FINANSFORBUNDET

Introduction to GDPR in employment relationships

5 September 2022

Introduction

Authors: Mette Hjøllunds Schousboe and Jan Jeppesen.

Mette and Jan constitute Finansforbundet’s GDPR group and have day-to-day responsibility for Finansforbundet’s GDPR compliance and operation.

Topics

- Fundamental principles for the processing of personal data
- General rights of applicants and employees
- Processing of information during the recruitment process
- Processing of information during the term of employment
- Processing of information after the term of employment
- Employee control
- Monitoring
- Home-based teleworking
- Key points

GDPR and employment law

The General Data Protection Regulation, GDPR, applies to all forms of processing of personal data.

The rules are the same whether you are processing shoe size data and email addresses in an online shoe shop or processing employee data in connection with an employment relationship.

The regulation contains various rules depending on the categories of personal data processed and the categories of persons the processed data relate to.

The Danish Data Protection Agency has prepared a guideline in Danish on the processing of personal data in employment relationships. This webinar is based on this guideline.

General aspects of the processing of personal data by employers

Fundamentally, the employer has the right to process a wide range of information about their employees before, during and after the term of employment.

This information typically covers the following (non-exhaustive) data:

- name, address, date of birth, contact details, (telephone, email), education, appraisal interviews, salary entry point, salary, bank account, warnings, termination, CV, civil registration number, pension details, tax information, work assignments, sickness absence, close family members...

The legal basis of the processing is often the employer's legitimate interest or obligations under employment law such as paying salary and managing the employment relationship (section 12(1)-(3) of the Data Protection Act) or section 11 of the Data Protection Act concerning the processing of the civil registration number.

General aspects of the processing of personal data by employers

The employer may also be required to process personal data to safeguard employee rights under other legislation.

This could be in connection with an application for sickness benefits.

Collective agreement: For example, the standard collective agreement’s provisions on professional work, clause 3, the union representative’s participation in interviews about wage reductions, instant dismissals and terminations.

Another example is the establishment of pension schemes, dental insurance, personal accident insurance and other mandatory employer’s insurance.

FINANSFORBUNDET

Fundamental principles in the processing of personal data

Lawful, fair and transparent processing

Data must be processed lawfully, fairly and in a transparent manner.

Personal data must only be processed for specified, explicit and legitimate purposes, and the data must not be further processed in a manner that is incompatible with the initial purpose (‘purpose limitation’).

Example
An employer processes the names and addresses of its employees as part of its general administration of employment relationships.

The employer would like to disclose the information to a company which, against the employee’s own payment, offers discounted services such as a gym membership.

Such processing of data (in this case disclosure of information) would not be considered to be compatible with the initial purpose. The employer would have to find another basis for the lawful disclosure of the information, e.g. in the form of a consent.

Data minimisation

Data minimisation
The information being processed must be relevant and limited to what is necessary in relation to the purposes for which the information is processed.

Example
As part of the employment process, an employer records information about the employee’s hobbies and memberships of local sports clubs.

Most often, it will not be relevant in an employment relationship or necessary to know the hobbies of the employees, or to hold information about their sports club memberships – unless it serves the purpose of the employer paying the membership dues.

Up to date, storage limitation, erasure, secure processing

Information must be kept up to date
The information must be kept up to date. Inaccurate information should generally be rectified or deleted.

Storage limitation
The information must not be kept for longer than necessary. Initially, the employer must assess for how long it is necessary to keep the information based on the purpose for which it is was collected.

Anonymised or erased
Once the purpose has ceased, the information must be erased or anonymised.

Secure processing
And finally, information must be processed in a manner that ensures appropriate security and confidentiality of the information.

FINANSFORBUNDET

General rights of applicants and employees

The data subject enjoys various rights

The data subject (applicant, employee or former employee) has various fundamental rights, of which the following are the most important:

- the right to receive information about the processing of his or her personal data (information to be provided)
- the right of access to information held about him or her (right of access)
- the right to have inaccurate information rectified (right to rectification)
- the right to have information erased (right to erasure)
- the right to object to the otherwise lawful processing of information (right to object)

The specific information being processed will often appear from the company's personal data policy. The regulation stipulates that employers must actively provide the information to applicants/employees, for example by submitting the personal data policy to them or making it easily accessible to them in some other way.

Considerations to take home
"Do you or your colleagues know your company's personal data policy applicable to the employees?"

Information to be provided

Besides the categories of information being processed, a range of additional information must be provided, e.g.:

- information about the controller
- the purpose of the processing for which the personal data are intended, and the legitimate interests pursued
- the expected period during which the information will be processed
- the origin of the information if not provided by the data subject (for example references or social media)
- the right to file a complaint with the Danish Data Protection Agency
- the existence of automated decision-making (for example if applications are automatically rejected based on various criteria, including applicant profiling)

The employer must be able to document having provided the information required. It is not enough to place the information on a website that the data subjects must find themselves.

Social media

Employers are permitted to collect and process personal data from social media (such as LinkedIn, Facebook, etc.)

Such collection and processing must be disclosed in, for example, the personal data policy.

Likewise, the processing must be confined to information that is necessary and limited to the purpose for which it is collected.

In other words, the employer needs to have a legitimate reason to process the information also in the case of social media.

This obligation is especially important to consider in situations with terminated employees.

Right of access

Employees have the right to know which personal data are processed and the purpose thereof.

The purpose is to give employees the possibility to see which personal data the employer is processing about them, thereby increasing transparency of how personal data are processed. It enables employees to check if the personal data are correct and otherwise processed in compliance with the law.

Right of access – an example

An employee requests access to information which the employer is processing about her. The employer then gives her a list detailing the type of information the company is processing.

The list contains items such as ‘name’, ‘address’ and ‘trade union membership’ but does not contain the actual personal data.

Simply supplying the employee with a list of the type of information the company processes does not enable the employee to check the accuracy of the information, and therefore the right of access has not been met.

Right of access – decision of the Danish Data Protection Agency

An applicant is asked as part of the recruitment process to take a personal profile test at an external recruitment agency.

The job application is rejected, and the applicant therefore requests access to his or her personal profile test at the recruitment agency. The agency denies the request on the grounds that the applicant is not trained in the specific profile.

The applicant subsequently complains to the Danish Data Protection Agency, which rules in favour of the applicant’s claim that a personal profile test is comprised by the right of access and must be provided on the basis of a request for access.

In the meantime, the recruitment agency deletes the profile, causing the Danish Data Protection Agency to express substantial criticism and to seek the imposition of a fine on the grounds that the agency, by having deleted the profile, has denied the data subject of the right of access to the information processed.

Right of access – decision of the Danish Data Protection Agency

A data subject complained to the Danish Data Protection Agency because an employer had denied a request for access to memos, letters and emails written by the data subject during the employment relationship/function. The employer had provided access to all personal data being processed and had asked the data subject to specify the contents of any additional requests (delimit the request for access to relevant information).

The Danish Data Protection Agency ruled in favour of the employer as the request for access to all material written and submitted as part of the employee's function was considered excessive and unfounded.

The Danish Data Protection Agency attached no importance to the fact that the data subject requested the information in connection with possible proceedings against the employer.

Right of access – not necessarily to everything

The right of access does not necessarily cover everything
Internal considerations and assessments made by HR or a manager about an employment relationship or information assumed to put the employer in a weak position, for example in pay negotiations, are generally exempt from the right of access.

This may also apply to memos, letters and emails that an employee has written, signed and submitted, etc. as part of the job assignments.

In this situation, the employer may deny an employee's or former employee's request for access to the documents on the grounds that the request is excessive or manifestly unfounded.

In other words, the right of access is not a channel through which to obtain 'access to documents', e.g. for use in proceedings against your employer (Note: The legislation on access to documents applies exclusively to the public domain and is not part of GDPR).

Rectification

The right to rectification means that the data subject has the right to have inaccurate personal data about them rectified.

It means, among other things, that an employer may not refuse to add further information to the information of, for example, a personnel case if it would make the case more complete and/or up to date.

Erasure

The right to erasure implies that the data subject – with certain exceptions – has the right to have information about him or her erased.

The data subject has the right to have his or her personal data erased without undue delay if any of the following applies:

- It is no longer necessary for the employer to store the information about him or her for the purposes for which they were collected.
- The employer has based the processing on a consent, and the employee withdraws his or her consent, and there is no other legal basis for the processing.
- The employer may not lawfully process the information.
- The employer has an obligation to erase the information under EU law or national law.
- The employer is required to erase the information as a result of the employee having exercised his or her right to object to the processing.

Erasure – exceptions

The right to erasure of information is subject to a number of exceptions.

Personnel history
For example, an employer is not required to erase information if storage thereof is necessary to document the historical events of a personnel case or if the employer is required by law to store the information.

Documentation requirement
This applies, for example, to payroll data subject to tax law provisions which the employer must comply with in the reporting of information to SKAT, the Danish tax authorities.

Legal claims
Likewise, if the employer needs the information in connection with a dismissal case, the employer may deny erasure of the information if it is necessary for the establishment of a legal claim.

Objection to processing

The right to object means that the data subject may – on grounds relating to his or her particular situation – object to the otherwise legal processing of his or her personal data.

Usually, there must be compelling reasons if the employer is to accommodate a request not to process information, provided that the employer can demonstrate a legitimate purpose, and the employer's interest in processing the information overrides the data subject's interests for the processing not to take place.

If, based on a new assessment, the employer finds that the processing is still necessary, the employer must be able to explain this to the employee, by giving an account of the completed, concrete assessment of the considerations, and explaining why the employer finds that the objection cannot be accommodated.

Objection – example

Example
An employer displays the name and business contact details of its employees on its public website.

For personal reasons, an employee requests not to have his or her name and contact details displayed on the company's public website.

In this situation, the employer MUST assess if the employer's legitimate interests override the employee's interest in displaying the information.

As part of this assessment, the employer must consider what the purpose and the need for displaying the information is. Is it a salesperson at a car dealer or a cook in the canteen?

If the employer decides to keep displaying the information, the employee has the possibility to complain about this decision to the Danish Data Protection Agency.

FINANSFORBUNDET

Processing of information during the recruitment process

Job application and CV

Information in job application and CV
During the recruitment process, the employer is permitted to process the personal data which applicants at their own initiative have actively made available to the employer in connection with the submission of a job application, including the letter of application and CV.

References may be taken based on consent
The collection of information from, for example, previous and present employers, is possible based on the applicant's consent. The applicant must, if applicable, be informed of whether the collection of information is confined to details about, for example, date of employment, work assignments and similar 'neutral' particulars, or whether information of a more subjective nature will also be collected, for example the applicant's professional or social skills, sensitive personal data or information about any criminal offences.

That an applicant is looking for a new job is generally confidential
Consent is required because the knowledge that someone is applying for a new job is considered information that you are not permitted to disclose (e.g. to previous or present employers) without the consent of the applicant.

Certificate of criminal record, statements of no previous convictions in respect of children, personality test

Certificates of criminal record and statements of no previous convictions in respect of children

The employer is only allowed to request or collect information about any criminal offences the applicant might have committed if it is relevant to the position applied for and if it is realistic that the applicant will be considered for the position.

Personality test

Is conditional upon the active participation of the applicant and will normally not involve data of a sensitive nature. If the test includes sensitive personal data, the employer may, prior to completion of the test, obtain the applicant’s consent to processing.

Information on social media

Information on social media
The employer may collect and use relevant publicly available information that job applicants have published about themselves, for example on social media.

For legitimate and proportionate purposes only!
Even if applicants have published the information themselves, the processing must always be limited to information that is legitimate and proportionate to the purpose of collecting it.

Requirement for information to be provided!
Employers that process information from social media about applicants are furthermore required to inform the applicants thereof.

Applicants who are not offered the job

Storage of information about applicants
Information (application, CV, etc.) about applicants who are not offered the job should, in principle, be erased once the position is filled.

Sometimes necessary to document a specific recruitment process
There may be situations in which the employer needs to document a specific recruitment process, for example if the employer is facing objections based on, for example, discrimination. Keeping the information for a period of time would generally be considered a legitimate purpose.

Health data

Health data
The employer is generally not permitted to process health data in connection with recruitment. However, the Act on the Use of Health Data does in certain situations permit the employer to process health data, for example if the data are necessary for the employer to assess an applicant’s ability to perform the job.

It is therefore a requirement that the data are essential to the assessment of the applicant’s ability to perform the job.

Applicants – example, social media

In the recruitment of a new employee, the employer collects information about previous positions on LinkedIn and finds out, on Facebook, that the applicant went through a divorce a year ago.

The information is recorded in the file, and the employer fails to inform the applicant that information is being collected from social media.

For legitimate and proportionate purposes only!
Firstly, it contravenes the employer's obligation to inform the applicant that information will be collected from social media, secondly, the information obtained about the divorce contravenes the requirement for legitimate and proportionate purposes as this information must be presumed irrelevant to determine if the applicant can do the job.

FINANSFORBUNDET

Processing of information during the term of employment

Processing of information during the term of employment

As mentioned previously, the employer may process a wide range of information about the employee as part of the general administration of the employment relationship.

Sensitive personal data
The processing of sensitive personal data (such as trade union membership, health data) often requires the explicit consent of the employee.

However, in some cases, the employer has the possibility of recording sensitive data without consent if permitted by other legislation, e.g. reimbursement under section 56 of the Danish Sickness Benefits Act or termination reasons under sections 2 and 12 of the Danish Salaried Employees Act.

The employer may in other situations process sensitive data if legal claims are to be established, e.g. in relation to a work-related injury.

The lawfulness of processing information must always be determined on a case-by-case basis.

Appraisal interviews, workplace risk assessments, member satisfaction surveys

Appraisal interview forms
The information entered in an appraisal interview form is comprised by the rules of the General Data Protection Regulation.

General personal data in the form may basically be processed without consent. Where sensitive data are concerned, the prohibition against processing may only be waived based on a consent obtained from the employee.

Workplace risk assessments, member satisfaction surveys, etc.
If the data are personally identifiable, they are comprised by the rules of the General Data Protection Regulation.

The processing of sensitive personal data may only take place by consent.

Warnings, sickness absence

Warnings
The Danish Data Protection Agency accepts indefinite storage (until the employment relationship ceases) as part of the historical events of a personnel file.

Sickness absence
Information on the reimbursement of sickness benefits may be stored until the requirement for any repayment has lapsed.

However, the information on sickness absence may be stored indefinitely (until the employment relationship ceases) as part of the historical events of a personnel file.

Disclosures from the employer to the union representative

Disclosure of information to the union representative
There are several situations in which the employer will have the opportunity to disclose information about the employee to a union representative for him or her to perform their tasks, including tasks following from the collective agreement.

See the agreement on professional work in clauses 2 and 3 of the standard collective agreement in connection with the recruitment of new employees, transfers, termination, wage reductions, warnings and instant dismissals.

Publication on the company’s website

Work-related information
Employers are generally entitled to publish work-related information about their employees on their website such as names, work areas and contact details (to which employees may object).

Information of a private nature
The publication of information of a private nature such as private address, telephone number and email address and information about hobbies or other private matters would rarely be considered to constitute a legitimate purpose and would generally require consent.

Employee photo on the company’s website

If the employer would like to display a portrait photo on its public website, it would generally require the consent of the employee.

If a consent is withdrawn, the portrait photo must be removed from the website.

In specific situations, the employer’s interests in publishing a photo of the employee on its website may outweigh the employee’s interests, in which case the photo may be published without consent. It will be sufficient to notify the employee thereof.

Photos of employees in marketing material

A consent is generally required if an employer would like to use photos of employees in marketing material.

Likewise, if a consent is withdrawn, any leaflets, advertisements or other material published as files on the website must be removed.

In this situation, the employer may alternatively consider drawing up an agreement (model contract) with the employee, defining which photos may be used, what they may be used for and for how long.

Photos on the intranet (internal phone book)

Depending on the specific circumstances, the employer may place employee photos on its intranet without obtaining prior consent, provided the employees are informed about it, and that they have the right to object.

Disclosure of information at the workplace

Disclosure of information about absence internally at the workplace
Information about absence could be details about holiday, days off or illness.

Information about illness
Information about absence due to illness with no other details provided will not be considered sensitive information.

If information about sickness absence/illness contains such precise and specific details that specific deductions can be made about the employee’s health, it is considered health data that must generally not be disclosed.

Disclosure of information about fertility treatment – decision of the Danish Data Protection Agency

An employee undergoing fertility treatment had discussed her support needs with her team manager.

The team manager sent out an email to her department (51 recipients), briefing them about the agreed support needs and the cause, which was fertility treatment.

The Danish Data Protection Agency has expressed serious criticism of the concerned local authority’s disclosure of unnecessary information about an employee, more specifically information that the employee was undergoing fertility treatment, stating that the information was to be considered confidential and could not lawfully be disclosed to the department’s employees.

Disclosure of information about termination

Disclosure of information about termination/dismissal
Employers may have a significant interest in informing their employees about the termination of an employee to avoid the spread of rumours.

But it is generally not necessary to disclose the reason for the termination/dismissal.

Disclosure of information about the reason for termination – decision of the Danish Data Protection Agency

Decision of the Danish Data Protection Agency on an employer's disclosure of information about a previous employee

A citizen complained to the Danish Data Protection Agency that his/her previous employer had disclosed information about him/her to the company's customers without authorisation.

In emails to two of the company's customers, the company had disclosed that the former employee had committed and admitted to having committed criminal offences in the employment relationship, providing details about how the criminal offence involving fraud was said to have happened.

In this case, the Danish Data Protection Agency ruled that it was unauthorised disclosure of information about a criminal offence.

The Danish Data Protection Agency has reported the company to the police, recommending the imposition of a fine of DKK 400,000.

FINANSFORBUNDET

Processing of information after the term of employment

Storage of information about former employees

Main rule
For as long as an administrative need/legitimate purpose exists – and up to five years, under the general limitation period.

Documentation of historical events in a personnel case
The Danish Data Protection Agency has in several specific cases stated that being able to document the historical events of a personnel case is to be considered a legitimate purpose. In addition, other legislation may stipulate that information must be stored for a certain period of time, for example in relation to payroll data and reporting to SKAT.

The legal claim's rule
The employer might also need to store information that is necessary to establish any legal claims arising from an employee dismissal or in the event of a work-related injury.

Employee control

Control of employees and the role of the union representative

Overall, Finansforbundet finds and believes that the implementation of control measures should generally always be discussed with the union representative before implementation.

Monitoring measures comprised by the management prerogative

The control of employees is generally comprised by the overall management prerogative and usually implies the processing of personal data.

Work tools
Smartphones, computers, tablets, GPS devices and the like make it possible for the employer to monitor employees in the workplace and at home.

The implementation of monitoring measures is subject to a number of requirements:

- Must be lawful, transparent and justified by operational reasons and reasonable purposes
- Must not violate the rights of the employees
- Must not inflict losses or noticeable inconvenience

Control measures are not subject to employee consent.

CCTV surveillance

Permitted if there is a legitimate reason and provided it does not go beyond what is necessary.

In addition to the general rules of the Danish Act on CCTV Surveillance (signage, etc.), the employer has an obligation to inform its employees of the use of CCTV surveillance, the purpose of CCTV surveillance and the cases in which the footage might be reviewed and handed over to the police.

Employees must also be informed of how long the footage will be stored.

The information must be provided in advance. New employees must be informed as part of the recruitment process, or when they start working on premises with CCTV surveillance.

Logging of internet activity and email usage

Logging of employees' internet activity and email usage
The employer may under certain conditions register (log) the employees' visited websites and subsequently review website visits and emails.

Employees must be informed in advance that registration/logging takes place, and that the registration of visited websites and email usage might be reviewed as part of control activities if a violation of the workplace's guidelines is suspected to have taken place.

Emails of previous employees
When an employee resigns and no longer has access to a personal email account at the workplace, the email account may be kept active for the shortest period of time necessary and maximum 12 months. Upon resignation, an auto reply should be activated to give information about the employee's resignation and any other relevant information. The resigning employee must be informed that the account will remain active for a period of time and the purpose thereof.

Recording of telephone conversations and control purposes

Basically, telephone conversations may be recorded only on consent by the data subject. However, the employer may, for purposes such as complying with other legislation, for example the rules on anti-money laundering, record telephone conversations internally between employees and between employees and customers without prior consent.

If telephone conversations are recorded, employees must be informed thereof, including the purpose of recording and their rights.

Likewise, recording may take place without consent if necessary to document the meeting, and a telephone recording is considered the only real way to do so.

FINANSFORBUNDET

Monitoring

Monitoring may result in an increased risk to employees

Excessive monitoring of employees could result in an increased risk to the rights and freedoms of employees.

Requirement for an impact assessment, if applicable
Depending on the extent and nature of monitoring, the employer may, prior to the implementation of monitoring, be required to carry out an impact assessment to evaluate the risk to the data subjects.

As a rule, an impact assessment must always be carried out if the processing is likely to result in a high risk to the employees.

Involvement of the union representative

Requirement for consultation of the data subject prior to implementation
If a specific situation requires that an impact assessment be carried out, the data subjects, or their representatives, must as part of the assessment be consulted on the intended processing prior to its implementation.

Finansforbundet finds it natural for the union representative to represent the employees in discussions of the impact assessment.

Should the impact assessment indicate a high risk that cannot be mitigated, the intended processing must be presented to the Danish Data Protection Agency for approval prior to the start of processing.

Impact assessment

The world of GDPR is deeply divided on the issue of when an impact assessment must be conducted.

While some believe that any form of monitoring/control calls for an impact assessment, others find that something more is needed.

.

Impact assessment

To guide this assessment, we can use the European Data Protection Board's Guidelines on Data Protection Impact Assessment. The guide includes impact assessment in relation to monitoring in an employment relationship as an example:

"A company systematically monitoring its employees' activities, including the monitoring of the employees' work station, internet activity, etc."

The EDPB's justification in this case is that it involves both (large-scale) systematic monitoring and data concerning vulnerable data subjects (due to the employees' power imbalance vis-a-vis the employer).

Awaiting decisions to clarify legal practice

We have yet to see cases and decisions in the area, and we therefore have no legal practice to lean on.

If you are unsure if monitoring takes place, or if you are unaware of its extent and nature, the works council is the place to bring it up with management.

FINANSFORBUNDET

Home-based teleworking

Home-based teleworking

Agreement on home-based teleworking
Confidential and sensitive personal data must not be processed in home-based teleworking, unless based on an agreement between the employer and the employee.

The employer’s obligations in relation to home-based teleworking
The employer must specifically ensure that data security requirements are met.

The requirements for security and security systems in home-based teleworking are the same as those at the workplace.

Storing of documents locally (on the device)
The device or files must be encrypted. No one else (children included) must have access to the device.

Files/documents must be uploaded to central systems as soon as possible.

Home-based teleworking

Physical documents containing personal data
Any physical documents containing personal data must be kept safely locked away and must be disposed of safely.

The employer’s control of security in home-based teleworking
It is not exactly clear how the employer is to carry out a control to see if the security in home-based teleworking is sufficient.

Employees have a higher degree of privacy protection when they work from home in relation to control possibilities, so the control must generally be carried out remotely.

Add to this the challenges of the physical layout of the workstation when working from home – that is a completely different matter deserving its own webinar ☺

Key points

Article 6 / sections 6 and 12	Article 9 / sections 7 and 12 + article 6	Article 10 / section 8	Article 87 / section 11
General information (non-exhaustive)	Sensitive personal data (exhaustive)	Information on convictions and offences	Civil registration number
➢ Name and address ➢ Civil status ➢ Finance ➢ Education and previous employment ➢ Pay and tax information ➢ Bank account no. ➢ Photos and recordings ➢ Pension information	➢ Race or ethnic origin (*but not nationality)* ➢ Political, religious or philosophical beliefs ➢ Trade union membership ➢ Genetic or biometric data ➢ Health data ➢ Sex life or sexual orientation	➢ Information about committed criminal offences or police reports ➢ Information on, for example, disqualification ➢ Information on certificate of criminal record ➢ Prison address	➢ Civil registration number
<u>Legal basis for processing</u> - Consent - Contract - Legal obligation - Labour law obligation or right under other legislation or collective agreement - Balancing of interests	<u>Legal basis for processing</u> - Explicit consent - Published information - Legal claim or labour law obligation or right - Balancing of interests	<u>Legal basis for processing</u> - Explicit consent - Strict balancing of interests (“must clearly outweigh the interests justifying non-disclosure”)	<u>Legal basis for processing</u> - Follows from legislation - Consent - The conditions for processing of sensitive information are met

Closing remarks

Any final questions?

Thank you for your participation. Remember that you can always write to us with questions or ask us for advice.

GDPR@finansforbundet.dk

FINANSFORBUNDET

Mette Hjøllunds Schousboe
and
Jan Jeppesen.

5 September 2022