Supervision of the Labor Market Supplementary Pension (ATP)

Date: 07-08-2020

Decision

Public authorities

Journal number: 2019-421-0035

Summary

In August 2020, the Danish Data Protection Agency completed a planned written inspection by the Labor Market Supplementary Pension (ATP). The audit focused on ATP's compliance with the rules on the duty to provide information when using control measures towards employees. The audit also focused on whether ATP's compliance with the duty to provide information complied with the regulation's basic principle of transparency, which i.a. implies that the data controller must provide employees with easily accessible and prior information about the control measures applied.

On the basis of the audit carried out, the Danish Data Protection Agency has found reason to express serious criticism of ATP's processing of personal data.

The Danish Data Protection Agency's concluding statement states, among other things, that ATP's compliance with the duty to provide information has been deficient because the authority has not provided employees with sufficiently clear information about the purpose of processing the information, the legal basis for processing, the affected categories of personal data and the period. will be kept, or if this is not possible, the criteria used to determine this period.

In addition, it appears that the information that ATP has provided to employees in accordance with the rules on the duty to provide information has not been provided to the employees in a sufficiently easily accessible form.

You can read the Danish Data Protection Agency's guidelines on data protection in connection with employment relationships here.

You can read the Danish Data Protection Agency's guide on data subjects' rights here.

Decision

1. Written supervision of ATP’s processing of personal data

Arbejdsmarkedets Erhvervssikring (AES) was among the authorities that the Danish Data Protection Agency had chosen to supervise in the autumn of 2019 in accordance with the Data Protection Ordinance [1] and the Data Protection Act [2].

The Danish Data Protection Agency therefore announced an audit of AES on 9 September 2019. The supervision was a written supervision which focused on AES 'compliance with the duty of disclosure in connection with control measures towards employees, cf. Articles 13 and 14 of the Regulation. 5 pieces. 1, letter a, which according to the Authority's assessment i.a. implies that the data controller must provide employees with easily accessible - prior - information about the control measures used.

By letters dated 7 October 2019 and 5 May 2020, AES has issued statements on the matter. It appears i.a. of AES 'statements that Arbejdsmarkedets Tillægspension (ATP) is data responsible for the processing of personal data that takes place in connection with the use of control measures against employees who perform tasks in AES' area of authority. As a reason for this, AES has stated that ATP is the appointing authority with instruction and management authority vis-à-vis the employees who handle tasks in AES 'area, and that processing of personal data in connection with the use of control measures vis-à-vis employees is to fulfill ATP's specific purpose.

As a result, the Danish Data Protection Agency decided instead to direct the written inspection towards ATP, which the inspection notified to ATP on 19 May 2020.

By letter dated 2 June 2020, ATP has confirmed the information that appears in AES 'statements of 7 October 2019 and 5 May 2020. In this connection, ATP has noted that AES' answers to the Danish Data Protection Agency's questions have been prepared in collaboration between ATP and AES.

Following the audit of ATP, the Danish Data Protection Agency finds reason to conclude:

That ATP's compliance with the duty to provide information pursuant to Articles 13 and 14 of the Regulation has been deficient, including in that the authority has not provided employees with sufficiently clear information about the purpose of the processing, the legal basis for the processing, the categories of personal data concerned and the period will be kept, or if this is not possible, the criteria used to determine this period.

That ATP's compliance with the duty to provide information has not taken place in a sufficiently easily accessible form in accordance with Article 12 (1) of the Regulation. 1.

The Data Inspectorate finds in relation to pkt. 1 and 2 grounds for expressing serious criticism that ATP's processing of personal data has not taken place in accordance with Article 12 (1) of the Data Protection Regulation. 1, Articles 13 and 14.

With regard to lack of information about the purpose of processing personal data, the Danish Data Protection Agency further

finds that ATP's processing of personal data has not taken place in accordance with the basic principle of transparency in Article 5 (1) of the Regulation. 1, letter a.

The Danish Data Protection Agency has noted that ATP on 4 October 2019, ie. after the date of notification of the supervision on 9 September 2019, has expanded the disclosure text that the authority uses to comply with the disclosure obligation. However, it is noted for the sake of good order that the Authority has not taken a position on the content of the expanded information text.

Below is a more detailed review of the information that has emerged in connection with the written inspection and a justification for the Danish Data Protection Agency's decision.

2. ATP's use of control measures against employees

ATP has initially confirmed what AES stated that ATP is data responsible for the processing of personal data that takes place in connection with the use of control measures against employees who perform tasks in AES 'area of authority.

ATP has subsequently stated that the authority makes use of the following control measures against employees who perform tasks in AES 'area of authority:

Logging of the use of internet, subject systems and rejected access attempts

Logging of access to physical locations and time registration

Assignment and follow-up of roles and rights in subject systems

Access to employee emails

Obtaining criminal records upon employment and during the employment relationship

Whistleblower scheme

TV surveillance

Fraud control

In relation to the use of logging of employees' use of the Internet, ATP has stated that logging can be followed up in the event of concrete suspicion of abuse or hacking.

With regard to logging of the employees' movements in professional systems, ATP has stated that the logging is checked by random sampling and data analyzes with the aim of ensuring that internal guidelines and rules are complied with, including whether employees make notices in cases that are not objectively justified. . In addition, checks are made of whether the

employees store and use work-related data in violation of internal rules, for example whether work-related social security numbers, etc. are stored. in Outlook or on drives not intended for this.

Regarding logging of rejected access attempts, ATP has stated that checks are made of rejected access attempts, which the employees do not have a work-related need to access. In addition, it is checked whether the employees send work-related tasks from the work e-mail to the employees' private e-mail.

In relation to logging access to physical locations and time registration, ATP has stated that the employees' access to buildings and premises is logged via the employees' access cards, and that in case of suspicion, checks can be made as to whether the employees' time registrations correspond to the actual working hours.

In relation to the allocation of and follow-up of roles and rights in professional systems, ATP has stated that the purpose of this measure is to ensure that employees only have access to cases in systems for which they have a work-related need.

It is generally the opinion of the Danish Data Protection Agency that allocation and follow-up of roles and rights in professional systems constitute a security measure within the meaning of Article 32 of the Data Protection Regulation, and that such a measure does not have the character of a control measure covered by this supervision. Thus, with this supervision, the Danish Data Protection Agency has not taken a position on ATP's observance of the duty to provide information in connection with the processing of personal data as part of the allocation and follow-up of roles and rights in professional systems.

With regard to access to employees 'e-mails, ATP has stated that the authority stores former employees' e-mail accounts and personal drives, etc., as it may be necessary for ATP to be able to access certain information for operational and business reasons.

Regarding obtaining criminal records at employment and during the employment relationship, ATP has stated that it is a condition for both employment and staying in the employment relationship that the employee's criminal record is not incompatible with an internally decided dignity requirement and general decorum rules. Employees must therefore present a criminal record when entering into a contract. In addition, during the employment relationship - on a random basis or in case of suspicion - it will be possible to obtain a criminal record for employees with prior consent.

In this connection, the Danish Data Protection Agency must note that in this decision the Authority has not taken a position on ATP's fulfillment of the duty to provide information in connection with obtaining criminal records during employment and during the employment relationship, just as the Authority has not taken a position on whether such processing of personal data can

be found. within the framework of the Data Protection Regulation. This is because the Danish Data Protection Agency has decided to take up a case of its own motion regarding ATP's processing of personal data in connection with obtaining criminal records during employment and during the employment relationship. ATP will receive a separate request in this regard.

In relation to the whistleblower scheme, ATP has stated that there will be an investigation of the report in question in cases where an employee has been reported under the whistleblower scheme.

In this connection, the Danish Data Protection Agency must note that the possibility of making reports via such a system, in the opinion of the Authority, does not in principle have the character of a control measure covered by this supervision.

The Danish Data Protection Agency has hereby, among other things, emphasized that any control will be outsourced to employees or other external parties who have the opportunity to make reports via the whistleblower system. In addition, the Data Inspectorate's immediate perception is that it will be the subsequent investigation that takes place on the basis of a report that could constitute a control measure covered by this supervision, as such an investigation may typically consist of one or more of the other control measures. , which ATP has stated in connection with this supervision, including, for example, control of various loggings or TV surveillance, etc. Thus, with this supervision, the Danish Data Protection Agency has not taken a position on ATP's compliance with the duty to provide information in connection with the processing of personal data as part of the authority's whistleblower system.

With regard to television surveillance, ATP has stated that the authority conducts television surveillance of physical facilities, entrances and selected premises. The surveillance has a preventive purpose with a view to securing properties and personnel, but the surveillance can exceptionally be used as part of the control of employees in the event of concrete suspicion of a potentially criminal offense.

Finally, ATP has stated in relation to fraud control that the authority - as far as the employees who handle compensation payments in AES 'area of authority are concerned - makes daily manual assurance of whether the employees' change of the account to which payment is to be made is documented in the case. The fraud check consists of a list being drawn every day in the NemKonto system, which shows which account number changes have been made on the previous day. The employees who handle compensation payments in AES 'area of authority then check whether the account information entered is correct. An employee may not check his or her own account number changes. Once the list has been checked and found ok among the employees, the list is passed on to a specific person for a final check, after which the list is put in a specific folder. If errors

are found in the account number change, the error must be corrected and the correction must be briefly described in the list.

In this connection, the Danish Data Protection Agency should note that such a fraud check, in the Authority's assessment, does not in principle have the character of a control measure covered by this supervision, as in the Authority's opinion it is an established procedure to ensure that compensation payments are made correctly. Thus, with this supervision, the Danish Data Protection Agency has not taken a position on ATP's observance of the duty to provide information in connection with the processing of personal data as part of the authority's fraud control.

3. Procedures, etc. in relation to the fulfillment of the duty to provide information and prior information on control measures

ATP has generally stated that the authority's employees are informed via the employment contract that they as an employee are covered by guidelines and rules applicable to the employment relationship, including e.g. the authority's information security policy and that these rules and guidelines can be accessed via the authority's intranet (employee portal). In this connection, ATP has sent a copy of such an employment contract to the Authority.

Upon joining, the employees receive a welcome email, which i.a. contains a direct link to ATP's employee portal, where the employee can read about what is otherwise expected of the individual employee in connection with the employment relationship. ATP has sent a copy of the welcome email to the Danish Data Protection Agency. In this connection, it is the Authority's assessment that employees are not made aware of the use of control measures in the welcome email.

For the purpose of complying with the rules on the duty to provide information, ATP has prepared a general information text regarding the authority's processing of personal data about employees, which the employees can access via the employee portal. The information text is supplemented by a number of separate information about the individual control measures, which can also be accessed via the employee portal.

ATP has subsequently stated that the authority - as part of an ongoing effort to uncover the authority's compliance with Articles 13 and 14 of the Data Protection Regulation in connection with employment relationships - has expanded the above-mentioned information text to employees. ATP has stated that the expanded text is valid from 4 October 2019, which is after the date of the Data Inspectorate's notification of the inspection to AES on 9 September 2019. The Data Inspectorate has thus not taken a position on the content of the expanded information text in this decision, but has noted that ATP has updated the text.

In connection with the audit, ATP has sent a copy of the information text regarding ATP's processing of employees' personal

data that was valid prior to 4 October 2019. In addition, ATP has sent a copy of the relevant information on the authority's employee portal, which relates to the authority's use of control measures. .

ATP's employment contracts, policy and guidelines for information security, the information text regarding the processing of employees' personal data and the other information on the employee portal are reviewed below under section 4.

It is after a review of the material submitted by ATP the Data Inspectorate's understanding that ATP has not prepared written procedures, etc. for the authority's compliance with the data protection regulation's rules on the duty to provide information and the requirement for prior information in connection with the use of control measures against employees.

In this connection, the Danish Data Protection Agency must recommend that ATP prepare procedures, etc. for the authority's compliance with the rules on the duty to provide information and prior information in connection with control measures towards employees, where it i.a. should state how and at what time employees must be informed of the processing of personal data that takes place in connection with the individual control measures.

Review of ATP's information text and information on the employee portal

ATP has stated [3] that the authority makes use of a number of control measures - which can be used for both operational, safety and control purposes - towards the authority's employees. The Danish Data Protection Agency cannot rule out that these are used for control purposes against the authority's employees, which is why this has been taken into account in the review of the submitted material.

In general, ATP has stated [4] that the authority's employees are informed via the employment contract that they as an employee of ATP are covered by guidelines and rules applicable to the employment relationship, including e.g. the Authority's information security policy and associated guidelines. In addition, ATP has prepared an information text regarding the authority's processing of personal data about employees, which the employees can access via the employee portal. The information text is supplemented by a number of separate information about the individual control measures, which can also be accessed via the employee portal.

Following a review of the submitted examples of employment contracts, the Danish Data Protection Agency's assessment is that the contracts do not contain specific information about ATP's processing of personal data in connection with the use of control measures against employees. Employees are only made aware that they are covered by - and obliged to keep up to date with - ATP's current guidelines and rules for the employment relationship, including e.g. the authority's information

security policy, which can be found on the employee portal. In addition, it appears from the contracts that it is a prerequisite for joining and remaining in the employment relationship that the employees' criminal record does not give rise to comments.

As the information text on the employee portal regarding ATP's processing of employees' personal data - in the Data Inspectorate's assessment - is of a more general nature and does not contain specific information about the individual control measures that the authority uses towards employees, the content of the information text is reviewed immediately. information on ATP's employee portal about the individual control measures is reviewed.

The information text regarding the processing of personal data about employees states that ATP processes information about the employees for the purpose of handling all administration related to the employment relationship, including salary payment, time registration, administration of sickness benefits, leave and maternity benefits, etc.

The information text contains a general description of the categories of personal data that ATP processes about employees. It thus appears that ATP processes information about name, address, civil registration number, position, education, salary conditions, tax conditions, bank account, working hours, absence and criminal conditions and the like. In continuation of this, the information text contains information about any categories of recipients of the information.

In addition, the information text contains information on how and for how long the information is stored. It thus appears that the information about the employees is stored in an electronic personnel case in a specific system, and that ATP deletes the employees' personal information five years after the end of the year in which the employees resign.

Employees are also informed about the right to request insight into and correction or deletion of personal data as well as the right to data portability. In continuation of this, contact information has been inserted on the authority's data protection adviser.

Finally, the appendix contains information on the possibility of complaining about ATP's processing of personal data to the Danish Data Protection Agency.

4.1. Regarding information on logging the use of the internet, professional systems and rejected access attempts

ATP has stated that employees are informed about logging of the use of the Internet, professional systems and rejected access attempts in the authority's policy and guidelines for information security, which are referred to in the employment contracts. In addition, employees are informed about the logging via the employee portal.

In connection with the audit, ATP has sent a copy of the authority's policy for information security. Following a review of the information security policy, the Danish Data Protection Agency's assessment is that the policy does not contain information

about the processing of personal data that takes place in connection with logging of the use of the Internet, professional systems and rejected access attempts. According to the Authority's assessment, the policy only contains information on ATP's internal policy for information security in a number of specified areas, including organization and function separation, operation / securing of facilities and IT solutions as well as logging.

ATP has also sent a copy of the authority's guidelines for information security, including guidelines for logging and monitoring. Following a review of the guidelines, the Danish Data Protection Agency's assessment is that these do not contain information on the processing of personal data that takes place in connection with logging of the use of the Internet, professional systems and rejected access attempts. The guidelines describe - in the Authority's assessment - only how the information security policy is to be handled in ATP's task solution, including e.g. which specific areas where logging should be performed as a starting point and how the log information should be protected against tampering and unauthorized access.

Finally, ATP has sent a copy of the information on logging the use of the internet, professional systems and rejected access attempts, which the employees can access via the employee portal.

On the employee portal, it appears about logging that ATP carries out inspections in professional systems, etc. to ensure that the authority's guidelines and rules are complied with. The checks are carried out by random sampling and data analyzes. In addition, it appears that there is no general monitoring and control of employees' use of the Internet, but that ATP can follow up on a logging if there is a concrete suspicion of abuse or hacking.

As the Data Inspectorate's opinion is collected from the employee himself, when he or she uses resp. Internet and professional systems, the Authority's assessment is that notification of the processing of personal data in connection with the logging of the use of the Internet, professional systems and rejected access attempts must comply with the requirements of Article 13 of the Data Protection Regulation.

After a review of the submitted material, including ATP's policy and guidelines for information security, the general information text on the processing of personal data and the information on logging on the employee portal, it is the Data Inspectorate's assessment that employees are not given information about the legal basis for processing.

In addition, it is the Data Inspectorate's assessment that employees are not given information about the period during which the logo information will be stored, or if this is not possible, the criteria used to determine this period. In this connection, the Danish Data Protection Agency has emphasized that it is not sufficiently clear from the general information text on the

processing of personal data how long the logo information is stored, as the information text only contains an overall description of when information about employees is processed in connection with personnel administration , deleted. The Danish Data Protection Agency has also emphasized that this information - in the Authority's view - is necessary to ensure fair and transparent processing as far as the employees are concerned.

On this basis, the Danish Data Protection Agency finds that ATP's notification of the processing of personal data in connection with logging of the use of the Internet, professional systems and rejected access attempts does not meet the requirements of Article 13 (1) of the Data Protection Regulation. 1, letter c and para. 2, letter a.

4.2. Regarding information on logging access to physical locations and time registration

ATP has stated that employees are informed about logging access to physical locations and time registration in the authority's policy and guidelines for information security, which are referred to in the employment contracts. In addition, employees are informed about the logging via the employee portal.

In connection with the audit, ATP has sent a copy of the authority's policy for information security. Following a review of the information security policy, the Danish Data Protection Agency's assessment is that the policy does not contain information on the processing of personal data that takes place in connection with logging of access to physical locations and time registration. According to the Authority's assessment, the information security policy only contains information on ATP's internal policy for information security in a number of specified areas, including e.g. organization and function separation, operation / securing of facilities and IT solutions as well as logging.

ATP has also sent a copy of the authority's guidelines for information security, including guidelines for physical perimeter security and access control. Following a review of the guidelines, the Danish Data Protection Agency's assessment is that these do not contain information on the processing of personal data that takes place in connection with logging of access to physical locations and time registration. The guidelines describe - in the Authority's assessment - only how the information security policy is to be handled in the authority's task solution. It states, among other things, that buildings must be designed in such a way that unauthorized persons are prevented from entering certain areas, and that electronic access control systems must ensure that only authorized persons have access to buildings, office areas and any special areas to which there is a work-related needs. In addition, it appears that everyone must carry a visible access card, and that access cards must not be lent to others, and that access cards must be able to be blocked in the access control system.

The employee portal states that ATP has established an access control system, and that access control has been set up at external access doors and internal doors to special areas, technical rooms and the like. Furthermore, it states that employees must use the access card both when they arrive in the morning and when they go home, and that this registration is important to keep track of who is in the building in case of evacuation.

In addition, it states how employees should use the access card and what to do if they have lost or forgotten their access cards.

Finally, it appears that the access control system is coupled with the flex time system. The first registration of the day will be used as arrival time and the last registration time of the day as walking time. The employee must therefore be aware that there may be a need to change their time registration if, for example, you exercise during working hours.

In the opinion of the Danish Data Protection Agency, as the personal data is collected from the employee himself when he uses his access card, the Authority's assessment is that notification of the processing of personal data in connection with access control must comply with the requirements of Article 13 of the Data Protection Regulation.

After a review of the submitted material, including ATP's policy and guidelines for information security, the general information text on the processing of personal data and the information on access to physical locations and time registration on the employee portal, it is the Data Inspectorate's assessment that employees are not given information about the purpose of processing. of the personal data and the legal basis for the processing. The Danish Data Protection Agency has emphasized that, in the Authority's opinion, it is not sufficiently clear that the logo information in question can also be used for control purposes against the employees.

In addition, it is the Data Inspectorate's assessment that employees are not given information about the period during which the logo information will be stored, or if this is not possible, the criteria used to determine this period. In this connection, the Danish Data Protection Agency has emphasized that it is not sufficiently clear from the general information text on the processing of personal data how long the information is stored, as the information text only contains an overall description of when information about employees is processed in connection with personnel administration, deleted. The Danish Data Protection Agency has also emphasized that this information - in the Authority's view - is necessary to ensure fair and transparent processing as far as employees are concerned.

On this basis, the Danish Data Protection Agency finds that ATP's notification of the processing of personal data in connection

with logging of access to physical locations and time registration does not meet the requirements of Article 13 (1) of the Data Protection Regulation. 1, letter c and para. 2, letter a.

In view of the fact that, in the opinion of the Danish Data Protection Agency, the control purpose has not been sufficiently transparent for employees, the Authority also finds that ATP's information on logging access to physical locations and time registration has not complied with the basic principle of transparency in Article 5 (1). 1, letter a. In this connection, the Danish Data Protection Agency must also emphasize that it is the Authority's assessment that the principle of transparency i.a. implies that the data controller must provide employees with easily accessible - prior - information about the control measures used, including in particular about the control purpose.

4.3. Regarding information about access to employees' e-mails

ATP has stated that the authority's employees are informed that their e-mail can be accessed after resigning on the employee portal.

In connection with the audit, ATP has sent a copy of the information on access to former employees' e-mails, which the employees can access via the employee portal

The employee portal states that ATP has the right to gain access to an employee's email account without consent, for example in situations where there is a need to find correspondence regarding a case or to insert an autoresponder if an employee has resigned or cannot be contacted. .

Furthermore, it appears that in such situations it will be the manager who - in agreement with HR -

reviews the mail account and forwards the relevant correspondence.

In continuation of this, it appears that ATP does not have the right to read employees' private emails, which is why it is recommended to write "privately" in the subject field in order for ATP to be able to identify private correspondence.

Finally, it appears that ATP can gain access to an employee's email account in order to be able to react quickly if a security breach occurs. In such cases, the employee will subsequently be informed of the background for this.

In the opinion of the Data Inspectorate, as the personal data is collected from the employee himself via the employee's e-mail account, the Authority's assessment is that notification of the processing of personal data in connection with access to employees' e-mails must meet the requirements of Article 13 of the Data Protection Regulation.

After a review of the submitted material, including ATP's general information text on the processing of personal data and the

information on access to employees' e-mails on the employee portal, it is the Data Inspectorate's assessment that employees are not given information on the purpose of processing personal data and the legal basis for processing. The Danish Data Protection Agency has emphasized that, in the Authority's view, it is not sufficiently clear that information processed in connection with access to the employee's e-mails can also be used for control purposes against the employees.

In addition, it is the Data Inspectorate's assessment that employees are not given information about the period during which the information will be stored, or if this is not possible, the criteria used to determine this period. In this connection, the Danish Data Protection Agency has stated that it is not sufficiently clear from the general information text on the processing of personal data how long the information is stored, as the information text only contains an overall description of when information about employees is processed in connection with personnel administration. deleted. The Danish Data Protection Agency has also emphasized that this information - in the Authority's view - is necessary to ensure fair and transparent processing as far as employees are concerned.

On this basis, the Danish Data Protection Agency finds that ATP's notification of the processing of personal data in connection with logging of access to employees' e-mails does not meet the requirements of Article 13 (1) of the Data Protection Regulation. 1, letter c and para. 2, letter a.

Considering that, in the opinion of the Danish Data Protection Agency, the control purpose has not been sufficiently transparent for employees, the Authority also finds that ATP's information regarding access to employees' e-mails has not complied with the basic principle of transparency in Article 5 (1) of the Regulation. 1, letter a. In this connection, the Danish Data Protection Agency must also emphasize that it is the Authority's assessment that the principle of transparency i.a. implies that the data controller must provide employees with easily accessible - prior - information about the control measures used, including in particular about the control purpose.

4.4. Regarding information on TV surveillance

ATP has stated that the authority's employees are informed about the TV surveillance via signage in and around buildings and physical locations. In this connection, ATP has sent pictures of the signage at the various locations.

Private and public authorities that carry out television surveillance of places or premises where there is general access to, or of workplaces, must, according to the Television Surveillance Act [5], provide information about the surveillance by means of signs or other clear means. In addition to the requirement for signage, the rules of the Data Protection Regulation and the Data

Protection Act on the duty to provide information to data subjects apply.

It thus follows from section 3 b of the Television Surveillance Act that the provision in Article 14 of the Data Protection Ordinance applies regardless of any signage pursuant to sections 3 and 3 a of the Act. to the requirements of Article 14 of the Data Protection Regulation.

Based on the images transmitted, the Danish Data Protection Agency can conclude that the signage only contains information about the fact that television surveillance is carried out. The sign consists of an image of a surveillance camera with a caption that says "The area is TV-monitored". In addition, a telephone number is specified on SensorTek, which the Danish Data Protection Agency assumes is the system supplier.

After a review of the submitted material, including ATP's signage regarding TV surveillance and the general information text on the processing of personal data, it is the Data Inspectorate's assessment that employees are not given information about the purpose of the processing of personal data and the legal basis for processing. In this connection, the Danish Data Protection Agency has emphasized that, in the Authority's view, it is not sufficiently clear that information processed in connection with television surveillance can also be used for control purposes vis-à-vis employees.

It is also the Data Inspectorate's assessment that employees are not given sufficient information about the affected categories of personal data. The Danish Data Protection Agency has emphasized that the general information text on the processing of personal data only contains an overall indication of the categories of personal data that are processed in connection with personnel administration, and that it does not appear from the information text or signage which categories of information are processed in in connection with television surveillance.

In addition, it is the Data Inspectorate's assessment that employees are not given information about the period during which the information will be stored, or if this is not possible, the criteria used to determine this period. In this connection, the Danish Data Protection Agency has stated that it is not sufficiently clear from either the signage or the general information text on the processing of personal data how long information processed in connection with television surveillance is stored. The Danish Data Protection Agency has also emphasized that this information - in the Authority's view - is necessary to ensure fair and transparent processing as far as employees are concerned.

On this basis, the Danish Data Protection Agency finds that ATP's notification of the processing of personal data in connection with logging of access to employees' e-mails does not meet the requirements of Article 14 (1) of the Data Protection

Regulation. 1, letters c and d, and para. 2, letter a.

In view of the fact that, in the opinion of the Danish Data Protection Agency, the purpose of control has not been sufficiently transparent for employees, the Authority also finds that ATP's information on television surveillance has not complied with the basic principle of transparency in Article 5 (1) of the Regulation. 1, letter a. In this connection, the Danish Data Protection Agency must also emphasize that it is the Authority's assessment that the principle of transparency i.a. implies that the data controller must provide employees with easily accessible - prior - information about the control measures used, including in particular about the control purpose.

As television surveillance is an intrusive form of processing of personal data, the Danish Data Protection Agency must generally emphasize the importance of ATP employees being informed of the processing of personal data that takes place in connection with the use of television surveillance as a control measure under Article 14 of the Regulation.

4.5. Observance of the duty to provide information in a transparent and easily accessible form

It follows from Article 12 (1) of the Data Protection Regulation 1, that the data controller must give any notification in accordance with i.a. Articles 13 and 14 on processing to the data subject in a concise, transparent, easy-to-understand and easily accessible form and in a clear and simple language.

ATP has stated that the authority's employees are to a certain extent informed about the use of control measures via the information in the employment agreement, including e.g. by referring the employees to the applicable guidelines and rules and by informing the employees that it is a prerequisite for joining and remaining in the employment relationship that the employees' criminal record does not give rise to remarks.

Upon joining, the employees also receive a welcome email, which i.a. contains a direct link to ATP's employee portal, where employees can read more about what is expected during the employment relationship. As mentioned [6], the Danish Data Protection Agency's assessment is that employees are not made aware of the use of control measures in the welcome email.

For the purpose of complying with the rules on the duty to provide information, ATP has prepared a general information text regarding the authority's processing of personal data about employees, which the employees can access via the employee portal. The information text is supplemented by a number of separate information about the individual control measures, which can also be accessed via the employee portal.

In connection with this supervision, the Danish Data Protection Agency has assessed whether the information provided by ATP

to employees in accordance with Articles 13 and 14 of the Regulation meets the requirements of Article 12 (1) of the Regulation. 1, including whether the information is provided to employees in a sufficiently easily accessible form.

After a review of the material submitted by ATP, the Danish Data Protection Agency finds that ATP's compliance with the duty of disclosure to employees in connection with the use of control measures has not taken place in accordance with Article 12 (1) of the Regulation. 1, as the information provided by ATP to employees pursuant to Articles 13 and 14 of the Regulation in connection with the use of control measures is not, in the opinion of the Authority, provided to employees in a sufficiently easily accessible form.

The Danish Data Protection Agency has emphasized that the employment contracts and the welcome email do not, in the Authority's assessment, contain information on the processing of personal data that takes place in connection with the use of control measures, nor that the employment contract or the welcome email refers to the specific places on the employee portal. , where employees can read about this. It is thus the Authority's assessment that it will require special attention from the employees if they are to become familiar with information about ATP's processing of personal data in connection with the use of control measures.

The Danish Data Protection Agency has noted that from 4 October 2019, ATP will present an expanded information text for employees, which contains more specific information about the use of control measures and the processing of personal data that takes place in this connection, already in connection with signing the employment contract.

5. Conclusion

Following the audit of ATP, the Danish Data Protection Agency finds reason to conclude:

That ATP's compliance with the duty to provide information pursuant to Articles 13 and 14 of the Regulation has been deficient, including in that the authority has not provided employees with sufficiently clear information about the purpose of the processing, the legal basis for the processing, the categories of personal data concerned and the period will be kept, or if this is not possible, the criteria used to determine this period.

That ATP's observance of observance of the duty to provide information has not taken place in a sufficiently easily accessible form in accordance with Article 12 (1) of the Regulation. 1.

The Data Inspectorate finds in relation to pkt. 1 and 2 basis for expressing serious criticism that ATP's processing of personal data has not taken place in accordance with Article 12 (1) of the Data Protection Regulation. 1, Articles 13 and 14. With regard

to lack of information about the purpose of processing personal data, the Danish Data Protection Agency further finds that ATP's processing of personal data has not taken place in accordance with the basic principle of transparency in Article 5 (1) of the Regulation. 1, letter a.

The Danish Data Protection Agency has noted that ATP on 4 October 2019, ie. after the date of notification of the supervision on 9 September 2019, has expanded the disclosure text that the authority uses to comply with the disclosure obligation. It is noted, however, for the sake of good order, that the Authority has not taken a position on the content of the extended information text.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to

on the processing of personal data and on the free movement of such data and on the repeal of Directive 95/46 / EC (General Data Protection Regulation).

[2] Act No. 502 of 23 May 2018 on supplementary provisions to the Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (the Data Protection Act).

[3] See Section 2 of the Decision

[4] See section 3 of the Decision

[5] Statutory Order no. 1190 of 11 October 2007 on television surveillance with subsequent amendments

[6] See section 3 of the Decision