads/2018/07/GDPR-User-Guide_digital.pdf

The European Federation of Public Service Unions has also published a useful trade union guide on GDPR.

https://www.epsu.org/article/epsu-guide-general-data-protection-regulation-gdpr-now-released

IndustriAll European Trade Union has a position paper on artificial intelligence which deals with the protection of workers' data when AI and machine learning are used in the workplace.

https://news.industriall-europe.eu/documents/upload/2022/6/637897670199433879_dopted%20-%20All%20eyes%20on%20AI.%20Artificial%20Intelligence%20as%20a%20challenge%20for%20workers%20and%20their%20representatives%20-%20EN.pdf

The European Trade Union Institute has published a paper on using GDPR to improve working conditions on digital labour platforms. It also provides a good information about sectoral codes of conduct.

https://www.etui.org/publications/using-gdpr-improve-legal-clarity-and-working-conditions-digital-labour-platforms

The Labour Research Department, a British trade union research organisation, has published a guide on GDPR. It provides useful information for trade union around Europe and specifically in the UK. There is a cost to download the publication.

https://www.lrdpublications.org.uk/securepdf_dl.php

industriAll
EUROPEAN TRADE UNION

news.industriall-europe.eu

FRIEDRICH EBERT STIFTUNG
Competence Centre Future of Work

www.fes.de