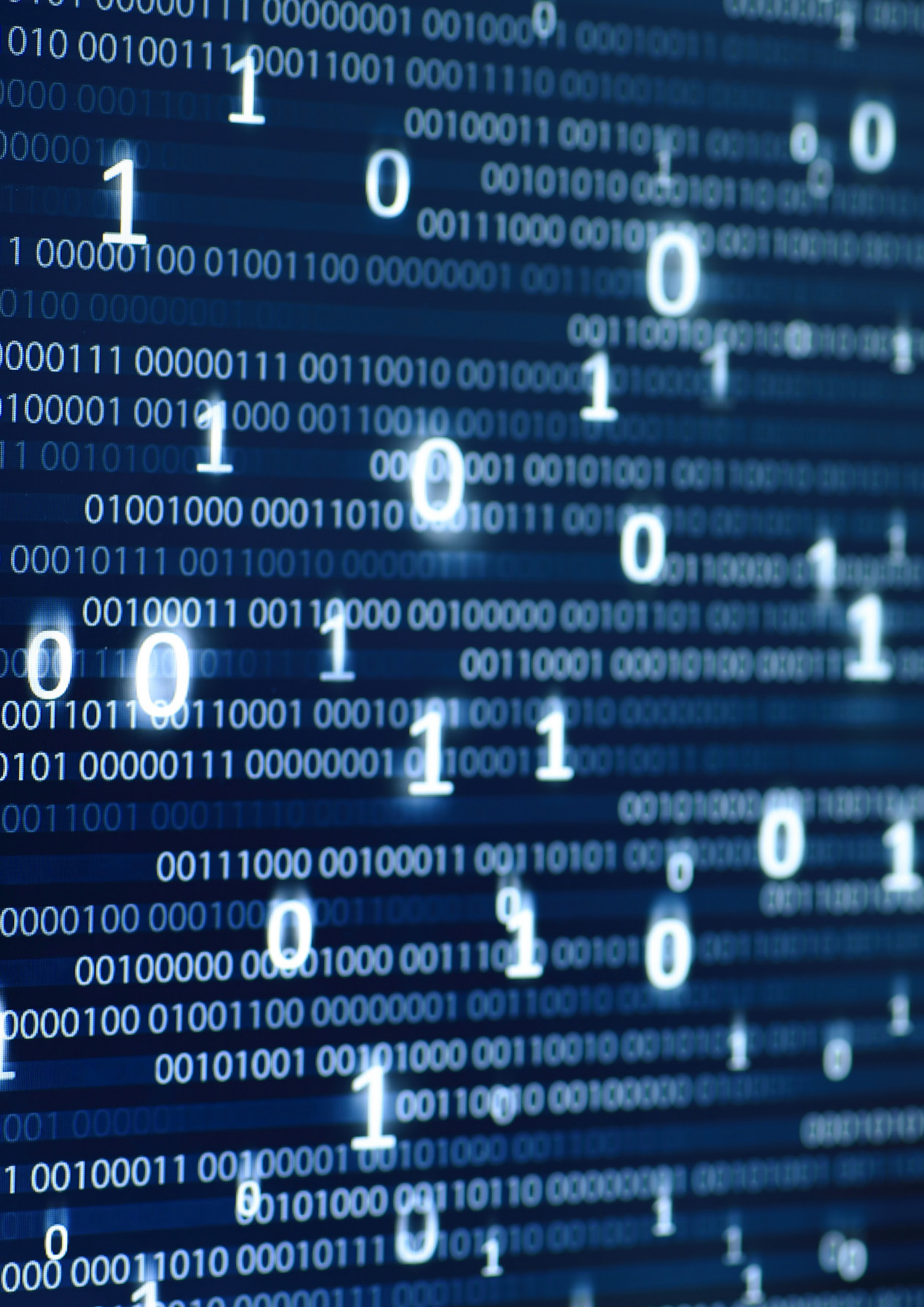
EPSU
EUROPEAN PUBLIC SERVICE UNION

The General Data Protection Regulation (GDPR)

AN EPSU BRIEFING



Foreword

The new General Data Protection Regulation (GDPR) came into force on 25 May 2018. For EPSU, data protection, privacy and cybersecurity in our public services and in trade unions are among the biggest regulatory issues we face. Public service workers and trade unionists can use the introduction of the GDPR as a way to improve how we deal with personal data and workers' privacy. Public services providers are using more and more data to perform their duties. Workers from the health care sector process and analyse sensitive data and have access to medical records. Public administrations also process large sets of personal data.

For this reason it is essential that trade unions use the new GDPR rules to the fullest extent for a more effective protection of workers' and citizens' data.

Compliance with the GDPR entails administrative and technical challenges. Since the entry into force of the new regulation, EPSU has been advocating full involvement of workers organizations in the implementation of the GDPR at all levels, in particular, to ensure workers' privacy. Our actions are aimed at ensuring that GDPR compliance does not create additional burdens for workers in applying and implementing data protection policies or lead to a shift of responsibility to them.

Employers are responsible for ensuring compliance, especially in cases of breaches of privacy. The entry into force of the new regulation can represent a change to the way they work. For this reason our role as trade unions is fundamental: workers need to be informed about their rights and responsibilities when they are data collectors and processors and more aware of their rights as data subjects.

This guide examines the GDPR from three different perspectives: the impact on workers, on public services as well as on trade unions. The last part is devoted to how we can ensure compliance in our trade unions.

We hope that this guide is a useful introduction to the issues raised by GDPR.

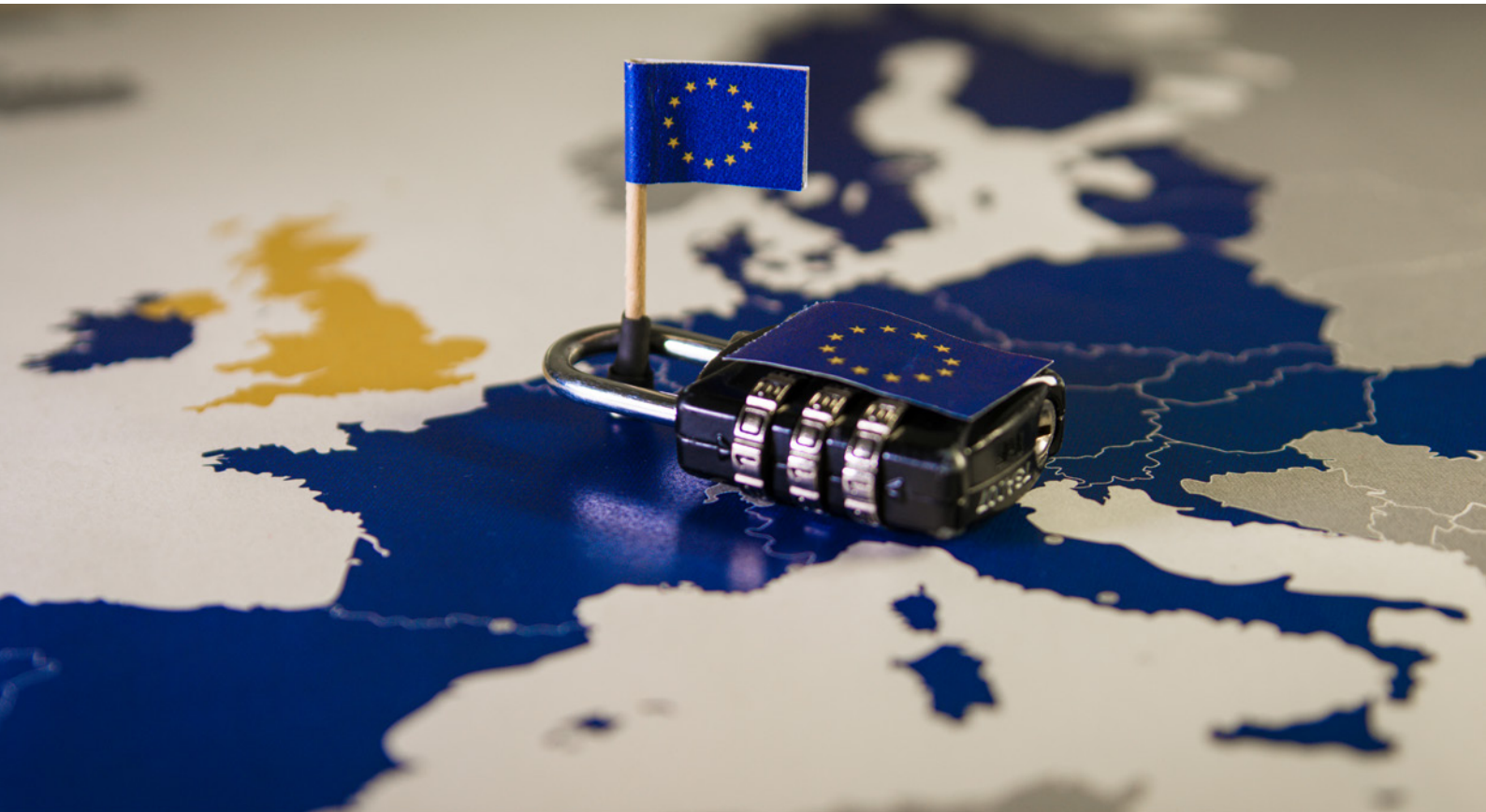
This guide has been developed by Paul Reuter.

Revisions from Aida Ponce, ETUI.

Supervision and Guidance from Luca Scarpiello, Penny Clarke, Richard Pond.

A huge Thank You to our affiliates and everyone who helped and contributed to this GDPR-related guide.

CONTENTS




33.2.55.33
Innovation
Branding
Solution
Marketing
Analysis
Ideas
Success
Management
Technology
Innovation
SYSTEM
0101010001001
100 00 010100
01 101000 001
100 00 010100
100 00 010100
0101010001001
60.50.3.1
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
Oct
Nov
Dec

Obligations and rights under the GDPR

What's new in the GDPR

This guide will consider the impact that the GDPR has on how this personal data[1] is collected and processed, how it is kept safe, how compliance is guaranteed, who is liable for what and what rights a citizen has. Member States have the right to pass further provisions in some aspects but information on the national implementation of the GDPR should be obtained from national data protection authorities.

The GDPR differentiates between data controllers, data processors and data protection officers (DPO).

The Data Controller and Data Processor

In general terms, the data controller the natural or legal person (could be a company or a non-profit organisation), public authority, agency or other body which, alone or jointly with others, the purposes, conditions and means of processing personal data. In other words, the controller owns the data and sets the rules how it is to be collected and processed. The controller therefore keeps a record of all processing activities and furthermore designates one or more data processors that can, in the name of the data controller, collect and process the data.

However, this distinction does not always clearly apply in practice, although it has existed in previous data protection regulations, and the status of employees of data controllers is still disputed. According to the UK data protection authority an employee of a data controller cannot be considered as a data processor[2], which would suggest that he or she is a data controller. However, if the same processing activities would be outsourced (e.g. to an external consultant), this external party would be considered as a data processor. The GDPR lacks a crucial point in the definition, which has implications for liability and responsibility.

---

[1] For the purposes of the GDPR, personal data means any information relating to an identified or identifiable individual. An identifiable person is one who can be identified, directly or indirectly, by reference to an identification number or one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity (such as name, date of birth, biometrics data, fingerprints or DNA).

[2] Information Commissioner's Office. "Data controllers and data processors: what the governance implications are." June 5, 2014. Accessed July 25, 2018 https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf p. 4.

The Data Protection Officer (DPO)

The Data Protection Officer has the role of ensuring that the organisation is processing personal data in compliance with GDPR rules. It has to be designated on the basis of professional qualities and knowledge of data protection law and practices. In some instances, the data controller has an obligation to appoint a data protection officer. This is the case if:

- the processing is carried out by a public authority;
- the core activities of the controller or the processor require "by virtue of their nature, their scope and/or their purposes, regular and systematic monitoring of data subjects on a large scale" (Art. 37, (1) b); or
- the core activities of the controller or the processor consist of processing, on a large scale, special categories of data or personal data relating to criminal convictions (see special categories of data).

However, national legislation might specify further cases where there is an obligation to appoint a DPO. In Germany, for instance, every organisation needs to appoint a DPO if there are more than 10 people constantly involved with automatic processing of data. If the DPO is to be a member of staff, then the works council has a right of co-determination. In general, it is strongly advised to appoint a DPO even if it is not an obligation.

The DPO's main task is to advise the controller and processors about how to comply with the regulation. In particular, the DPO's roles are to:

- inform and advise the employees of the data controller or processor on their obligations arising from the GDPR and any other national data protection rules;
- monitor compliance with the data protection legislation;
- check if the responsibilities of the controller and processor have correctly been assigned, and if awareness-raising and sufficient training for staff have taken place;
- provide advice on the data protection impact assessment and monitor its performance;
- cooperate with the supervisory authority, and to act as a contact person for them; and
- be available for inquiries from data subjects (individuals whose data the controller possesses), for issues of data processing or where individuals want to make use of one of their rights (these will be discussed later).

Data protection officers can work for several organisations as long as they remain "easily accessible". Furthermore, they can be a member of the staff or fulfil their tasks on the basis of a service contract.

DPOs also enjoy specific rights such as to have sufficient resources to fulfil the tasks assigned to them. They also have the right of access to the entities' data processing personnel and operations and to training in order to "maintain their expert knowledge". Moreover, data protection officers should have significant independence in carring out their tasks and reporting to the highest management level. They can also fulfil other tasks as long as there is no conflict of interest with their role as DPO. Many of the tasks that are assigned to the data controller (e.g. documenting processing activities etc.) can hence also be assumed by the DPO. Lastly, DPOs enjoy a high level of job security. They

cannot be fired, nor can penalties be imposed on the ground of performing their responsibilities as a DPO. There is no length of tenure for this position.

This has financial and staff implications for public authorities as well as companies and organisations who process a large amount of data, which may be reduced by appointing one DPO for several organisations.

How should data be processed?

The regulation sets out seven guiding principles on how data can be collected and on which legal basis the processing can take place. These principles can help an employee understand if the data their employer holds on them or on any other data subject is rightfully collected and processed. As the Bărbulescu v. Romania case shows, employees can rely on these principles if an employer violates their privacy.[3]

Guiding principles of data protection

1. Lawfulness, fairness and transparency

The reason to collect data needs to be established on a legal basis. The GDPR provides several grounds, such as processing based on consent, public interest or legitimate interests. These different legal grounds will be discussed in the next section.

The principle of fairness applies which means that data should be handled in a way that people would expect to be reasonable. This includes how data has been collected. If somebody has been deceived to obtain their data, the data controller is in breach of the principle of fairness.

One needs to be transparent for example, about which data is collected, for what purpose, for whom and for how long it will be kept. This information needs to be written as clearly as possible in an easily understandable language. For more information see the section on individual rights.

2. Purpose limitation

Personal data shall be collected for specified, explicit and legitimate purposes and cannot be further processed in a way that is incompatible with those purposes. At least one of the reasons that are mentioned for the collection of data must be fulfilled in order to be allowed to start the processing. This means that in the context of employment the data controller (in this case the employer) needs to specify for which purposes the data on the employee is collected. Some other special conditions might apply in the employment context[4].

However, in some instances the data can still be processed for new purposes if those are compatible with the original one (e.g. archiving in the public interest; scientific or

[3] European Court of Human Rights – Grand Chamber. CASE OF BĂRBULESCU v. ROMANIA. September 5, 2017. Accessed on July 30, 2018 http://hudoc.echr.coe.int/eng?i=001-177082

[4] Cfr. in other chapters

historical research; and statistical purposes), providing that the data subject gives consent for the new purpose or there is a new legal provision that requires processing or allows it in the public interest.

3. Data minimisation

Personal data should be adequate, relevant and limited to what is necessary. The minimum amount of personal data that are needed for processing should be identified, before any data collection takes place. The data should therefore be adequate or sufficient, relevant or with a clear link with the purpose and limited to fulfil the purposes for which they are processed.

For example, an employer may collect data on the blood type of his employees who do hazardous work because this information might be relevant for health and safety measures, even if it is unlikely to be needed. However, if the employer decides to collect data on the blood type of employees not doing hazardous work, this would constitute a breach of the principle of data minimisation.

4. Accuracy

The data needs to be accurate and kept up to date. There is an obligation on the data controller to proactively ensure the accuracy of data and if any of it is inaccurate, incorrect or misleading, then to either delete or rectify it without delay. In some cases the controller can rely on demands from data subjects, for instance if they want their address to be updated in the database. In others, for example when an employee receives a pay rise, his or her payroll records will need to be updated.

5. Storage limitation

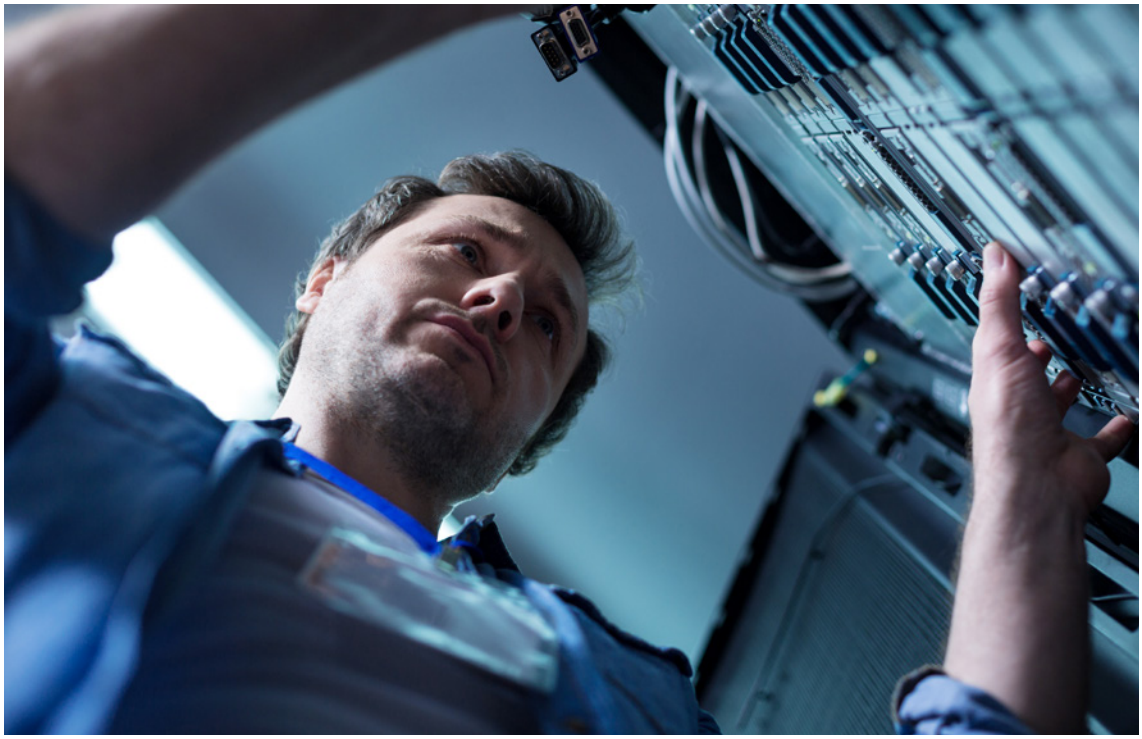
Personal data should be kept for a determined period of time and no longer than necessary. When the purpose for keeping the data is no longer relevant or it is out of date the data should be deleted or anonymised. This principle prevents data from becoming irrelevant, excessive, inaccurate or out of date and encourages controllers to set policies on retention limits

6. Integrity and confidentiality

Personal data should be kept secure. Appropriate measures need to be taken to ensure the security of the data, including protection against unauthorised or unlawful processing, and against accidental loss, destruction or damage (see sections on data security).

7. Accountability

The accountability principle makes the data controller responsible and therefore accountable for compliance with the GDPR, putting in place all necessary measures, such as the implementation of a privacy management framework.



Lawful basis and limits to processing personal data

To collect and process data, the controller must rely on a legal basis which implies different obligations. It is therefore helpful to be aware on which basis the data are collected.

Consent of the data subject

To be allowed to collect and process personal data, the data controller can use consent of the data subject to process his or her data for one or more specific purposes. It should be made as easy as possible to give and to withdraw consent. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters. This shall be done in an intelligible and easily accessible form, using clear and plain language. This means that ticking a box suffices to be considered as an active consent to data processing. However, the box should not be pre-ticked. The form should also specify if any third party could be allowed to process the data and that the person has the right to withdraw consent at any time.

Evidence of the consent needs to be kept to show to whom, when and to what a person has consented. Since consent must be given freely, making it a precondition for the provision of services is a breach of the regulation. For example, if a service provider makes consent to collect unnecessary data a precondition for providing the service then this is seen as an act of coercion of data subjects. Hence, in the context of employment or public service provision, where power relations are evident, the use of consent as a legal basis is not advised, since it could be regarded as unfair.

Explicit consent has to be obtained in situations where serious data protection risks emerge: on the processing of special categories of data; in the absence of adequate safeguards on data transfers to third countries or international organisations, and when there are decisions taken by technological means without human involvement (automated individual decision-making and when there is profiling.

Performance of a contract

Processing can also be allowed if it needs to be done to fulfil the purposes of a contract or if the person asks to take preliminary steps before entering a contract for which data must be collected. For example, if somebody asks for a quote for, the data controller does not have to ask for consent to process the data.

The contractual basis does not have to be in written form.

Compliance with a legal obligation

If the process is necessary to comply with a legal obligation in national or EU law then consent is not necessary. For instance, an employer might be obliged to collect data on his employees on behalf of the national tax authority. In this case, the employer would need to document what this legal basis might be. Referring to a government site that explains the obligation would be considered sufficient proof.

Protection of vital interest

When the life of a person is at stake, one is allowed to process his or her data. This applies in particular to emergency services, where medical records are needed to protect the person's vital interests. However, if the person is still able to provide consent, vital interest cannot be used as a basis for processing.

Legitimate interest

Legitimate interest is where one needs to show that the controller or a third-party has a legitimate interest to process the data and that there is no other, less intrusive way to achieve the same result. However, such interests cannot override the fundamental rights or freedoms of the data subject.

There are three steps to consider if one wants to use legitimate interests as a lawful basis. First, one should ask what these legitimate interests could be, how important they are and who benefits from them? Secondly, one should ask if there is no less intrusive way to achieve the same result. Thirdly, one needs to balance the interests. This part addresses questions such as: whether people would expect you to use their data in this way; whether you are happy to explain it to them; and whether some people are likely to object or find it intrusive. The results of these tests should be documented to show compliance upon request. For example, in the UK the Information Commissioner's Office or the Data Protection Network provide some guidance on how to carry out such a test.

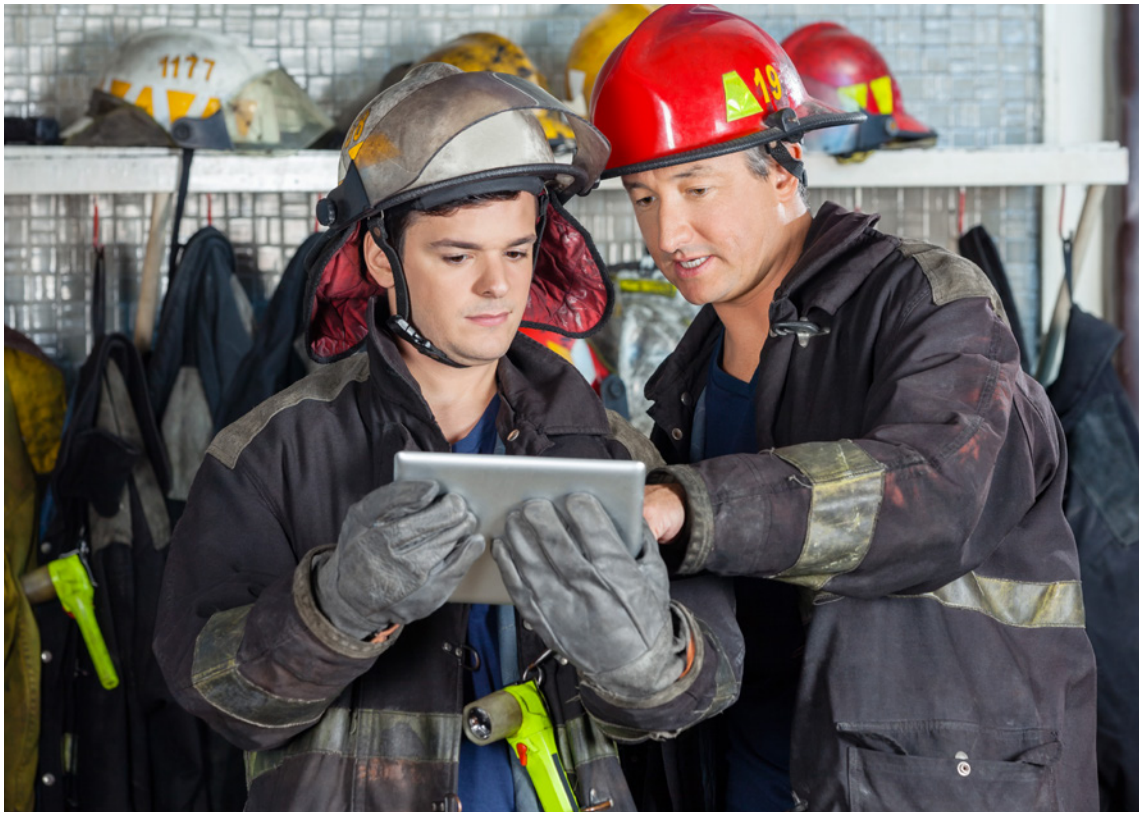
The GDPR specifically mentions employee or client data as one of the cases where data controllers can invoke legitimate interests.

Processing special categories of data

The processing of special categories of data is prohibited unless there are specific grounds for doing so. This covers data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as the processing of genetic data, biometric data for the purpose of uniquely identifying a person, data concerning health or data concerning a person's sex life or sexual orientation.

The processing and collection of special categories of data is only allowed under special conditions:

- if no other national or European Union law prohibits the data subject from giving its consent to the collection of special categories of data, he or she can agree to it;
- in the context of employment or social security law, as long as national or European Union law or a collective agreement safeguards the fundamental rights of the employee;
- to protect the vital interests of the data subject or another subject if incapable of giving consent;
- if processing is carried out in the course of legitimate activities of foundations, associations or any other not-for-profit bodies with a political, philosophical, religious or trade union aim. However, the data can only relate to members, former members or persons who are in regular contact with the organisation and when it is in connection with its purpose. These data must not be disclosed outside the organisation without the consent of the data subject;
- when the special categories of data are made public by the data subject;



- when the processing is necessary for the establishment or exercise of legal claims;
- "For the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services." (Art. 9 (2), h) However, the processor must in this case be subject to professional secrecy; or
- when processing is necessary for substantial public interest.

Some Member States have chosen to go beyond the GDPR definition of special categories of data and have imposed additional restrictions to its processing.

Processing data on criminal offences

Processing of data concerning criminal convictions or offences can only be carried out if it has a legal basis and if it meets one of these conditions:

- the processing takes place under official authority, or
- "when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects."

However, no register of criminal convictions or offences can be kept by a private entity.

Processing in the context of employment

Employment constitutes a specific situation for processing personal data. By law or by collective agreement more specific rules to ensure the protection of "the rights and freedoms in respect of the processing of employees' personal data in the employment context might be taken. This could be the case in particular for the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, protection of employer's or customer's property and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship." (Art. 88)

A key aspect is to "safeguard the data subject's human dignity, legitimate interests and fundamental rights, with particular regard to the transparency of processing, the transfer of personal data within a group of undertakings, or a group of enterprises engaged in a joint economic activity and monitoring systems at the work place."

These rules could, for instance, cover monitoring at workplace or geo-tracking. If a Member State takes some measures in this context, it has to communicate them to the European Commission in order to ensure that the new rules are compliant with the current regulation. According to the Austrian private service trade union, GPA-djp, so far only Belgium, Germany, Latvia, Slovakia and Hungary have used this opening clause.[5] However, trade unions also have the possibility to take additional measures by collective agreement at company level.

In general, if a company has any monitoring provisions, the employer must inform the employee of its existence and they need to prove that it is an appropriate measure that ensures a balance with the fundamental rights and freedoms of employees.

[5] Clara Fritsch. *Die Europäische Datenschutzverordnung*. 2nd ed. Vienna, Austria: GPA-djp, Mai 2018.

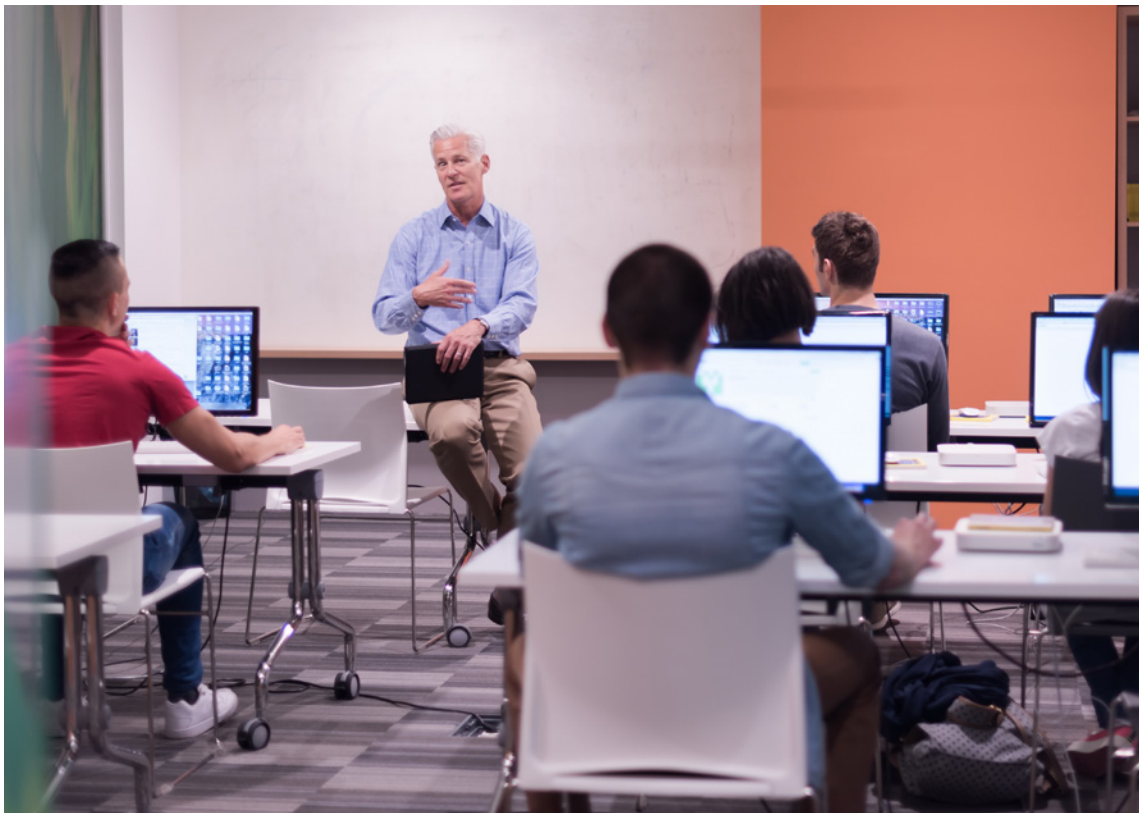
Individual Rights of data subjects

The GDPR provides eight clear individual rights which data subjects exercise and which controllers have to respect.

1. Right to be informed

Data subjects have the right to be informed in a transparent manner about what personal data are being collected and processed. The data controller needs to provide information on which data are retained for which purpose at the moment when the data are obtained (e.g. providing all relevant information when somebody registers through a form). This should be done in a precise, transparent and easily accessible way. The information should be written in plain language. The data subject can file a request for additional information that needs to be processed within a month. The reply needs to state for which purpose and how long the data will be stored, as well as who will have access to it (including any third parties). Furthermore, the data subject needs to be informed that he or she has a right to access, rectify, erase or restrict the processing of his or her data, or to object to processing and a right to data portability.

If there is a change of purpose for the collected data, the data controller needs to inform the data subject of the change before any processing can take place.



2. Right to access

Data subjects have the right to obtain a copy of their personal data and other supplementary information related to it. Requests can also be filed to access the collected data at reasonable intervals of time.[6] The reply should be free of charge and should include:

- the purpose of the processing and the categories of personal data concerned;
- the recipients or categories of recipients to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
- where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
- the right to lodge a complaint with a supervisory authority;
- where the personal data are not collected from the data subject, any available information as to their source; and
- the existence of automated decision-making, including profiling and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

[6] One can for example not ask every week to access his or her data.

3. Right to rectification

Data subjects have the right to request the rectification of their personal data or to have it completed. The data controller has the obligation to respond without undue delay or within a month of the receipt of the request. This period of time can be extended by two months if the request is complex. It is important to take into account that the data controller must provide the data to the data subject free of charge.

4. Right to erasure

Data subjects have the right, under special circumstances to have their data erased or the 'right to be forgotten'. This is the case where:

- data are no longer related to the purpose for which they were collected or processed;
- the data subject withdraws his or her consent (if the legal ground for processing was consent);
- the data was unlawfully processed;
- the person objects to the processing and the controller cannot demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject (if legitimate interests were used as legal ground for processing);
- the person allowed the collection of data when he/she was a child (in general defined as being under 16 years old, however this depends on national legislation).

The data controller has to act upon request without undue delay and has one month to respond or up to three months if the request is complex.

The right to erasure does not apply if processing:

- concerns the right of freedom of expression or information;
- is necessary to be compliant with other laws;
- is in the public interest;
- concerns public health;
- is needed for the establishment of a legal claim; or
- is done for archiving purposes in the public interest.

The right to erasure is hence conditional. For example, Google might decline a request to delete an article where you no longer agree with your original statement of consent, since they believe that their legitimate grounds override your rights and freedoms.

5. Right to restrict processing

Data subjects have the right to request the restriction or suppression of their personal data. This right limits the way that the controller can use the data. This can apply when accuracy of data is contested and the data subject might ask to restrict access for a period in order for the controller to verify its accuracy; in cases of unlawful processing the data subject can oppose the erasure and ask instead for a restriction of access. In cases where it is not clear that the legitimate ground for the processing by the data processor overrides the interests of the data subject (if legitimate interests were used as legal ground for processing), the data should be restricted during the verification of the claim.

The data controller can implement various measures to restrict data, for example by moving it for a certain period of time to another reprocessing system or website or by making it unavailable to other users or viewers. The data controller has one month from the receipt of the request to comply with it.

This right should not be confused with the right to rectification and objection, although there are some linkages.

6. Right to data portability

Data subjects have the right to move their personal data easily from one controller's IT system to another. This means that they have the right to receive their personal data in a structured and secure format that is commonly used to be read by another machine or in an interoperable format and to transmit it to another data controller without hindrance from the first. However, this only applies if the first data controller relied on consent or the performance of a contract as a lawful basis and if the processing is carried out by automated means. The exercise of the data portability right requires technical feasibility, that the IT systems and processes of the controllers are able to export and receive the data. The data controller has one month from the receipt of the request to comply with it.

This right helps the free flow of data and assists individuals in switching, for example, between telecom providers or applications such as iTunes or Spotify, taking with them their data and history. It could allow, for instance, platform workers (e.g. an Uber driver) to get a copy of their data and get it transferred to another controller (or service platform), if it is technically feasible. If the conditions are met, the data on the "digital reputation" (reviews) could be additional personal data that can be transferred.

7. Right to object

Data subjects can, under certain circumstances, object to and stop the processing of their personal data. An individual can object at any time to the processing of his or her data if it is for direct marketing purposes. This right is not absolute, for example, when the controller relies on public interest or legitimate interests as a lawful basis for processing. The controller may no longer process the data unless it demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject.

When an objection has been received, the controller must stop using and processing the personal data but this does not imply that the data needs to be erased. The data controller has one month from the receipt of the request to comply with it.

8. Rights related to automatic decision making, including profiling

Data subjects have the right not to be subject of automated decision making or of profiling, and have the right to get enough information about the decisions made by automated means (taken without any human involvement) which have a legal impact on them. Practical examples are when an algorithm refuses an online financial loan appli-

cation or in recruitment aptitude tests without human intervention when a system flags employees who have reached a specified number days of sick leave.

Additionally these types of processing include 'profiling' which the GDPR defines as any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movement.

Since this type of processing implies high risks, the controller must conduct a Data Processing Impact Assessment to identify and manage the related risks before implementing an automated decision-making process. Additionally automatic decision making can only be used if the data subject explicitly consented to it, if it is necessary to enter into a contract or if it is authorised by law (e.g. to fight tax fraud). If automatic decision-making concerns special categories of data, it can only be carried out if the data subject has explicitly consented to it or if it is necessary for demonstrable reasons of substantial public interest. It is essential to take into account that in the exercise of this right, data subjects should receive meaningful information of the logic involved in the automated decision-making process. Controllers should take measures to prevent bias, discrimination and errors. The ways to receive meaningful information related to decisions made by algorithms need to be further investigated, as well as concerns related to readability, intelligibility and clarity of the explanation.

Failure to provide information

If the data controller is unable to provide the information to the data subject, they have one month to reply stating the reason for not taking any action. The reply should also inform the requesting person that he or she has the right to lodge a complaint with the data protection authority.

In case a request is unfounded or excessive, the data controller also has the right to charge a fee for providing the information or to refuse the request by further communicating this to the data subject.

Restriction of rights

These rights are not absolute and can be restricted by European Union or Member State law. Some of the restrictions cover primarily the public sector and will therefore be discussed in the next part. In Article 23 the GDPR provides a long list of areas in which a restriction can be implemented ranging from national security and defence to the protection of judicial independence and judicial proceedings.

A major improvement compared to the previous Directive 95/46/EC is the possibility to mandate a not-for-profit organisation to lodge a complaint on the behalf of the data subject. This opens the prospect for collective action against data controllers and processors. Furthermore, since the complaint will be treated at the national level, most collective lawsuits will probably be processed in the Member States with more advantageous collective action rules.

Data security

Data privacy and security are interlinked and security needs to be systematically built into and implemented in the organisation. There is a need for physical security in the premises, workstations, video-surveillance cameras, etc and security of the systems, including the internal network, mobile equipment, servers, websites, etc.

Data protection by design and by default

These are two principles in the GDPR and both responsibility of the data controller. *Data protection by design* is about the capacity to apply technical and organisational measures, including an ethical dimension, appropriate and effective to ensure privacy.

The European Data Protection authority clarifies that processing of personal data, partially or completely supported by IT systems should always be the outcome of a design project.

Data protection by default requires the controller by default, to collect and process only personal data that are necessary for each specific purpose of the processing, in compliance with the law and transparently notified to the data subjects concerned. Hence, data subjects do not have to make 'extra efforts' to protect their own privacy.

Data controllers need to be proactive and preventative and take measures to safeguard data. They should, for example, anonymise data on a technical as well as organisational level and provide permanent protection to personal data. The encryption of personal data and provision of delete functionalities - guaranteeing that the data is only accessible to a restricted set of people - should be taken both at the time of the determination of the means for processing and at the time of the processing itself "by design".

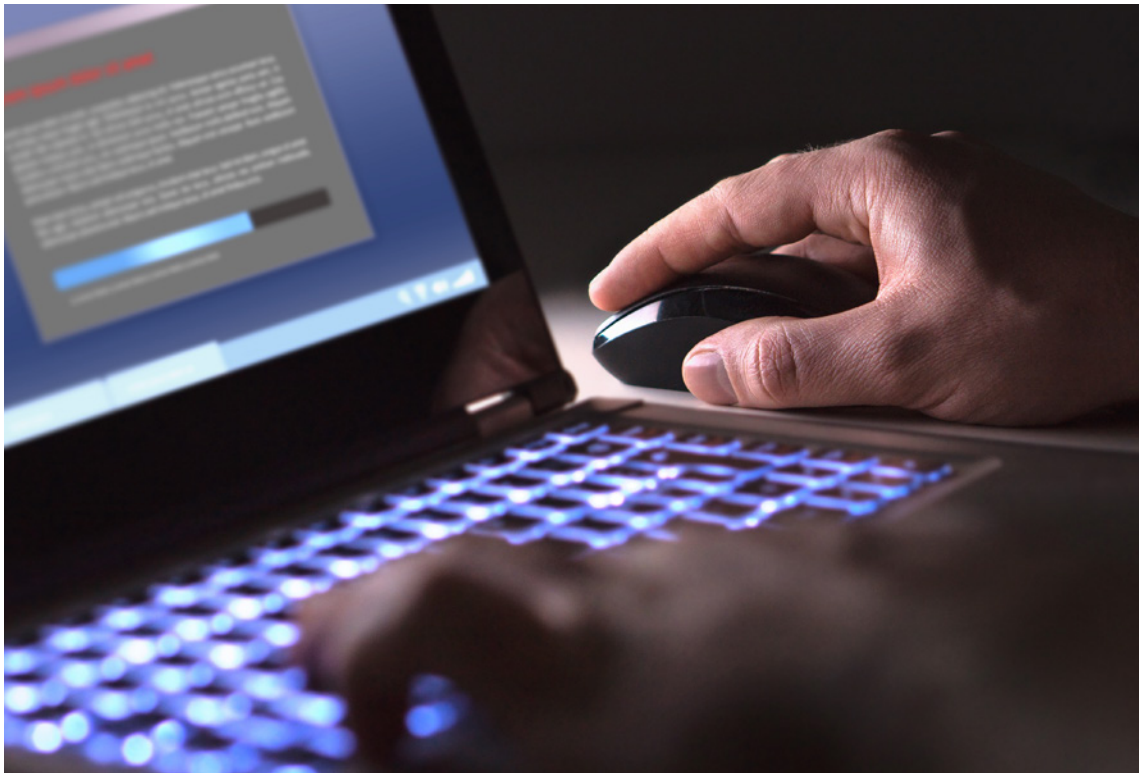
On the organisational level, the controller needs to ensure that all employees dealing with the processing of data receive sufficient information about the risks and have training on the new data protection rules. The seven data-protection principles should provide guidance on which data can be collected.

Data controllers need to be able to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services, and to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident. A process must be put in place for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

The processor and controller should assess the scope, context and purpose of processing and any costs for implementation before implementing new security measures.

Contracts

The data protection by design and default provision does also apply any (third-party) processor. Hence, the data controller should establish a contract with any processor, stating the responsibilities and liabilities of both parties, the legal basis for the data processing and giving guidance about which data can be processed and for which purpose.



Documentation

In case an organisation is employing more than 250 persons, or when the processing is likely to result in a risk to the rights and freedoms of the data subjects, the processing is not occasional, the processing includes special categories of data or data in relation to criminal convictions or offences, the organisation needs to document the processing activities under its responsibility.

While it is best for the data controller to document all the processing activities, safeguard mechanisms, records of consent and location of data etc., the GDPR only provides for some obligations which can be consulted in article 30 of the regulation.

If employees/data subjects want to make use of their rights deriving from the regulation, documentation allows them to get a better picture of what is processed and for which reason.

Data protection impact assessment (DPIA)

This is an important document to issue when there is a high risk to a person's rights and freedoms, including the potential for any significant social or economic disadvantage. Before any processing, the controller shall conduct an assessment of the impact of the envisaged processing operation on the protection of personal data. Furthermore, a data protection impact assessment (DPIA) is necessary if the data controller or processor makes systematic and extensive use of profiling, processes special categories of data on a large scale or systematically monitors publicly accessible places. The national data protection authority shall provide a list of the kind of processing operations for which a DPIA is required. It is crucial for the controller to seek the views of data subjects or their representatives on the intended processing and works and staff councils might therefore want a role in the DPIA process.

The data protection officer should provide advice on how to reduce the risks to data protection. When the data controller identifies a high risk, which cannot be mitigated, he or she has to consult the national data protection authority. The Data Protection Working Party[7] gives some additional guidance when a DPIA is needed and how to conduct it.[8] Guidelines on other provisions can also be consulted on the Article 29 Working Party's webpage.[9]

A DPIA is, for instance, an obligation when an employer wants to introduce geo-tracking technology or to collect data on employees' trade union membership. In general, when (new) technologies or software need employees' personal data for processing, the data controller is advised to conduct a DPIA.

---

[7] The Data Protection Working Party is established by Article 29 of Directive 95/46/EC. It provides the European Commission with independent advice on data protection matters and helps in the development of harmonised policies for data protection in the EU Member States.

[8] Article 29 Working Party Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation (EU) 2016/679, 4 April 2017

[9] Article 29 Working Party "Guidelines", accessed on 18.07.2018. http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1360&tpa_id=6936

Data breach

A data breach is any unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. It can take several forms, ranging from a loss of data (e.g. theft of a computer or mobile phone) to hacking of servers. Under the GDPR every data breach that implies risks to personal rights and freedoms, needs to be reported to the supervisory authority, irrespective to when it took place (e.g. a data breach might be undiscovered for a few months, yet as soon as it is detected it needs to be reported). The terms of employment might specify the procedure on how to act in case of a breach.

Controllers and processors need to develop a security breach response plan and implement policy accordingly. When a data breach happens, the employee, data subject, data processors and data protection officer need to immediately (within 72 hours) inform the controller as soon as they detect the breach, independent of the scope of the breach. The controller must then assess the severity of the breach and might need to inform the supervisory authority and the data subjects whose data have been compromised.

The latter can also be done by a public announcement if it is too complex to reach out to every data subject. If the responsible authorities are not notified within 72 hours, the data controller needs to provide a reasonable justification (e.g. disruption to regular business operations etc.) for the delay.

The notification to the supervisory authorities and affected data subjects should include which data have been accessed, how many people are concerned by the breach, the name of the data protection officer, what the possible consequences could be, and what will be done to mitigate the breach.

Ensuring compliance

There are several ways for data controllers to improve compliance by adopting additional safeguards.

Codes of conduct

The GDPR provides the possibility for associations or other bodies representing categories of controllers or processors to conclude sectoral codes of conduct which can apply on national and, if needed, on European level. Organisations that are established outside the EU can also choose to adhere to a code of conduct on a contractual and binding basis.

The codes of conduct need to cover the GDPR rules to ensure compliance with the regulation and can introduce additional restrictions if the sector covers "high risk" data. The draft code of conduct needs to be sent to the supervisory authority which will provide an opinion. If sufficient measures have been taken to safeguard data protection it will approve and publish the code of conduct. If it concerns several Member States this role should fall to the European Data Protection Board[10].

Binding corporate rules

Companies can agree on internal binding corporate rules, which apply to every entity of the company. These rules are in general drafted by the employer and only need approval by the supervisory authority. After approval, the company can start to transfer data to their different entities.

Certification

The European Data Protection Board and the national supervisory authorities also have the possibility to accredit certification bodies. Organisations can demonstrate their compliance by adhering to these certificates.

Independent supervisory authority

The powers and competences of national data protection agencies have increased with the new regulation. They can now ban some kinds of data processing or impose fines. Furthermore, cooperation between the different authorities has also been strengthened. Their aim is first and foremost to monitor and enforce the Regulation. See the section on independent supervisory authorities in the GDPR and the Public Sector for further details.

[10] The European Data Protection Board (EDPB) is an independent European body, which contributes to the consistent application of data protection rules throughout the European Union, and promotes cooperation between the EU's data protection authorities. The EDPB is composed of representatives of the national data protection authorities, and the European Data Protection Supervisor (EDPS).

Liability

Fines

The GDPR allows for the imposition of fines of up to 20 million Euro or 4% of the annual turnover of a company. However, this is only the case when the company or organisation repeatedly breaks the law on data protection and is benefiting from doing so. The imposition of fines depends among other things on the severity of the breach, cooperation with authorities, measures taken to mitigate it and number of people affected by it. National data protection authorities will prefer to issue a warning or an order on how to resolve the problem without imposing fines in case of a minor breach of the regulation.

A data subject has the right to demand compensation from the controller or processor for any material or non-material damage.

Data controller

In general, the data controller is always liable for any non-compliance. Under the GDPR the liability can seldom be transferred to the data protection officer, who only assumes an advisory role. However, this is quite controversial. In some instances liability can be transferred to the data processor, while in others both might be liable.

If the controller or processor can prove that they are not responsible for the damage, they cannot be held liable. The 2017 case against the UK supermarket chain Morrisons showed that even in the case of a deliberate data breach by an employee, the employer is liable.[11]

Data processor

Since the processor is the natural person or organisation that processes data on behalf of the controller, the processor is only liable if he or she did not comply with the GDPR on processing or acted outside the instructions of the controller. For contracts, this can, for instance, be the case if he or she used sub-contractors without authorisation from the controller, did not cooperate with the authority, did not ensure the safety measures or did not keep records of processing activities etc.

Joint and several liability

When both the processor and the controller or more than one controller or processor caused the data breaches, each of them is liable for the entire damage. They can nevertheless claim back a part of the compensation from the other processor or controllers corresponding to their share of responsibility for the damage.

Data protection officer

While the GDPR does not state that the data protection officer can be held liable for his or her action, legal opinion is divided on this question. The International Association of Privacy Professionals believes that national laws on data protection that include a criminal liability of DPOs in case of non-compliance are compatible with the GDPR. In Ireland,

[11] Sarah Butler, "Morrisons Found Liable for Staff Data Leak in Landmark Ruling," The Guardian, 1 December 2017, accessed July 17, 2018, https://www.theguardian.com/business/2017/dec/01/morrisons-liable-staff-data-leak-landmark-decision

DPOs can personally be criminally liable if they consent to the violation while in the UK, they are liable if it is proved that they provided false advice.

Thiébaut Devergranne, professor of IT law, deems that even without additional legal grounds, courts might create a civil liability for DPOs.[12] He gives as examples where the DPO might have had knowledge about a problem without reporting it to the controller or was completely incompetent. These would constitute cases of grave misconduct and any protections for the DPO would not apply. Further court rulings on this issue will be needed to clarify liability issues.

Employee

As the data controller is in general liable for any damages, an employee is usually not personally accountable. However, as the Morrisons case shows, when a breach of the regulation happens on purpose, the employee causing the breach might still face a criminal conviction and face dismissal.

Similar cases involving criminal offences committed by the employee may not fall under the data protection regulation. It is therefore hard to estimate the real impact on employees who unintentionally cause a breach. Some questions therefore still need to be addressed. For example, if an employee can be held liable for a data breach then does an employee of a controller (who does the work of a data controller) have a higher liability than an employee of a processor? On what grounds can he or she be held liable? The GDPR is still lacking answers to these important questions.

[12] Thiébaut Devergranne. "Answer to: Who is insuring Data Protection Officers for GDPR liability?" Quora. April 23, 2018. Accessed July 25, 2018. https://www.quora.com/Who-is-insuring-Data-Protection-Officers-for-GDPR-liability/answer/Thi%C3%A9baut-Devergranne-1

The GDPR and the public sector

The regulation differentiates between public authorities or bodies and processing carried out in the public interest by private entities. The latter are, for instance, allowed to process data for archiving purposes in the public interest, however they are not permitted to hold a comprehensive register of criminal convictions. This illustrates that some special provisions apply to public authorities or bodies which cannot be transferred to private entities.

This chapter covers the notion of public interest and the special provisions and derogations for public authorities or bodies. The increased responsibilities of the data protection authority will also be discussed. It should be noted that all of the provisions of the GDPR still apply and that the following points should only be considered as special derogations.

Public interest

The notion of public interest is not specified in the regulation and will therefore depend on the specific context and national practice. However, the GDPR does allow for some leeway in processing for both public and private actors when the purpose is in the public interest:

- The principle of purpose limitation (no further processing of data if it is incompatible with the purpose for which it was collected) does not apply if processing data takes place "for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes." In this case data can be stored for longer periods if the principle of data minimisation is upheld. Furthermore, the rights of the data subjects do not apply if they render the purpose impossible or seriously impair the achievement of it.
- The same applies for special categories of data if there is a legal ground in European Union or Member State law.
- There can be a legal basis if "processing is necessary for the performance of a task in the public interest or in the exercise of official authority vested in the controller" (Art. 6 (1) e).
- Processing of special categories of data is also permitted as long as the public interest is "substantial" and if it has a legal basis in European Union or Member State law.
- For reasons of public interest in the area of public health, processing of special categories of data is permissible. Yet again, a legal ground in European Union or Member State law is required that sufficiently safeguards fundamental rights and freedoms.

Member States may require controllers to consult with the data protection authority if they want to be authorised to use public interest as a lawful basis.

Important reasons of public interest can also be invoked to transfer data to a third country without having a prior assessment by the European Commission of the safeguards for the data. However, this public interest must be recognised by European Union or Member State law.

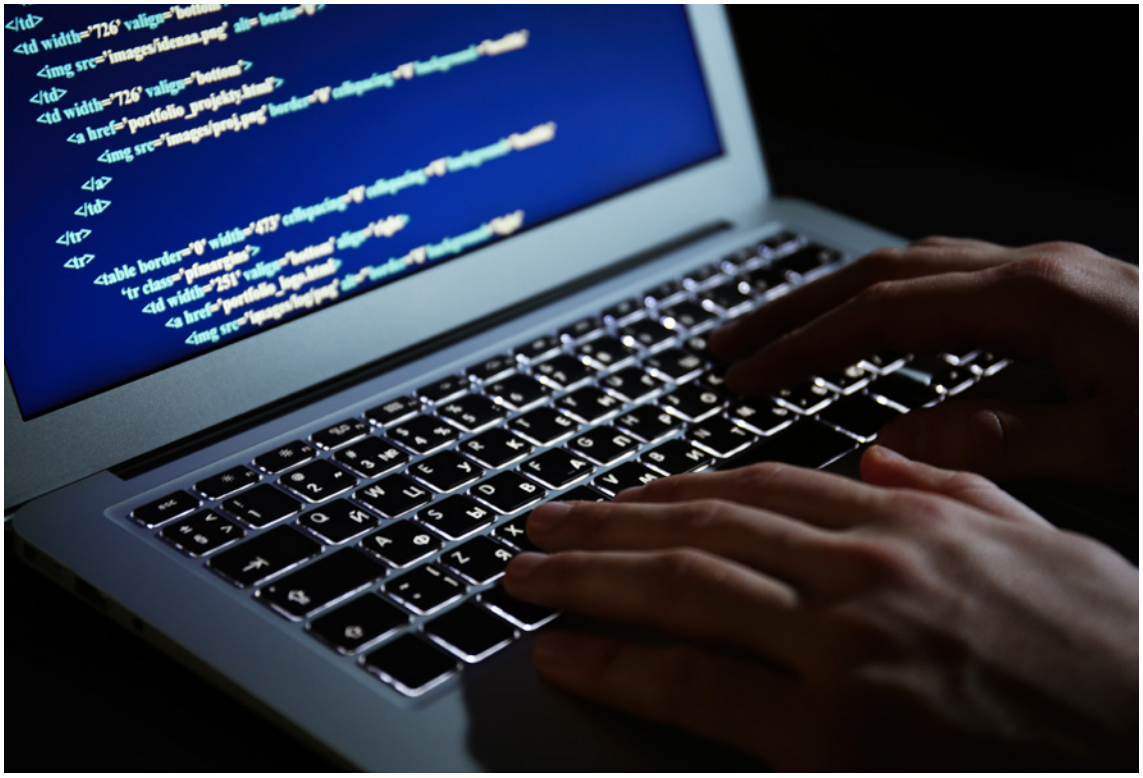
Finally, if one wants to issue a complaint the "one-stop-shop mechanism[15]" does not apply for public authorities or private bodies who act in the public interest. Only the data protection authority where the public or private body is established should be competent for these cases.

Public authorities or bodies

There are two types of derogations for public authorities or bodies. They are either regulated by other laws (the GDPR does not apply) or they can process data and exercise rights which are prohibited for private entities.

The following cases are not regulated by the GDPR:

- EU institutions and agencies are regulated by the Regulation (EC) No 45/2001.
- When public administrations collect data in the framework of a particular investigation in accordance with a legal obligation for the exercise of their official mission, the GDPR does not apply. This is for instance for inquiries by tax and customs authorities, financial investigation units, independent administrative authorities, or financial market authorities responsible for the regulation and supervision of securities markets.
- If the authorities can demonstrate that processing takes place in the context of the EU Common Foreign and Security Policy.
- Data is collected and processed for the purpose "of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security." In these cases the EU Directive 2016/680 applies.



In addition to the above-mentioned derogations relating to public interest, special provisions are granted to public authorities where there is no need for consent for the processing of data when "processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller". However, the public authority needs to demonstrate that processing is in the "public interest" and falls within its legal competences. This is a clear difference from the "legitimate interest" clause for private entities. It does not suffice for a public institution to claim legitimate grounds for data processing if they cannot demonstrate that it is in line with the public interest. For example, is the collection and diffusion of (e-mail) addresses by government agencies strictly necessary for carrying out their tasks within their legal competences?

There is also a derogation for courts that act in their judicial capacity to process special categories of data.

Only public authorities are allowed to keep a comprehensive register of criminal convictions under their control.

Member States can choose whether and to which extent public authorities should be subject to administrative fines.

However, public authorities also have an obligation that doesn't apply to private entities: the appointment of a data protection officer who will advise them on how to ensure compliance. Taking into account public authorities/bodies organisational structure and size, a DPO can be appointed by several institutions at the same time. This might help share the financial costs of the appointment. Only courts acting in their judicial capacity are exempted from appointing a DPO.

Independent supervisory authority

While it is not necessarily a new obligation, Member States need to have one or more independent data protection supervisory authorities and to designate one of them as the lead authority, to be represented in the European Data Protection Board. The independence of the supervisory authority is paramount and members of the authority are therefore not allowed to take on any occupation that is incompatible with their position as a member of the authority. Member States also have to provide data protection authorities with sufficient human, financial and technical resources necessary to carry out their tasks.

Data protection authority members benefit from a high degree of job security. Their duties only end in the event of the expiry of the term of office, resignation, compulsory retirement or in cases of serious misconduct. Members are furthermore subject to professional secrecy rules.

Since the scope of the GDPR has increased compared to previous data protection law, the tasks and powers of the supervisory authority have also increased. Their main task is to monitor and enforce the Regulation as well as to handle complaints. Additionally, they are allowed to conduct investigations, give advice on processing and raise public awareness on the subject of data protection. The full list of tasks can be found in Article 57 of the Regulation. They have powers to order the controller or processor to hand over any information required to perform their task as a data protection authority, to issue warnings or reprimands to a controller or processor if processing is (likely) to infringe the regulation and to accredit certification bodies. The list of supervisory authority powers is substantially longer than in the previous regulation and is set out in Article 58 of the GDPR.

A major improvement on previous regulations is the one-stop-shop mechanism and the increased cooperation of different supervisory authorities. The one-stop-mechanism allows a data subject to lodge a complaint in the Member State where the main establishment of a private entity is based. This data protection authority will then take the lead in a case which can cover all foreign branches of the private entity. The lead authority will have to cooperate with the other data protection authorities where the company has activities to seek agreement on how to proceed. If they do not manage to find a consensus, the case goes to the European data protection board which will take a binding decision how to interpret the GDPR. Cooperation is also strengthened by imposing a deadline of one month for a reply to another supervisory authority and by creating rules for joint operations.

Guidelines on compliance for trade unions

The GDPR impacts trade unions in several ways and also provides news rights and provisions that unions can benefit from. Unions need to know how to benefit from them while taking measures to ensure compliance. Some of the suggested measures below might already be included in your trade union practice:

On data collection and mapping:

1) A good way to start would be to **organize an information session on the GDPR** for union staff and people who are directly involved in data processing.
2) Identify the **data protection officer** and ask him or her to help you to identify crucial trade union issues in your specific organisation or workplace.
3) When new data are collected, the trade union shall **ask for explicit consent** to process it for the specified purposes.
4) There is no need to ask for consent for data already collected if the trade union can show that consent was given at the time of collection (self-inscription to the mailing list/membership form etc.). In some cases they can also rely on their legitimate interests as a trade union as a legal basis (e.g. newsletter). However, if no legal basis for the data can be established it is best to delete the data.
5) There is a prohibition on collecting **special categories of personal data.** However, information on racial ethnicity, health, age, allergies/diary preferences of participants for a conference may be shared at an aggregated level, in order to avoid handing out personal information. For instance: "Among the 10 participants at the conference 3 are vegetarians".
6) Check with the national data protection authority at **what age a person is no longer considered a child**, this may vary between 13 and 16 years, depending on Member State legislation. Where a trade union holds data on children, it needs the active consent of their parents.
7) The union needs to make an **inventory of which personal data the union possesses** on its members, affiliates, supporters etc. and with whom this data is shared.

On data security:

8) **Identify the risks** that might impact your particular organisation, **minimise** them and **educate** employees about how to prevent them.
9) Develop a comprehensive **privacy and security programme** for the organisation, ensuring confidentiality and protecting it from unauthorised access.
10) **Create a secure (password protected or encrypted) database**, limit the people who have access to it and store it in a secure place, in a protected server with limited access. Put the focus on special categories of data, which should in many instances only be collected if in line with the aims of the trade union (see special categories of data).

11) **Raise awareness on phishing (spam)**, communicating the risks frequently to staff
12) Draft a plan to follow when **breaches** occur.
13) Evaluate your **providers** in terms of security

On technical measures:

1) Make sure that the relevant technical and organisational measures are put in place (such as auditing and testing) and be aware of those that cannot be put in place and understand the justification for that.

On policies and procedures:

2) Identify the applicable laws and regulations at European and national level as well as any opinions from authorities and data protection practices.
3) **Review the privacy notices and policies** that are shown at the moment when data are collected (e.g. registration form). The retention period and the specific purpose of data collection need to be stated at this point as well as the rights of data subjects. The users/members need to be informed about any change in the privacy terms.
4) **Write an internal procedure** that clearly explains how, why and for what period of time personal data are stored and how processed. The procedure should cover all individual rights (see rights of the data subject), how the trade union will handle different requests and who will be responsible for dealing with them. This should also include how to react in the case of a data breach. The internal procedure needs to state the **name of the data controller**, **data processor** (and if applicable the **data protection officer**) who will be responsible for applying the new rules.
5) **Write a review the privacy policy** and publish it on the website. The privacy policy should follow the principle of lawful processing. It should include the following elements:
    a. What data are collected?
    b. For which purpose?
    c. For how long?
    d. How are they collected?
    e. How are they processed?
    f. How is the process carried out?
    g. Is it likely that this data will be processed in any other way in the future and, if so, how?
    h. How can data subjects exercise their rights?
    i. With whom is the data shared?
    j. What safeguards have been put in place?

The principle of data minimisation applies here and it is therefore best to reduce the number of third party processors. It is suggested to avoid using social media plugins for the website or to only use those that do not collect any data on visitors.

6) If need be conduct a **data protection impact assessment.**
7) Make a list of the **practices that should be avoided**. Such as sharing data and passwords.
8) **Trade unions as employers** need to respect the GDPR when processing data on their employees.

Practical recommendations on data protection

Keeping data safe is the utmost priority. In order to protect data subjects and avoid any data breaches it is best to consider the following recommendations:

1) Make sure employees have **constant and sufficient information and training**.
2) Make sure there are **data protection policies in the organisation**, including security measures and protection of employment and staffing data.
3) **Protect passwords** on all computers, laptops and other devices and regularly change them. Lock them away over night.
4) **Store paper records in locked cabinets** and keep them out of view of visitors.
5) Regularly **update software** and anti-virus programmes.
6) **Encrypt all the databases** and documents with special categories of data such as union membership.
7) Adopt good practices. Send emails to mailing lists or put the email addresses of the receivers **into the blind copy (BCC) field**.
8) **Secure your websites** and if cookies are required collect consent.
9) **Develop a more anonymous approach of your data.** Anonymise (un-link data) or delete files as soon as possible. If you create case files you can state either as legal basis that it falls under the trade union's legitimate activities or that it is used for legal claims. However, the safety of this data needs to be ensured and after the case is closed it should either be erased or anonymised.
10) Make sure employers are aware of their responsibilities as controllers.
11) Know when to contact the **Supervisory Authority**

Help us to keep the focus on the GDPR

Upon the rollout of GDPR, many trade unions and shop stewards were left wondering what they needed to do. Numerous public and private entities were slow to take action, and in spring 2018, most of them were not prepared for the new legislation. Since the GDPR compliance deadline of 25 May 2018, we have been trying to reach out to trade unions in public services to ask them to share the steps they took while starting the process as well as any practical GDPR case studies, problems and challenges encountered in their daily work. For this reason, if you have concrete questions, examples of good or bad practices to share or are looking for guidance in dealing with the GDPR, you can write to gdpr@epsu.org.

Further information and reading

The General Data Protection Regulation: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1465452422595&uri=CELEX:32016R0679

Article 29 Working Party "Guidelines": http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1360&tpa_id=6936

Buffard, Sally, *The General Data Protection Regulation – a practical guide for trade unionists,* Labour Research Department Booklets, March 2018

Commission Nationale de l'Informatique et des Libertés, Security of Personal Data. The CNIL Guides 2018, France, www.cnil.fr

European Trade Union Committee for Education (ETUCE), "ETUCE's guidelines on the new EU General Data Protection Regulation (GDPR)", May 2018, https://www.csee-etuce.org/images/attachments/GDPR-guidelines-2018.pdf

Fritsch, Clara. „Die Europäische Datenschutzverordnung." 2nd ed. Vienna, Austria: GPA-djp, Mai 2018

Information Commissioner's Office, *Guide to the General Data Protection Regulation,* https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/


GDPR

EPSU is the European Federation of Public Service Unions. It is the largest federation of the ETUC and comprises 8 million public service workers from over 260 trade unions across Europe. EPSU organises workers in the energy, water and waste sectors, health and social services and local, regional and central government, in all European countries including the EU's Eastern Neighbourhood. It is the recognised regional organisation of Public Services International (PSI). For more information please go to: www.epsu.org